ONTAP 9 ドキュメント

ONTAP 9

NetApp
October 24, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/index.html on October 24, 2025.
Always check docs.netapp.com for the latest.

目次

ONTAP 9 ドキュメント . . . 1
リリースノート . . . 2
ONTAP 9リリースのハイライト . . . 2
ONTAP 9.17.1のハイライト . . . 2
ONTAP 9 .16.1の特長 . . . 3
ONTAP 9 .15.1の特長 . . . 4
ONTAP 9.14.1のハイライト . . . 5
ONTAP 9 .13.1の特長 . . . 6
ONTAP 9.12.1のハイライト . . . 7
ONTAP 9.11.1のハイライト . . . 8
ONTAP 9.10.1のハイライト . . . 9
ONTAP 9.9.1のハイライト . . . 10
ONTAP 9.17.1の新機能 . . . 10
データ保護 . . . 11
S3オブジェクトストレージ . . . 11
セキュリティ . . . 12
ストレージリソース管理の機能拡張 . . . 12
ONTAP 9.16.1の新機能 . . . 13
データ保護 . . . 13
ネットワーク . . . 14
S3オブジェクトストレージ . . . 14
SAN . . . 15
セキュリティ . . . 15
Storage Efficiency . . . 16
ストレージリソース管理の機能拡張 . . . 16
System Manager . . . 17
ONTAP 9.15.1の新機能 . . . 17
データ保護 . . . 18
セキュリティ . . . 18
Storage Efficiency . . . 19
ストレージリソース管理の機能拡張 . . . 20
System Manager . . . 20
アップグレード . . . 20
ONTAP 9.14.1の新機能 . . . 21
データ保護 . . . 21
ファイル アクセス プロトコル . . . 22
S3オブジェクトストレージ . . . 22
SAN . . . 22
セキュリティ . . . 23

Storage Efficiency . . . 23
ストレージリソース管理の機能拡張 . . . 24
SVM管理の機能拡張 . . . 24
System Manager . . . 24
ONTAP 9.13.1の新機能 . . . 25
データ保護 . . . 25
ファイル アクセス プロトコル . . . 26
ネットワーク . . . 26
S3オブジェクトストレージ . . . 26
SAN . . . 27
セキュリティ . . . 27
Storage Efficiency . . . 27
ストレージリソース管理の機能拡張 . . . 28
SVM管理の機能拡張 . . . 28
System Manager . . . 29
ONTAP 9.12.1の新機能 . . . 29
データ保護 . . . 29
ファイル アクセス プロトコル . . . 30
ネットワーク . . . 31
S3オブジェクトストレージ . . . 31
SAN . . . 31
セキュリティ . . . 32
Storage Efficiency . . . 32
ストレージリソース管理の機能拡張 . . . 32
SVM管理の機能拡張 . . . 33
System Manager . . . 33
ONTAP 9.11.1の新機能 . . . 34
データ保護 . . . 34
ファイル アクセス プロトコル . . . 35
ネットワーク . . . 36
S3オブジェクトストレージ . . . 36
SAN . . . 36
セキュリティ . . . 36
Storage Efficiency . . . 37
ストレージリソース管理の機能拡張 . . . 37
SVM管理の機能拡張 . . . 37
System Manager . . . 38
ONTAP 9.10.1の新機能 . . . 39
データ保護 . . . 39
ファイル アクセス プロトコル . . . 39
ネットワーク . . . 40
S3オブジェクトストレージ . . . 40

SAN 40
セキュリティ 41
Storage Efficiency 41
ストレージリソース管理の機能拡張 41
SVM管理の機能拡張 41
System Manager 42
ONTAP 9.9.1の新機能 43
データ保護 43
ファイル アクセス プロトコル 44
ネットワーク 44
S3オブジェクトストレージ 45
SAN 45
セキュリティ 45
Storage Efficiency 46
ストレージリソース管理の機能拡張 46
System Manager 46
ONTAPの制限とデフォルトに対する変更 48
ONTAPノテフオルトノヘンコウ 48
ONTAPの制限に対する変更 49
ONTAP 9リリースのサポート 51
サポート レベル 52
開始する 53
ONTAPの詳細 53
ONTAPプラットフォーム 53
ONTAPユーザインターフェイス 54
ONTAP System Manager とNetAppコンソールを統合する 55
クラスタストレエシ 57
ハイアベイラビリティペア 58
AutoSupportとデジタルアドバイザ 59
ネットワークアーキテクチャ 60
クライアントプロトコル 64
ディスクとローカル階層 66
ボリューム、qtree、ファイル、LUN 72
ストレージ仮想化 74
パスのフェイルオーバー 77
ONTAPテノロオトハランシンク 80
レプリケーション 82
Storage Efficiency 89
セキュリティ 101
ONTAPとVMware vSphere 107
FabricPool 109
ONTAP でのクイックスタート 109

ONTAPクラスタをセットアップする 111
ONTAPクラスタセットアップワークフローの概要 111
ONTAPクラスタをセットアップするための情報を収集します。 112
ONTAPクラスタを作成してノードを追加 116
必要に応じて、ONTAP管理LIFをIPv4からIPv6に変換する 120
Digital Advisor Config AdvisorでONTAPクラスタを確認する 121
ONTAPクラスタ全体のシステム時間を同期する 122
ONTAPソフトウェアとファームウェアのアップグレードとリバート 126
ONTAPのアップグレード 126
ONTAPアップグレードの詳細 126
ONTAPはいつアップグレードすればよいですか。 126
計画的アップグレードの前にONTAPの自動アップグレード前チェックを実行 128
ONTAPのアップグレードの準備 141
アップグレード前にONTAPソフトウェアイメージをダウンロードする 230
ONTAPのアップグレード方法 231
ONTAPアップグレード後の作業 288
ファームウェア、システム、セキュリティの更新 303
ONTAPでのファームウェア、システム、セキュリティの更新の概要 303
インストールの自動更新をスケジュールする方法 305
自動更新を有効にする 306
自動更新の変更 308
推奨される自動更新の管理 309
ファームウェアの手動更新 310
ONTAPのリバート 314
ONTAPクラスタをリバートするにはテクニカルサポートが必要ですか。 314
サポートされるONTAPリバートパス 314
ONTAPのリバートに関する問題と制限事項 315
ONTAPリバートの準備 316
ONTAPソフトウェアイメージのダウンロードとインストール 335
ONTAPクラスタをリバートします。 337
ONTAPリバート後の処理 346
クラスタの管理 356
System Managerでのクラスタ管理 356
ONTAP System Managerを使用したクラスタ管理について学習します 356
System Managerを使用してONTAPクラスタにアクセスする 357
ONTAPクラスタでプロトコルを設定する 359
ONTAP System Managerでライセンスキーを追加して新機能を有効にする 359
ONTAP System Managerを使用してクラスタ構成をダウンロードする 359
ONTAP System Managerを使用してクラスタにタグを割り当てる 360
ONTAP System Manager を使用してサポートケースを表示および送信する 361
ONTAP System ManagerでストレージVMの最大容量制限を管理する 362

ONTAP System Managerでクラスタ、階層、SVMの容量を監視する 363
ONTAP System Managerでハードウェア構成を表示して問題を特定します 366
ONTAP System Managerを使用してノードを管理する 371
ライセンス管理 373
ONTAPライセンスの概要 373
NetAppサポートサイトからNetAppライセンスファイル（NLF）をダウンロードします。 376
ONTAPへのNetAppライセンスのインストール 377
ONTAPライセンスを管理します。 379
ライセンスタイプとライセンス方式 381
ONTAPテノライセンスノカンリヨウコマント 382
CLIを使用したクラスタ管理 383
ONTAP CLIを使用したクラスタ管理について 383
クラスタ管理者とSVM管理者 383
CLIを使用したクラスタへのアクセス（クラスタ管理者のみ） 385
ONTAPコマンドライン インターフェイスの使用 398
ONTAP CLIセッションの記録と記録されたセッションの管理 413
クラスタ管理（クラスタ管理者のみ） 414
ノードの管理 419
SP / BMCネットワークの設定 444
SP / BMCを使用したノードのリモート管理 451
ONTAPクラスタ時間の管理（クラスタ管理者のみ） 481
バナーとMOTDの管理 483
ONTAPジョブおよびジョブスケジュールを管理します。 493
クラスタ構成のバックアップとリストア（クラスタ管理者のみ） 496
ONTAPクラスタのノードコアダンプの管理（クラスタ管理者のみ） 506
ディスクと階層の管理 508
ディスクとONTAPローカル階層 508
ローカル階層の管理 509
ディスクの管理 552
RAID構成の管理 586
Flash Poolローカル階層を管理します。 592
FabricPool階層の管理 608
ONTAP FabricPoolによるデータ階層化の詳細 608
ONTAP FabricPoolの使用要件 609
ONTAP FabricPoolポリシーによるデータの効率的な階層化 614
ONTAP FabricPool の設定と管理タスクについて学習します 618
FabricPoolの設定 619
FabricPoolの管理 638
FabricPoolミラーを管理します。 662
FabricPoolリソースを管理するためのONTAPコマンド 670
SVMのデータ移動 673

SVMのデータ移動の概要 673
SVMの移行 681
ボリューム移行の監視 683
SVM 移行を一時停止して再開します 683
SVMの移行をキャンセルする 684
クライアントの手動カットオーバー 685
クライアントのカットオーバー後にソースSVMを手動で削除する 685
HAペアの管理 685
ONTAPクラスタにおけるHAペア管理について学ぶ 685
ONTAP クラスタにおけるハードウェアアシストテイクオーバーについて学ぶ 687
ONTAP クラスタの自動テイクオーバーとギブバックについて学ぶ 688
ONTAP自動テイクオーバーコマンド 692
ONTAP自動ギブバックコマンド 692
ONTAP 手動テイクオーバーコマンド 695
ONTAP 手動ギブバックコマンド 698
ONTAP クラスタでのテイクオーバーとギブバックのテスト 701
HAペアを監視するためのONTAPコマンド 703
ストレージフェイルオーバーを有効または無効にするONTAPコマンド 708
2ノードクラスタでテイクオーバーを開始せずにONTAPノードを停止または再起動する 708
System ManagerによるREST API管理 711
System ManagerによるREST API管理 711
REST APIログへのアクセス 712
ボリューム管理 714
System ManagerによるボリュームとLUNの管理 714
ONTAP System Manager によるボリューム管理の概要について学習します 714
ボリュームの管理 714
ONTAP System ManagerでLUNを管理する 720
ONTAP System Managerでストレージを拡張 723
ONTAP System Manager による圧縮、コンパクション、重複排除を使用してストレージスペースを節約します。 724
ONTAP System Managerを使用してLUNを移動することで負荷を分散します 725
ONTAP System Managerを使用してボリュームを別の階層に移動することで負荷を分散します 726
Ansible Playbook を使用して、ONTAP System Manager でボリュームまたは LUN を追加または編集します。 726
ONTAP System Managerでストレージ効率ポリシーを管理する 728
ONTAP System Managerでクォータを使用してリソースを管理する 729
ONTAP System Managerでクォータを設定してリソースの使用を制限する 730
ONTAP System Manager でテストするためのボリュームと LUN のクローンを作成する 730
ONTAP System Managerで情報を検索、フィルタリング、並べ替える 733
CLIを使用した論理ストレージ管理 735
CLIを使用した論理ストレージ管理の概要 735

ボリュームの作成と管理 736
ボリュームの移動とコピー 757
FlexCloneボリュームを使用してFlexVolボリュームの効率的なコピーを作成する 765
FlexCloneファイルとFlexClone LUNを使用して、ファイルとLUNの効率的なコピーを作成する 771
qtreeを使用してFlexVolをパーティショニングする 780
ボリュームの論理スペースのレポートと適用 785
クォータを使用してリソース使用量を制限または追跡する 793
重複排除、データ圧縮、データコンパクションを使用してストレージ効率を向上 838
あるSVMから別のSVMにボリュームをリホストする 868
推奨されるボリュームとファイルまたはLUNの設定の組み合わせ 876
ファイルおよびディレクトリの容量を変更する際の注意事項および考慮事項 881
FlexCloneファイルとFlexClone LUNでサポートされる機能 884
FlexGroupホリユウムノカンリ 887
CLIを使用したONTAP FlexGroupボリューム管理の詳細 887
ONTAP FlexGroupボリュームの詳細 887
ONTAP FlexGroupボリュームでサポートされる構成とサポートされない構成 888
FlexGroupボリュームのセットアップ 893
FlexGroupボリュームを管理します。 901
FlexGroupのデータ保護 940
FlexGroupボリュームのデータ保護処理を管理します。 961
FlexVolボリュームからFlexGroupボリュームへの変換 979
FlexCacheホリユウムノカンリ 986
ONTAP FlexCacheボリュームの詳細 986
ONTAP FlexCacheでサポートされる機能とサポートされない機能 988
ONTAP FlexCacheボリュームのサイジングに関するガイドライン 994
ONTAP FlexCacheボリュームの作成 994
FlexCacheライトバック 999
FlexCacheボリュームを管理します。 1015
FlexCacheによるホットスポット修復 1022
ネットワーク管理 1036
開始する 1036
System Managerを使用したONTAPネットワークの可視化 1036
ONTAPクラスタのネットワークコンポーネントの詳細 1037
ONTAPネットワークケーブル接続のベストプラクティス 1039
ONTAPネットワークで使用するLIFフェイルオーバーポリシーを決定する 1041
NAS パスのフェイルオーバーワークフロー 1043
ONTAPネットワークでのNASパスのフェイルオーバーの設定 1043
ONTAPネットワークでのNASパスのフェイルオーバーに関するワークシート 1044
ネットワークポート 1050
ONTAPネットワークポート設定の詳細 1050
ネットワークポートの設定 1051

IPspace 1082
ONTAP IPspace設定の詳細 1082
ONTAPネットワーク用のIPspaceの作成 1085
ONTAPネットワーク上のIPspaceの表示 1087
ONTAPネットワークからのIPspaceの削除 1087
ブロードキャストドメイン 1088
ONTAPブロードキャストドメインの詳細 1088
ONTAPブロードキャストドメインの作成 1089
ONTAPブロードキャストドメインのポートを追加または削除する 1092
ONTAPポートの到達可能性を修復 1095
ONTAPブロードキャストドメインをIPspaceに移動します。 1102
ONTAPブロードキャストドメインのスプリット 1103
ONTAPブロードキャストドメインのマージ 1104
ONTAPブロードキャストドメインのポートのMTU値を変更する 1105
ONTAPブロードキャストドメインの表示 1106
ONTAPブロードキャストドメインの削除 1107
フェイルオーバーグループとポリシー 1108
ONTAPネットワークでのLIFフェイルオーバーの詳細 1108
ONTAPフェイルオーバーグループを作成する 1109
LIFのONTAPフェイルオーバーを設定します。 1110
フェイルオーバーグループとポリシーの管理用ONTAPコマンド 1112
サブネット（クラスタ管理者のみ） 1112
ONTAPネットワークのサブネットについて 1112
ONTAPネットワークのサブネットを作成する 1113
ONTAPネットワークのサブネットに対してIPアドレスを追加または削除する 1115
ONTAPネットワークのサブネットプロパティの変更 1117
ONTAPネットワークのサブネットを表示する 1119
ONTAPネットワークからサブネットを削除する 1120
ONTAPネットワーク用のSVMの作成 1120
論理インターフェイス（LIF） 1128
LIFの概要 1128
LIFの管理 1139
ONTAP仮想IP（VIP）LIFの設定 1159
ネットワーク負荷の分散 1167
DNSロードバランシングを使用したONTAPネットワークトラフィックの最適化 1167
ONTAPネットワークのDNSロードバランシングの詳細 1167
ONTAPネットワーク用のDNSロードバランシングゾーンを作成する 1167
ロードバランシングゾーンに対するONTAP LIFの追加または削除 1168
ONTAPネットワーク用のDNSサービスの設定 1169
ONTAPネットワークの動的DNSサービスの設定 1172
ホストメイカイケツ 1173

ONTAPネットワークのホスト名解決について 1173
ONTAPネットワークのホスト名解決に使用するDNSの設定 1174
ONTAP hostsテーブルを管理するONTAPコマンド 1175
ネットワークのセキュリティを確保 1176
すべてのSSL接続にFIPSを使用したONTAPネットワークセキュリティの設定 1176
IPSec転送中暗号化の設定 1180
ONTAPネットワーク内のLIFのファイアウォールポリシーを設定する 1189
ファイアウォールサービスとポリシーを管理するためのONTAPコマンド 1195
QoSマーキング（クラスタ管理者のみ） 1196
ONTAPネットワークQuality of Service（QoS；サービス品質）の詳細 1196
ONTAPネットワークのQoSマーキング値を変更します。 1196
ONTAPネットワークのQoSマーキング値の表示 1197
SNMPの管理（クラスタ管理者のみ） 1197
ONTAPネットワーク上のSNMPの詳細 1198
ONTAPネットワーク用のSNMPコミュニティの作成 1199
ONTAPクラスタでのSNMPv3ユーザの設定 1202
ONTAPネットワークでSNMPのトラップホストを設定する 1206
ONTAPクラスタでのSNMPポーリングの確認 1207
SNMP、トラップ、およびトラップホストを管理するためのONTAPコマンド 1208
SVMのルーティングを管理します。 1211
ONTAPネットワークでのSVMルーティングの詳細 1211
ONTAPネットワークの静的ルートを作成する 1211
ONTAPネットワークのマルチパスルーティングを有効にする 1212
ONTAPネットワークから静的ルートを削除する 1212
ONTAPルーティング情報の表示 1213
ONTAPネットワークのルーティングテーブルから動的ルートを削除する 1215
ONTAPネットワーク情報 1216
ONTAPネットワーク情報の表示 1216
ONTAPのネットワークポート情報の表示 1216
ONTAP VLAN情報の表示 1218
ONTAPインターフェイスグループ情報の表示 1219
ONTAP LIF情報の表示 1220
ONTAPネットワークのルーティング情報の表示 1223
ONTAP DNSホストテーブルエントリの表示 1225
ONTAP DNSドメイン設定情報の表示 1225
ONTAPフェイルオーバーグループの情報を表示します。 1226
ONTAP LIFのフェイルオーバーターゲットの表示 1227
ロードバランシングゾーンのONTAP LIFを表示する 1229
ONTAPクラスタ接続の表示 1230
ネットワークの問題を診断するためのONTAPコマンド 1236
近接探索プロトコルによるネットワーク接続の表示 1237

NASストレージの管理 1250
System Managerを使用したNASプロトコルの管理 1250
ONTAP System Managerを使用したNAS管理について学ぶ 1250
ONTAP System Manager を使用して VMware データストア用の NFS ストレージをプロビジョニングする 1250
ONTAP System Manager を使用してホームディレクトリ用の NAS ストレージをプロビジョニングする 1251
ONTAP System Manager で NFS を使用して Linux サーバー用の NAS ストレージをプロビジョニングする 1252
ONTAP System Manager でエクスポート ポリシーを使用してアクセスを管理する 1254
ONTAP System Manager で SMB を使用して Windows サーバー用の NAS ストレージをプロビジョニングする 1255
ONTAP System Manager で NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングします。 1257
ONTAP System Manager を使用して Kerberos でクライアント アクセスを保護する 1259
ONTAP System Managerを使用してネームサービスによるクライアントアクセスを提供する 1261
ONTAP System Managerでディレクトリとファイルを管理する 1262
ONTAP System Managerを使用してホスト固有のユーザーとグループを管理する 1262
ONTAP System ManagerでNFSアクティブクライアントを監視する 1265
NASストレージの有効化 1266
CLIを使用したNFSの設定 1270
ONTAP CLIを使用したNFS設定の詳細 1270
ONTAP NFS構成ワークフローについて学ぶ 1271
準備 1272
SVMへのNFSアクセスの設定 1285
NFS対応SVMにストレージ容量を追加する 1321
ONTAP NFSの追加情報はどこで入手できますか 1336
ONTAPエクスポートと7-Modeエクスポートの違い 1337
CLIを使用したNFSの管理 1341
NFSプロトコルのONTAPファイルアクセスについて学ぶ 1341
NASファイルアクセスについて理解する 1342
NASネームスペースでのデータボリュームの作成と管理 1350
セキュリティ形式の設定 1356
NFSを使用したファイルアクセスの設定 1361
NFSを使用したファイルアクセスの管理 1399
サポートされるNFSのバージョンとクライアント 1454
NFSトSMBノフアイルオヨヒテイレクトリノメイメイキソク 1458
NFSトランキングを管理します。 1464
ONTAP NFSトランキングの詳細 1464
トランキング用に新しいNFSサーバとエクスポートを設定する 1465
既存のNFSエクスポートをトランキングに適合させる 1470
RDMA経由のNFSを管理します。 1475

ONTAPでのRDMA経由のNFSの詳細 1475
NFS over RDMA用のNICの設定 1477
RDMA経由のNFS用のLIFの設定 1480
NFS設定を変更する 1482
CLIを使用したSMBの設定 1482
ONTAP CLIを使用したSMB設定の詳細 1482
ONTAP SMBの設定ワークフロー 1483
準備 1484
SVMへのSMBアクセスの設定 1495
共有ストレージへのSMBクライアントアクセスの設定 1518
CLIを使用したSMBの管理 1528
ONTAP SMBの詳細 1528
SMBサーバのサポート 1528
SMBサーバを管理します。 1535
SMBを使用したファイルアクセスのセットアップ 1633
SMBを使用したファイルアクセスの管理 1700
SMBクライアントベースのサービスを導入する 1794
SMBサーバベースのサービスの導入 1809
NFSトSMBノフアイルオヨヒテイレクトリノメイメイキソク 1879
NASデータへのS3クライアントアクセスの提供 1885
ONTAP S3 マルチプロトコルサポートについて学ぶ 1885
ONTAP S3クライアントアクセスのNASデータ要件について学ぶ 1888
ONTAP SVM上のNASデータへのS3プロトコルアクセスを有効にする 1889
ONTAP S3 NASバケットを作成する 1892
ONTAP S3クライアントユーザーを有効にする 1894
Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ 1897
Microsoft Hyper-VおよびSQL Server向けのSMBの設定の概要 1897
Microsoft Hyper-VおよびSQL Server over SMBソリューション用のONTAPの設定 1898
Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨン 1899
リモートVSSによる共有ベースのバックアップ 1903
Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピーオフロードの使用方法 1907
設定に関する要件と考慮事項 1908
SQL ServerおよびHyper-V over SMB構成に関する推奨事項 1916
Hyper-VまたはSQL Server over SMB構成の計画 1917
Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現する ONTAP構成の作成 1920
Hyper-VおよびSQL Server over SMB構成を管理します。 1934
統計を使用してHyper-VおよびSQL Server over SMBのアクティビティを監視する 1939
構成がノンストップオペレーションに対応していることを確認する 1942
SANストレージの管理 1959
SANの概念 1959

iSCSIを使用したSANプロビジョニング 1959
iSCSIサービスの管理 1960
FCを使用したSANプロビジョニング 1966
NVMeを使用したSANプロビジョニング 1968
SANホリユウム 1969
SANホスト側のスペース管理 1974
igroupについて 1975
igroupのイニシエータのWWPNとiSCSIノード名を指定する 1976
VMwareとMicrosoftのコピーオフロードによるストレージ仮想化 1976
SAN管理 1983
SANプロビジョニング 1983
NVMeプロビジョニング 1994
LUNの管理 2007
igroupとポートセットを管理します。 2021
iSCSIプロトコルを管理します。 2027
FCプロトコルを管理します。 2034
NVMeプロトコルを管理します。 2037
FCアダプタを搭載したシステムを管理する 2047
すべてのSANプロトコルのLIFを管理します。 2055
SANプロトコルのONTAPスペース割り当てを有効にする 2062
推奨されるボリュームとファイルまたはLUNの設定の組み合わせ 2064
SANのデータ保護 2070
SAN環境向けのONTAPデータ保護方法 2070
ONTAPスナップショットから単一のLUNをリストアする 2071
ONTAP Snapshotからのボリューム内のすべてのLUNのリストア 2072
ONTAP FlexClone LUNでデータを保護 2074
SAN環境でのSnapVaultバックアップの設定と使用 2075
ホストバックアップシステムをONTAPに接続するための推奨構成 2084
ホストバックアップシステムを使用してONTAPストレージシステム上のLUNを保護する 2084
SAN構成のリファレンス 2086
ONTAP SAN構成の詳細 2086
iSCSIコウセイ 2086
FCコウセイ 2089
FCoEコウセイ 2097
FCオヨヒFCoEソオニンク 2101
ONTAPシステムとNetApp以外のシステムに接続されたSANホストの要件 2104
MetroCluster環境でのSAN構成 2105
SANホストのマルチパスに対するONTAPのサポート 2107
構成の制限 2108
S3オブジェクトストレージの管理 2124
ONTAP 9でのS3サポートの詳細 2124

ONTAP S3設定の詳細 2124
FlexGroupボリュームを使用したONTAP S3アーキテクチャ 2125
ONTAP S3の主なユースケース 2127
計画 2127
ONTAPのバージョンとプラットフォームでS3オブジェクトストレージをサポート 2128
ONTAP S3でサポートされる操作 2129
ONTAP S3の相互運用性 2139
ONTAP で S3 を使用する検証済みのサードパーティ ソリューション 2141
設定 2142
S3の設定プロセスの概要 2142
SVMへのS3アクセスの設定 2147
S3対応SVMにストレージ容量を追加する 2162
アクセスポリシーステートメントの作成または変更 2179
S3オブジェクトストレージへのクライアントアクセスを有効にする 2194
ONTAP S3ストレージサービスレベル 2197
ONTAP S3バケット用のCross-Origin Resource Sharing（CORS）の設定 2198
SnapMirror S3でバケットを保護 2203
ONTAP SnapMirror S3の詳細 2203
リモートクラスタでのミラーとバックアップの保護 2207
ローカルクラスタでのミラーとバックアップの保護 2218
クラウドターゲットを使用したバックアップ保護 2229
ONTAP SnapMirror S3ポリシーを変更する 2238
SnapshotでS3データを保護 2239
ONTAP S3スナップショットの詳細 2239
ONTAP S3 Snapshotを作成する 2241
ONTAP S3 Snapshotの表示とリストア 2243
ONTAP S3 Snapshotの削除 2245
S3イベントの監査 2246
ONTAP S3イベントの監査について 2246
ONTAP S3監査の設定を計画する 2249
ONTAP S3監査の設定を作成して有効にする 2252
ONTAP S3の監査用のバケットを選択します。 2253
ONTAP S3の監査設定を変更する 2254
ONTAP S3監査の設定の表示 2255
認証とアクセス制御 2258
ニンシヨウトアクセスセイキヨノカイヨウ 2258
クライアント認証と許可 2258
カンリシヤニンシヨウトRBAC 2258
管理者認証とRBACの管理 2258
ONTAPでの管理者認証とRBACの詳細 2258
ONTAP管理者認証とRBACのワークフロー 2259

ONTAP管理者認証とRBACのセットアップのワークシート 2260
ログインアカウントの作成 2275
アクセス制御ロールを管理します。 2291
管理者アカウントの管理 2304
マルチ管理者認証の管理 2330
動的許可の管理 2363
OAuth 2.0を使用した認証と許可 2373
ONTAP OAuth 2.0実装の概要 2373
概念 2376
構成と導入 2392
リモートONTAPユーザーの SAML 認証を構成する 2400
SAML認証を有効にする 2400
SAML認証の無効化 2405
サードパーティのIdPを構成する 2406
SAMLの設定に関する問題のトラブルシューティング 2408
ONTAPでのOAuth 2.0またはSAML IdPグループの使用 2410
グループの識別方法 2410
名前付きのグループを管理します。 2411
UUIDを使用したグループの管理 2412
WebAuthn MFAを使用した認証と許可 2414
ONTAP System Managerユーザー向けのWebAuthn多要素認証について学ぶ 2414
ONTAP System Managerのユーザまたはグループに対してWebAuthn MFAを有効にする 2415
ONTAP System ManagerユーザのWebAuthn MFAを無効にする 2417
ONTAP WebAuthn MFA設定の表示とクレデンシャルの管理 2418
Webサービスを管理します。 2420
Webサービスの管理の概要 2420
ONTAP Webサービスへのアクセスを管理する 2421
ONTAPでWebプロトコルエンジンを管理します。 2423
WebプロトコルエンジンをONTAPコマンド 2424
ONTAP Webサービスへのアクセスを構成する 2425
WebサービスをONTAPコマンド 2426
ONTAPノード上のマウントポイントを管理するためのコマンド 2427
ONTAPでSSLを管理する 2427
ONTAP WebサービスにHSTSを使用する 2428
ONTAP Webサービスアクセスの問題のトラブルシューティング 2430
証明書を使用してリモートサーバのIDを確認する 2433
ONTAPの証明書を使用してリモート サーバーの ID を検証する方法について説明します。 2433
ONTAPのOCSPを使用してデジタル証明書が有効であることを確認する 2433
ONTAPで TLS ベースのアプリケーションのデフォルト証明書を表示する 2435
クラスタとKMIPサーバの相互認証 2436
ONTAPクラスタとKMIPサーバの相互認証の概要 2436

ONTAPでクラスタの証明書署名要求を生成する 2436
ONTAPクラスタ用のCA署名サーバ証明書をインストールする 2437
ONTAPのKMIPサーバ用のCA署名付きクライアント証明書をインストールする 2438
セキュリティとデータ暗号化 2440
自律型ランサムウェア対策 2440
ONTAP自律型ランサムウェア対策の詳細 2440
ONTAP自律型ランサムウェア対策のユースケースと考慮事項 2446
ONTAP自律型ランサムウェア対策を有効にする 2450
新しいボリュームでONTAP Autonomous Ransomware Protectionをデフォルトで有効にする 2453
ONTAP ARP/AIを有効にする 2456
AI（ARP / AI）でONTAP自律型ランサムウェア対策を更新 2457
学習期間後にONTAP ARPでアクティブモードに切り替える 2459
SANボリュームのONTAP ARP評価期間について学ぶ 2461
ONTAP Autonomous Ransomware Protectionを一時停止して、ワークロードイベントを分析対象から除外する 2463
ONTAP自律型ランサムウェア対策攻撃検出パラメータの管理 2466
ONTAP ARPによって検出された異常なアクティビティへの対応 2470
ランサムウェア攻撃後にONTAP ARPスナップショットからデータをリストア 2476
自動生成されたARPスナップショットの設定を調整する 2480
Vscanによるウィルス保護 2484
ONTAP Vscanを使用したウイルス対策設定について学ぶ 2484
NetAppアンチウイルスによる保護について 2484
Vscanサーバのインストールと設定 2491
スキャナプールを設定 2499
オンアクセススキャンの設定 2507
オンデマンドスキャンの設定 2512
ONTAP Vscan のオフボックスウイルス対策機能を設定するためのベストプラクティス 2517
SVM ONTAP Vscanでウイルススキャンを有効にする 2519
ONTAP Vscanでスキャンしたファイルのステータスをリセットする 2519
ONTAPを使用したVscanイベントログ情報の表示 2520
接続の問題の監視とトラブルシューティング 2521
SVMでのNASイベントの監査 2526
SMBプロトコルとNFSプロトコル両方のONTAPを使用したファイルアクセスの監査について 2526
監査の仕組み 2528
ONTAP監査の前提条件 2530
ONTAP監査レコードのステージングファイルのサイズ制限 2532
ONTAP監査イベントログでサポートされる形式について 2532
ONTAP監査イベントログの表示と処理 2533
カンサテキルSMBイヘント 2534
NFSファイルおよびディレクトリアクセスイベントのONTAP監査について 2540
ONTAP SVMでの監査の設定を計画する 2541

SVMでファイルとディレクトリの監査設定を作成します。 2548
ファイルおよびフォルダの監査ポリシーを設定する 2551
ファイルおよびディレクトリに適用されている監査ポリシーに関する情報を表示する 2555
監査できるCLI変更イベント 2562
監査設定を管理します。 2569
ONTAPの監査とステージングボリュームのスペースに関する問題のトラブルシューティング 2574
SVMでのファイルの監視と管理にFPolicyを使用する 2575
FPolicyについて 2576
FPolicy設定を計画する 2584
FPolicy設定の作成 2622
FPolicy設定を管理します。 2630
セキュリティトレースを使用したアクセスの確認 2639
ONTAP セキュリティ トレースの詳細 2639
ONTAP SVMでセキュリティトレースが監視するアクセスチェックの種類 2640
ONTAP SVM でセキュリティ トレースを作成する際の考慮事項 2640
セキュリティトレースの実行 2641
ONTAP セキュリティ トレースの結果を解釈する 2650
ONTAP SVMに関する追加情報の入手先 2651
System Managerによる暗号化の管理 2652
ソフトウェアベースの暗号化を使用して、 ONTAPクラスタに保存されたデータを暗号化します。 2652
自己暗号化ドライブを使用してONTAPクラスタに保存されたデータを暗号化します 2652
CLIを使用した暗号化の管理 2653
ONTAPの保存データの暗号化について学ぶ 2653
NetAppボリュームとアグリゲートの暗号化を構成する 2653
NetAppハードウェアベースの暗号化の設定 2691
NetApp暗号化の管理 2715
データ保護とディザスタリカバリ 2752
クラスタとSVMのピアリング 2752
ONTAPクラスタとSVMのピアリングの詳細 2752
クラスタとSVMのピアリングの準備 2752
クラスタ間LIFを設定 2756
ピア関係の設定 2769
ピア関係に対してONTAPクラスタピアリング暗号化を有効にする 2778
ピア関係からONTAPクラスタピアリング暗号化を削除する 2779
ローカルSnapshotを管理します。 2780
ローカルONTAPスナップショットの管理について 2780
ONTAPの長期保存スナップショットについて学ぶ 2781
カスタムSnapshotポリシーの設定 2781
Snapshotを手動で管理する 2785
Snapshotリザーブの管理 2788
スナップショットからファイルをリストア 2792

SnapMirrorボリュームのレプリケーション 2798
SnapMirrorボリュームレプリケーションの詳細 2799
SnapMirrorボリュームレプリケーションの設定 2827
SnapMirrorボリュームのレプリケーションを管理します。 2848
SnapMirror SVMレプリケーションを管理します。 2877
ONTAP SnapMirror SVMレプリケーションの詳細 2877
SVM設定のレプリケート 2885
SnapMirror SVM DRデスティネーションからのデータの提供 2899
SnapMirrorソースSVMを再アクティブ化する 2904
ONTAP SnapMirrorボリュームDR関係をSVM DR関係に変換する 2915
ONTAP SnapMirror SVMレプリケーション関係を削除する 2917
SnapMirrorルートボリュームのレプリケーションを管理します。 2918
ONTAP SnapMirrorルートボリュームレプリケーションの詳細 2918
ONTAP負荷共有ミラー関係を作成して初期化する 2919
ONTAP負荷共有ミラー関係を更新する 2920
ONTAP負荷共有ミラーの昇格 2921
クラウドへのバックアップ 2922
ONTAP SnapMirrorクラウドライセンスをインストールする 2922
ONTAP SnapMirrorを使用したデータのクラウドへのバックアップ 2923
NetApp Backup and Recoveryを使用してデータをバックアップする 2926
SnapLockテクノロジを使用したアーカイブとコンプライアンス 2930
ONTAP SnapLockについて学ぶ 2930
SnapLockの設定 2935
WORMファイルを管理します。 2950
ONTAP SnapLockボリュームを移動する 2967
ランサムウェア攻撃から保護するためにONTAPスナップショットをロックする 2968
整合グループ 2976
ONTAPコンシステンシーグループについて学ぶ 2976
ONTAP整合性グループの制限について学ぶ 2982
単一のONTAPコンシステンシーグループを構成する 2983
階層型ONTAPコンシステンシーグループを構成する 2989
ONTAPコンシステンシグループを保護する 2993
ONTAPコンシステンシグループのメンバーボリュームを変更する 3001
ONTAPコンシステンシグループのジオメトリを変更する 3007
ONTAP整合性グループのアプリケーションとコンポーネントのタグを変更する 3013
ONTAPコンシステンシーグループのクローンを作成する 3014
ONTAPコンシステンシーグループを削除する 3017
SnapMirrorアクティブ同期 3017
はじめに 3017
計画 3030
設定 3040

SnapMirrorアクティブ同期の管理とデータの保護 3083
トラブルシューティング 3101
MetroCluster および SnapMirror アクティブ同期用の ONTAP Mediator 3110
ONTAP Mediatorの詳細 3110
ONTAP Mediatorの新機能 3112
インストールまたはアップグレード 3117
ONTAPメディエーターの管理 3164
ONTAPメディエーター用のホストOSの保守 3194
ONTAP System Managerを使用したMetroCluster IPサイト管理について学習します 3198
テープバックアップを使用したデータ保護 3199
ONTAP FlexVolボリュームのテープバックアップについて学ぶ 3199
ONTAPテープ バックアップと復元のワークフロー 3199
ONTAP SMTapeおよびダンプバックアップエンジンの使用例 3200
テープドライブを管理します。 3201
テープ・ドライブについて 3207
ストレージシステム間でのデータ転送 3217
FlexVol用NDMP 3221
ONTAP FlexGroupボリュームでのNDMPサポートについて学ぶ 3244
ONTAP SnapLockボリュームを使用したNDMPについて学ぶ 3244
FlexVolのノードを対象としたNDMPモードを管理します。 3244
FlexVolのSVMを対象としたNDMPモードを管理します。 3246
FlexVolのダンプエンジンについて 3253
FlexVolのSMTapeエンジンについて 3265
FlexVolのテープバックアップおよびリストア処理を監視する 3270
FlexVolのテープバックアップおよびリストアに関するエラーメッセージ 3274
NDMP構成 3295
ONTAP NDMP構成の詳細 3295
ONTAP NDMP構成ワークフローについて学ぶ 3296
ONTAP NDMP構成を準備する 3296
ONTAP NDMPテープデバイスの接続を確認する 3299
ONTAP NDMPバックアップ操作のテープ予約を有効にする 3300
SVMを対象としたNDMPの設定 3301
ノードを対象としたNDMPの設定 3311
ONTAP NDMP構成用のバックアップアプリケーションを構成する 3317
NetApp ElementソフトウェアとONTAP間のレプリケーションの概要 3318
イベント、パフォーマンス、健全性の監視 3319
System Managerを使用したクラスタパフォーマンスの監視 3319
ONTAP System Managerを使用してクラスタのパフォーマンスを監視する 3319
ONTAP System Managerダッシュボードでクラスタを表示する方法について学習します 3319
ONTAP System Managerでホットボリュームやその他のオブジェクトを識別する 3321
ONTAP System ManagerでQoSを変更する 3321

ONTAP System Managerでリスクを監視する 3321
ONTAP System Managerの分析情報でシステムを最適化 3324
ONTAP System Managerでネイティブ FPolicyを設定する 3326
CLIを使用したクラスタパフォーマンスの監視と管理 3326
ONTAP Active IQ Unified Managerのパフォーマンス監視と管理について学ぶ 3326
パフォーマンスの監視 3327
ONTAP Active IQ Digital Advisorを使用してシステムパフォーマンスを表示します 3338
パフォーマンスの問題の管理 3338
ONTAP Unified Managerでクラスタのパフォーマンスを監視する 3366
ONTAP Data Infrastructure Insightsでクラスタのパフォーマンスを監視する 3366
すべてのリソースを監視、トラブルシューティング、最適化 3367
監査ロギング 3367
ONTAP監査ログ実装の詳細 3367
ONTAP監査ログの変更について 3368
ONTAP監査ログの内容を表示します。 3369
ONTAP監査GET要求設定を管理します。 3370
ONTAPクラスタ間監査を有効にする 3371
ONTAP監査ログのデスティネーションを管理します。 3372
AutoSupport 3375
AutoSupportの詳細 3375
計画 3389
設定 3396
AutoSupportを使用したファイルのアップロード 3399
トラブルシューティング 3401
健全性の監視 3408
ONTAPシステムの健常性監視の詳細 3408
ONTAPの健全性監視コンポーネントの詳細 3408
ONTAPのシステムヘルスアラートの対応について 3409
ONTAPシステムヘルスアラートのカスタマイズの詳細 3409
ONTAP AutoSupport健全性アラートのトリガーについて 3410
使用可能なONTAPクラスタヘルスモニタの詳細 3410
ONTAPシステムヘルスアラートの自動受信 3412
デグレードしたONTAPシステムヘルスへの対応 3412
デグレードしたONTAPシステムヘルスへの対応について 3413
ONTAPシステムのヘルスの監視用コマンド 3416
ONTAP環境情報の表示 3419
ファイルシステム分析 3419
ONTAPファイルシステム分析の詳細 3419
ONTAPファイルシステム分析を有効にする 3422
FSA を使用して ONTAP ファイルシステムのアクティビティを表示する 3425
FSA による ONTAP アクティビティ追跡の有効化 3426

FSA による ONTAP 使用状況分析の有効化 3428
FSAのONTAP分析に基づいて是正措置を講じる 3429
ONTAPファイルシステム分析によるロールベースアクセス制御 3431
ONTAPファイルシステム分析に関する考慮事項 3434
EMSノセツテイ 3435
ONTAP EMS構成の詳細 3435
System Managerを使用したONTAP EMSイベント通知とフィルタの設定 3435
CLIを使用したEMSイベント通知の設定 3439
廃止されたEMSイベントマッピングを更新する 3445
ONTAPコマンド リファレンス 3453
限定サポートバージョンのONTAPのコマンドリファレンス（PDFのみ） 3453
CLI比較ツール 3453
法的通知 3454
著作権 3454
商標 3454
特許 3454
プライバシーポリシー 3454
オープンソース 3454
ONTAP 3454
MetroCluster IP構成向けONTAPメディエーター 3454

ONTAP 9 ドキュメント

リリースノート

ONTAP 9リリースのハイライト

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

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

- 詳細はこちらをご覧ください "ONTAP MetroClusterの新機能と強化された機能"。
- 学ぶ "NetApp AFXストレージシステム向けの新しいONTAPソフトウェア機能と強化された機能" 。
- 学ぶ "NetApp ASA r2 ストレージ システム向けの新しい ONTAP ソフトウェア機能と強化されたONTAPソフトウェア機能" 。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート" 。
- の更新について説明します。 "ONTAP REST API"

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

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

ONTAP 9.17.1のハイライト

ONTAP 9.17.1 は、SAN 向けの AI を活用した自律型ランサムウェア保護の革新を実現し、 SnapMirrorアクティブ同期と整合性グループ階層管理による NVMe フロントエンド ホストのサポートを追加します。これらの機能強化により、データ セキュリティとサイバー レジリエンスにおける NetApp のリーダーシップが強化され、 ONTAP のパフォーマンス、スケーラビリティ、効率性、ビジネス継続性が向上します。新機能と拡張機能の完全なリストについては、こちらをご覧ください。 ONTAP 9.17.1の新機能 。

- 自律型ランサムウェア防御を備えたSANのサポート

  ARPは、暗号化ベースの異常検出機能を備えたSANボリュームをサポートし、詳細なエントロピー統計情報を提供する新しいコマンドを導入し、これまでNASに特化していたSystem Managerのランサムウェア対策メッセージを統合しました。設定可能な検出しきい値と、より決定論的なスナップショット保持により、多様なワークロードに柔軟に対応できます。

- HTTP Strict Transport Security (HSTS) のサポート

  ONTAP 9.17.1 は、Web サービスに対して HTTP Strict Transport Security をサポートし、ユーザーのブラウザとONTAP間の安全な HTTPS 通信を強制できるようになります。

- リンクアグリゲーショングループによるIPsecハードウェアオフロード

  ONTAP 9.17.1 は、リンク アグリゲーション グループの IPsec ハードウェア オフロードをサポートし、ONTAP 9.16.1 で導入されたハードウェア オフロード サポートを拡張します。

- IPsec 耐量子事前共有鍵サポート

  ONTAP は、将来の量子コンピュータ攻撃から保護するために、IPsec のポスト量子事前共有キーをサポートしています。

- OpenStack Barbican キーマネージャーのサポート

  ONTAP は、 NetApp Volume Encryption (NVE) キー用の OpenStack の Barbican キー マネージャーをサポートしています。

- ジャストインタイム (JIT) 権限昇格のサポート

  ONTAPは、ロールベースアクセス制御（RBAC）のためのJIT権限昇格をサポートしています。ユーザーは、設定されたロールへの一時的な昇格を要求し、オンデマンドで特権コマンドへのアクセスを許可できます。クラスタ管理者は、JIT権限昇格にアクセスできるユーザー、アクセスを許可するタイミング、およびアクセス期間を設定できます。

- SAML認証のためのEntra IdPとIdPグループのサポート

  ONTAPは、SAMLアイデンティティプロバイダーとしてMicrosoft Entraをサポートしています。さらに、IdPが提供するグループ情報をONTAPロールにマッピングできます。

- NVMe経由のホストアクセスのためのSnapMirrorアクティブ同期サポート

  SnapMirror Active Sync は、2ノードONTAPクラスタの NVMe/TCP および NVMe/FC ホストアクセスを使用した VMware ワークロードの NVMe アクセスをサポートします。VMware

- SnapMirror Active Sync によるONTAP Cloud Mediator のサポート

  ONTAP Cloud MediatorはONTAP 9.17.1で導入され、 SnapMirror Active Sync関係をサポートします。クラウドベースのMediatorは、 ONTAP Mediatorと同様に、 SnapMirror Active Sync関係のクォーラム監視として機能し、透過的なフェイルオーバーを実現するとともに、第3サイトの保守・管理に伴う運用上の複雑さを軽減します。

ONTAP 9 .16.1の特長

ONTAP 9 .16.1は、セキュリティ管理、データ保護、ネットワーク、SAN管理、ストレージ管理の分野で新機能と拡張機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.16.1の新機能。

- Multi-admin verification（MAV）の機能拡張

  MAVフレームワークには、悪意のある内部ユーザからの保護を強化するためのコマンドが追加されていますONTAP 9。これらの機能拡張には、多数の整合グループ（CG）、VscanとAutonomous Ransomware Protection（ARP）管理、NVMe設定コマンドなどがあります。

- AIの機能強化による自律型ランサムウェア対策（ARP / AI）

  ARPは、新しいAI機能でアップグレードされ、99%の精度でランサムウェア攻撃を検出して対応できるようになりました。AIは包括的なデータセットでトレーニングされるため、FlexVolボリュームでARPを実行するための学習期間がなくなり、ARP / AIがすぐにアクティブモードで開始されます。また、ARP/AIでは、ONTAPのアップグレードに依存しない自動更新機能も導入されているため、最新の脅威に対する継続的な保護と耐障害性が確保されます。

- NVMe/TCP over TLS 1.3

  シンプルな構成とIPSecよりも優れたパフォーマンスにより、プロトコルレイヤでNVMe/TCPを「ネットワークを介して」保護します。

- 新しいネットワークカードに対するIPSec HWオフロードのサポート

  ONTAP 9.16.1は、最新世代のAFF AシリーズおよびAFF Cシリーズシステムプラットフォームで導入されたオフロードカードでIPSecハードウェアオフロード機能を使用すると、より高い「ネットワーク上」の暗号化パフォーマンスを提供します。

- NVMeスペースの割り当て解除のサポート

  NVMeネームスペースで、スペース割り当て解除（「ホールパンチング」や「マッピング解除」とも呼ばれます）がサポートされるようになりました。スペースの割り当て解除は、ホスト アプリケーションによってデータが削除されたときに、シン プロビジョニングされたボリュームと NVMe 名前空間が未使用のスペースを再利用するのに役立ちます。これにより、全体的なストレージ効率が大幅に向上します。特に、データの書き換えが頻繁なファイルシステムには大きな効果があります。

- FlexGroupボリュームの高度な容量分散

  NetApp FlexGroupでは、必要に応じて、1つのファイル内のデータを複数のバックエンドコンスティチュエントボリュームにストライピングすることができます。これにより、パフォーマンスのボトルネックが軽減され、バックエンドコンスティチュエントボリューム間で容量を分散する際の一貫性が向上

- MetroCluster構成の移行におけるSVMデータ移動のサポート

  ONTAPでサポートされるMetroCluster SVMの移行は次のとおりです。

  - MetroCluster以外の構成とMetroCluster IP構成の間でのSVMの移行
  - 2つのMetroCluster IP構成間でのSVMの移行
  - MetroCluster FC構成とMetroCluster IP構成間でのSVMの移行

ONTAP 9 .15.1の特長

ONTAP 9 .15.1は、セキュリティ管理、データ保護、NASワークロードサポートの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.15.1の新機能。

- "新しいAFF Aシリーズシステムをサポート、AI向けに構築"

  ONTAP 9 .15.1は、AI / MLのトレーニングや推論などの次世代のビジネスワークロード向けに設計された、新しいハイパフォーマンスAFF A1K、AFF A90、AFF A70システムをサポートしています。この新しいクラスのシステムは、既存のAFF Aシリーズ製品の最大2倍のパフォーマンスを提供し、パフォーマンスを犠牲にすることなく、「常時稼働」の優れたストレージ効率を実現します。

- Windows バックアップ アプリケーションとサーバー上の Unix スタイルのシンボリック リンク

  ONTAP 9.15.1以降では、シンボリックリンクが指すデータではなくシンボリックリンク自体をバックアップするオプションも用意されています。これにより、バックアップアプリケーションのパフォーマンスの向上など、いくつかの利点が得られます。この機能は、ONTAP CLIまたはREST APIを使用して有効にできます。

- 動的許可

  ONTAP 9.15.1では、動的許可の初期フレームワークが導入されています。これは、管理者アカウントによるコマンドを拒否するかどうか、追加の認証を要求するかどうか、プロセスの続行を許可するかどうかを判断できるセキュリティ機能です。その判断は、時間帯、場所、IPアドレス、信頼されたデバイスの使用状況、ユーザの認証と許可の履歴などの要因を考慮しながら、ユーザ アカウントの信頼スコアに基づいて行われます。

- マルチ管理者認証の影響範囲の拡大

  悪意のある侵入者からの保護を強化するために、ONTAP 9.15.1 RC1では、MAVフレームワークに100個以上の新しいコマンドが追加されました。

- クラスタピアリングなどでのTLS 1.3暗号化のサポート

  ONTAP 9 .15.1では、S3ストレージ、FlexCache、SnapMirror、およびクラスタピアリングの暗号化でTLS 1.3暗号化がサポートされるようになりました。FabricPool、Microsoft Azureページブロブストレージ、SnapMirrorクラウドなどのアプリケーションでは、9.15.1リリースで引き続きTLS 1.2が使用されます。

- TLS経由のSMTPトラフィックのサポート

  TLSをサポートすることで、AutoSupportデータをEメールでセキュアに送信できます。

- 対称アクティブ / アクティブ構成のSnapMirrorアクティブ同期

  この新機能により、ビジネス継続性とディザスタ リカバリに対応した双方向同期レプリケーションが可能になります。複数の障害ドメインにわたるデータへの同時読み取り / 書き込みアクセスを使用して、重要なSANワークロードに対するデータ アクセスを保護します。これにより、災害やシステム障害の発生時にも運用の中断を回避し、ダウンタイムを最小限に抑えられます。

- FlexCacheライトバック

  FlexCacheライトバックにより、クライアントはFlexCacheボリュームにローカルに書き込むことができるため、元のボリュームに直接書き込む場合に比べてレイテンシが低減し、パフォーマンスが向上します。新しく書き込まれたデータは非同期で元のボリュームにレプリケートされます。

- NFSv3 over RDMA

  NFSv3 over RDMAのサポートにより、TCP経由で低レイテンシで広帯域幅のアクセスが提供され、ハイパフォーマンス要件に対応するのに役立ちます。

ONTAP 9.14.1のハイライト

ONTAP 9 .14.1は、FabricPool、ランサムウェア対策、OAuthなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.14.1の新機能。

- WAFL予約の削減

  ONTAP 9 .14.1では、30TB以上のアグリゲートのWAFLリザーブが削減されることで、FASシステムとCloud Volumes ONTAPシステムで使用可能スペースが5%増加しました。

- FabricPoolの機能拡張

FabricPoolを使用する読み取りパフォーマンスと、クラウドへの直接書き込みが可能になり、コールドデータを低コストのストレージ階層に移動することで、スペース不足のリスクが軽減され、ストレージコストが削減されます。

- "OAuth 2.0のサポート"

  ONTAPは、System Managerを使用して設定できるOAuth 2.0フレームワークをサポートしています。OAuth 2.0を使用すると、ユーザIDとパスワードをプレーン テキスト スクリプトやランブックに作成したり公開したりすることなく、自動化フレームワークのためのONTAPへのセキュアなアクセスを実現できます。

- "自律型ランサムウェア対策（ARP）の機能拡張"

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

- System ManagerでのSnapMirrorディザスタ リカバリのリハーサル

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

- S3オブジェクト ロックのサポート

  ONTAP S3ではobject-lock APIコマンドがサポートされています。このコマンドを使用すると、S3でONTAPに書き込まれたデータを標準のS3 APIコマンドを使用して削除から保護し、重要なデータを適切な期間にわたって保護できます。

- クラスタボリュームタグ付け

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

ONTAP 9 .13.1の特長

ONTAP 9 .13.1は、ランサムウェア対策、整合グループ、サービス品質（QoS）、テナント容量管理などの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してくださいいONTAP 9.13.1の新機能。

- Autonomous Ransomware Protection（ARP）の機能強化：
  - シトウユウコウカ

    ONTAP 9 .13.1では、十分な学習データが得られると、ARPは自動的にトレーニングモードから本番モードに移行します。これにより、管理者が30日間有効にする必要がなくなります。

  - マルチ管理者検証のサポート

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

  - FlexGroupのサポート

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

- System Managerでの整合グループのパフォーマンスと容量の監視

  パフォーマンスと容量を監視することで、整合グループごとの詳細な監視が可能になり、データ オブジェクト レベルにとどまらずアプリケーション レベルで、潜在的な問題をすばやく特定して報告できます。

- テナントの容量管理

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

- サービス品質の上限と下限

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

ONTAP 9.12.1のハイライト

ONTAP 9 12.1は、セキュリティ強化、保持、パフォーマンスなどの分野で新機能と拡張機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.12.1の新機能。

- Snapshotの改ざんを防止

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

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

- 自律型ランサムウェア対策（ARP）の機能拡張

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

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

- FPolicy

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

- セキュリティ強化：改ざん防止保持ロギング

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

ることはできません。

発生元に関係なく、すべての管理者操作のログと監査情報を取得することで、データに影響を与えるすべての操作が確実にキャプチャされます。システム監査ログが何らかの形で改ざんされると、アラートが生成され、管理者に変更が通知されます。

- セキュリティの強化：多要素認証の拡張

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

- ファイルとオブジェクトの二重性（マルチプロトコルアクセス）

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

- FlexGroupリバランシング

  FlexGroupコンスティチュエントの負荷がアンバランスになった場合は、FlexGroupを無停止でリバランシングし、CLI、REST API、およびSystem Managerから管理できます。最適なパフォーマンスを実現するには、FlexGroup内のコンスティチュエントメンバーに使用容量を均等に分散させる必要があります。

- ストレージ容量の拡張

  WAFLのスペースリザベーションが大幅に削減され、アグリゲートあたりの使用可能容量が最大40TiB増えました。

ONTAP 9.11.1のハイライト

ONTAP 9 .11.1は、セキュリティ、保持、パフォーマンスなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.11.1の新機能。

- マルチ管理者認証

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

- 自律型ランサムウェア対策の強化

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

- SnapLock Compliance for FlexGroupボリューム

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

- 非同期ディレクトリの削除

  ONTAP 9 .11.1では、ONTAPシステムのバックグラウンドでファイルが削除されるため、大規模なディレクトリを簡単に削除しながら、ホストI/Oへのパフォーマンスやレイテンシの影響を排除できます。

- S3の機能拡張

  ONTAPに追加されたAPIエンドポイントおよびバケット レベルのオブジェクト バージョン管理機能により、S3のオブジェクト データ管理機能が簡易化および拡張され、オブジェクトの複数のバージョンを同じバケットに格納できるようになりました。

- System Managerの機能拡張

  System Managerは、ストレージ リソースを最適化し、監査管理を強化するための高度な機能をサポートしています。今回の更新には、ストレージ アグリゲートの管理と設定の強化、システム分析のさらなる可視化、FASシステムのハードウェア可視化などが含まれます。

ONTAP 9.10.1のハイライト

ONTAP 9 .10.1は、セキュリティ強化、パフォーマンス分析、NVMeプロトコルのサポート、オブジェクトストレージのバックアップオプションに関する新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.10.1の新機能。

- 自律型ランサムウェア対策

  自律型ランサムウェア対策は、ボリュームのSnapshotを自動的に作成し、異常なアクティビティが検出されたときに管理者にアラートを送信することで、ランサムウェア攻撃を迅速に検出し、より迅速にリカバリすることができます。

- System Managerの機能拡張

  System Manager は、ディスク、シェルフ、サービス プロセッサのファームウェア アップデートを自動的にダウンロードするほか、 Active IQ Digital Advisor (Digital Advisorとも呼ばれます)、 NetApp Console、証明書管理との新しい統合も提供します。これらの機能拡張により、管理が簡易化され、ビジネスの継続性が維持されます。

- ファイルシステム分析の機能拡張

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

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

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

- NetApp FASシステムでのNVMe over Fibre Channel（NVMe / FC）のサポート

  ハイブリッド アレイでNVMe / FCプロトコルを使用することで、NVMeへの均等な移行を実現します。

- オブジェクト ストレージ向けのハイブリッド クラウド ネイティブ バックアップ

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

- FlexCacheによるグローバル ファイルロック

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

ONTAP 9.9.1のハイライト

ONTAP 9 .91.1は、ストレージ効率化、多要素認証、ディザスタリカバリなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してくださいONTAP 9.9.1の新機能。

- CLIによるリモートアクセス管理のセキュリティの強化

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

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

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

- SnapMirrorアクティブ同期

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

- SANのパフォーマンスの向上

  VMwareデータストアなどの単一のLUNアプリケーションのSANパフォーマンスが最大4倍に向上するため、SAN環境で高いパフォーマンスを実現できます。

- ハイブリッド クラウド向けの新しいオブジェクト ストレージのオプション

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

次のステップ

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

ONTAP 9.17.1の新機能

ONTAP 9.17.1で利用できる新機能について説明します。

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウン

トでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "NetApp AFXストレージシステム向けの新しいONTAPソフトウェア機能と強化された機能" 。
- 学ぶ "NetApp ASA r2 ストレージ システム向けの新しい ONTAP ソフトウェア機能と強化されたONTAPソフトウェア機能" 。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート" 。
- の更新について説明します。 "ONTAP REST API"

ONTAPを最新バージョンにアップグレードするには、を参照してください"ONTAPをアップグレードする準備"。

データ保護

更新	説明
NVMe経由のホストアクセスのためのSnapMirrorアクティブ同期サポート	SnapMirror Active Sync は、2ノードONTAPクラスタの NVMe/TCP および NVMe/FC ホストアクセスを使用した VMware ワークロードの NVMe アクセスをサポートします。VMwareワークロードの NVMe/TCP サポートは、VMware のバグが修正されることを条件とします。
SnapMirror Active Sync によるONTAP Cloud Mediator のサポート	ONTAP Cloud MediatorはONTAP 9.17.1で導入され、 SnapMirror Active Sync関係をサポートします。クラウドベースのMediatorは、 ONTAP Mediatorと同様に、 SnapMirror Active Sync関係のクォーラム監視として機能し、透過的なフェイルオーバーを実現するとともに、第3サイトの保守・管理に伴う運用上の複雑さを軽減します。

S3オブジェクトストレージ

更新	説明
ONTAP S3 NASバケットでのCopyObjectアクションのサポート	CopyObject アクションは、 ONTAP S3 NAS バケット内でサポートされます。
S3 NASバケットをジャンクションパスにリンクするためのサポート	ONTAP CLI を使用して S3 NAS バケットを作成する際、ジャンクションパスではなくボリュームにバケットをリンクすることを選択できます。ボリュームにリンクすると、ボリュームのマウントまたはアンマウントなど、パスが変更された場合にジャンクションパスが自動的に更新されます。
タグ付けとメタデータのための S3 マルチプロトコル サポート	タグ付けとユーザー メタデータのキー/値のペアは、マルチプロトコル (S3 および NAS) 環境の CreateMultipartUpload アクションによってサポートされます。

セキュリティ

更新	説明
HTTP Strict Transport Security (HSTS) のサポート	ONTAP は、Web サービスに対して HTTP Strict Transport Security をサポートしており、ユーザーのブラウザとONTAP間の安全な HTTPS 通信を強制できます。
リンクアグリゲーショングループによるIPsecハードウェアオフロード	ONTAP は、リンク アグリゲーション グループの IPsec ハードウェア オフロードをサポートし、9.16.1 で導入されたハードウェア オフロード サポートを拡張します。
IPsec 耐量子事前共有鍵サポート	ONTAP は、将来の量子コンピュータ攻撃から保護するために、IPsec のポスト量子事前共有キーをサポートしています。
OpenStack Barbican キーマネージャーのサポート	ONTAP は、 NetApp Volume Encryption (NVE) キー用の OpenStack の Barbican キー マネージャーをサポートしています。
ジャストインタイム (JIT) 権限昇格のサポート	ONTAPは、ロールベースアクセス制御（RBAC）のためのJIT権限昇格をサポートしています。ユーザーは、設定されたロールへの一時的な昇格を要求し、オンデマンドで特権コマンドへのアクセスを許可できます。クラスタ管理者は、JIT権限昇格にアクセスできるユーザー、アクセスを許可するタイミング、およびアクセス期間を設定できます。
SAML認証のためのEntra IdPとIdPグループのサポート	ONTAPは、SAMLアイデンティティプロバイダーとしてMicrosoft Entraをサポートしています。さらに、IdPが提供するグループ情報をONTAPロールにマッピングできます。
クラスタ間リクエストの監査	監査操作は、開始元のソースクラスタとデスティネーション（実行側）クラスタの両方で設定および実行できます。以前のリリースでは、クライアントからの要求を受信したクラスタのみが監査を実行していました。この機能により、クラスタ間の要求を処理するピアクラスタもアクティビティをログに記録できるようになります。これらの監査操作は有効化でき、ONTAP内で開始されるすべてのSET要求またはGET要求に拡張できます。
自律型ランサムウェア防御を備えたSANのサポート	ARPは、暗号化ベースの異常検出機能を備えたSANボリュームをサポートし、詳細なエントロピー統計情報を提供する新しいコマンドを導入し、これまでNASに特化していたSystem Managerのランサムウェア対策メッセージを統合しました。設定可能な検出しきい値と、より決定論的なスナップショット保持により、多様なワークロードに柔軟に対応できます。

ストレージリソース管理の機能拡張

更新	説明
新しいボリュームでは FSA がデフォルトで有効になっています	NASプロトコル用に割り当てられたONTAPクラスタ上の新規SVMに作成されたボリュームでは、ファイルシステム分析（FSA）がデフォルトで有効になっています。FSAはボリュームの作成と同時に自動的に有効化され、追加設定なしですぐに分析機能を利用できます。
FlexGroupボリュームの直接削除の進行状況を表示するためのサポートが強化されました	ONTAP CLIコマンド `volume file async-delete show`クライアントから発行された非同期削除ジョブを含めるように拡張されました。

ONTAP 9.16.1の新機能

ONTAP 9で利用できる新しい機能について説明します。16.1

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "NetApp ASA r2 ストレージ システム向けの新しい ONTAP ソフトウェア機能と強化されたONTAPソフトウェア機能" 。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート" 。
- の更新について説明します。 "ONTAP REST API"

ONTAPを最新バージョンにアップグレードするには、を参照してください"ONTAPをアップグレードする準備"。

データ保護

更新	説明
マルチノードでのSnapMirrorアクティブ同期のサポート	以前の2ノードの制限から拡張されたSnapMirror Active Syncでは、4ノードクラスタがサポートされるため、大規模なワークロードのデータレプリケーションが可能になります。
SnapMirrorクラウドでのファンアウト関係の作成のサポート	SnapMirror Cloudでは、同じソースボリュームまたはFlexGroupから2つの異なるオブジェクトストアへのファンアウト関係がサポートされます。ファンアウトには、2つのオブジェクトストアと、オブジェクトストア内の1つまたは2つのバケットを指定できます。

更新	説明
移行したボリュームからのSnapMirrorクラウドバックアップのサポート	SnapMirror Cloudは、既存のONTAP REST APIを使用してクラウドに移行されたボリュームのバックアップをサポートしています。新しい機能では、クラウドに移行されたボリュームから同じデスティネーションオブジェクトストアエンドポイントへのSnapMirrorクラウドバックアップがサポートされます。ベースラインの再処理を実行する必要はありません。FlexVolボリュームとFlexGroupボリュームの両方がサポートされます。

ネットワーク

更新	説明
BGPピアグループのMD5認証サポート	ONTAPはBGPピアグループでMD5認証をサポートして、BGPセッションを保護します。MD5がイネーブルの場合、BGPセッションは許可されたピア間でのみ確立および処理されるため、攻撃者がBGPアップデートをスプーフィングしてネットワークに誤ったルーティング情報を注入しようとするルートハイジャックなどの攻撃を防ぐことができます。
IPSecハードウェアオフロードのサポート	IPセキュリティ（IPsec）は、クライアントとONTAPノード間のすべてのIPトラフィックを保護するために使用できるデータインモーションセキュリティオプションです。このプロトコルは当初ONTAP 9 .8で利用可能であり、ソフトウェアとしてのみ実装されている。ONTAP 9 .16.1以降では、暗号化や整合性チェックなど、計算負荷の高い特定の処理を、ストレージノードに取り付けられたサポートされているネットワークインターフェイスコントローラ（NIC）カードにオフロードすることができます。このハードウェアオフロードオプションを使用すると、IPsecで保護されるネットワークトラフィックのパフォーマンスとスループットが大幅に向上します。

S3オブジェクトストレージ

更新	説明
マルチプロトコルS3バケットによるS3オブジェクトのメタデータとタグ付けのサポート	ONTAP 9.16.1以降では、S3オブジェクトのタグ付けが、非マルチプロトコルのONTAP S3バケットからNASおよびS3マルチプロトコルのONTAP S3バケットに拡張されました。タグはS3プロトコルでのみ表示されます。S3クライアントを使用してS3オブジェクトに適用する "タグとメタデータ" と、ONTAPにオブジェクトまたはファイルとして格納されているデータに対してライフサイクル、バックチャージ、データカテゴリ、カスタムワークフローを定義できます。BedrockやAthenaなどのAWSデータサービスと統合すると、タグ付けとメタデータは、これらのサービスが提供するData Processingの中心になります。 S3のネイティブバケットでのタグとユーザ定義メタデータのサポートは、ONTAP 9.9.1から開始されました。

更新	説明
マルチプロトコルS3バケットでのマルチパートアップロードのサポート	マルチパートアップロードはS3の中核的な機能で、マルチプロトコル以外のONTAP S3バケットでサポートされています。ONTAP 9.16.1以降では、このコア機能がNASおよびS3マルチプロトコルONTAP S3バケットに拡張されました。
ONTAP S3バケットでのCross-Origin Resource Sharing（CORS）のサポート	Cross-Origin Resource Sharing（CORS）を使用すると、Webアプリケーションの可能性を最大限に引き出すことができます。CORSを使用すると、あるドメインのクライアントアプリケーションと別のドメインのリソース間のシームレスな対話が可能になります。CORSサポートを統合することで、リソースへの選択的なクロスオリジンアクセスにより、ONTAP S3ベースのWebアプリケーションを強化できます。
ONTAPでは、ONTAP S3バケットのSnapshotの作成がサポートされます。	ONTAP S3バケットの読み取り専用のポイントインタイムSnapshotを生成できます。S3のSnapshot機能を使用すると、Snapshotを手動で作成することも、Snapshotポリシーを使用して自動的に生成することもできます。また、S3クライアントを使用して、S3 Snapshotを表示、参照、削除し、Snapshotのコンテンツをリストアすることもできます。

SAN

更新	説明
NVMeスペースの割り当て解除がデフォルトで有効	スペースの割り当て解除 (「ホール パンチング」や「アンマップ」とも呼ばれます) は、NVMe 名前空間に対してデフォルトで有効になっています。スペース割り当て解除機能により、ホストはネームスペースで使用されていないブロックの割り当てを解除してスペースを再利用できます。これにより、全体的なストレージ効率が大幅に向上します。特に、データの書き換えが頻繁なファイルシステムには大きな効果があります。

セキュリティ

更新	説明
マルチ管理者検証用に拡張されたルール保護されたコマンドセット	管理者は、複数の管理者による検証ルールを作成して整合グループを保護できます。これには、処理の作成、削除、変更、整合グループSnapshotの作成と削除、その他のコマンドが含まれます。

更新	説明
AIの機能強化による自律型ランサムウェア対策（ARP / AI）	ARPは、新しいAI機能でアップグレードされ、99%の精度でランサムウェア攻撃を検出して対応できるようになりました。AIは包括的なデータセットでトレーニングされるため、FlexVolボリュームでARPを実行するための学習期間がなくなり、ARP / AIがすぐにアクティブモードで開始されます。ARP/AIには、最新の脅威に対する継続的な保護と耐障害性を確保するための自動更新機能も搭載されています。 現在、ARP/AI機能はNASのみをサポートしています。自動更新機能では、System Managerへの導入に使用できる新しいセキュリティファイルが表示されますが、これらの更新プログラムはNASワークロードの保護にのみ適用されます。
NVMe/TCP over TLS 1.3	シンプルな構成とIPSecよりも優れたパフォーマンスにより、プロトコルレイヤでNVMe/TCPを「ネットワークを介して」保護します。
FabricPoolオブジェクトストアの通信でのTLS 1.3のサポート	ONTAPでは、FabricPoolオブジェクトストアの通信でTLS 1.3がサポートされます。
Microsoft Entra ID用OAuth 2.0	ONTAP 9 14.1で導入されたOAuth 2.0のサポートは、標準のOAuth 2.0要求を持つMicrosoft Entra ID認証サーバー(旧Azure AD)をサポートするように拡張されました。さらに、UUIDスタイル値に基づくEntra ID標準グループ要求は、新しいグループおよびロールマッピング機能によってサポートされています。新しい外部ロールマッピング機能も導入されました。これはEntra IDでテストされていますが、サポートされている任意の認証サーバで使用できます。

Storage Efficiency

更新	説明
qtreeのパフォーマンス監視機能を拡張し、レイテンシの指標と履歴統計を追加	以前のONTAPリリースでは、読み取りや書き込みなどのいくつかのカテゴリで、1秒あたりのI/O処理数やスループットなど、qtreeの使用状況を堅牢なリアルタイム指標で表示できます。ONTAP 9 .16.1以降では、リアルタイムのレイテンシ統計にアクセスしたり、アーカイブされた履歴データを表示したりすることもできます。これらの新機能により、ITストレージ管理者はシステムのパフォーマンスをより詳細に把握し、長期間にわたる傾向を分析できます。これにより、データセンターおよびクラウドストレージリソースの運用と計画に関して、より多くの情報に基づいてデータ主体の意思決定を下すことができます。

ストレージリソース管理の機能拡張

更新	説明
ストレージ制限が有効なSVMでのデータ保護ボリュームのサポート	ストレージ制限が有効になっているSVMにはデータ保護ボリュームを含めることができます。カスケードを使用しない非同期ディザスタリカバリ関係のFlexVol、同期ディザスタリカバリ関係、およびリストア関係がサポートされます。 ONTAP 9.15.1以前のリリースでは、データ保護ボリュームを含むSVM、SnapMirror関係にあるボリューム、またはMetroCluster構成にストレージ制限を設定することはできません。
FlexGroupの高度な容量分散のサポート	高度な容量分散機能を有効にすると、大容量ファイルが拡張されて1つのメンバーボリュームのスペースが消費された場合に、ファイル内のデータがFlexGroupメンバーボリューム間で分散されます。
MetroCluster構成の移行におけるSVMデータ移動のサポート	ONTAPでサポートされるMetroCluster SVMの移行は次のとおりです。 • MetroCluster以外の構成とMetroCluster IP構成の間でのSVMの移行 • 2つのMetroCluster IP構成間でのSVMの移行 • MetroCluster FC構成からMetroCluster IP構成へのSVMの移行

System Manager

更新	説明
System ManagerでのフィッシングWebAuthn多要素認証のサポート	ONTAP 9 .16.1ではWebAuthn MFAログインがサポートされているため、ハードウェアセキュリティキーを2つ目の認証方法として使用できます。

ONTAP 9.15.1の新機能

ONTAP 9で利用できる新しい機能について説明します。15.1

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート"。
- の更新について説明します。 "ONTAP REST API"

ONTAPを最新バージョンにアップグレードするには、を参照してください"ONTAPをアップグレードする準備"。

データ保護

更新	説明
Windows バックアップ アプリケーションとサーバー上の Unix スタイルのシンボリックリンク	WindowsバックアップアプリケーションでUNIX形式のシンボリックリンク（symlink）が検出されると、リンクがたどり、ONTAPから実際のデータが返されてバックアップされます。ONTAP 9.15.1以降では、シンボリックリンクが指すデータではなくシンボリックリンク自体をバックアップするオプションも用意されています。これにより、バックアップアプリケーションのパフォーマンスの向上など、いくつかの利点が得られます。この機能は、ONTAP CLIまたはREST APIを使用して有効にできます。
SnapMirror Active Syncは対称アクティブ/アクティブ構成をサポート	SnapMirrorアクティブ同期（旧SnapMirrorビジネス継続性）では、対称アクティブ/アクティブ構成がサポートされるようになりました。これにより、保護されたLUNの両方のコピーからの読み取りおよび書き込みI/O処理が可能になり、双方向の同期レプリケーションが可能になります。
SnapMirror非同期を使用した整合性グループ内のボリューム数の増加	SnapMirror非同期保護を使用する整合グループでは、整合グループ内で最大80個のボリュームがサポートされるようになりました。
整合グループを使用したREST APIおよびCLI処理の管理者権限レベルのサポート	整合グループに対するCLI処理とREST API処理が管理者権限レベルでサポートされるようになりました。
Windows Serverフェイルオーバークラスタリングを使用したVMware仮想ボリュームの永続的予約	ONTAPは現在、VMwareのVirtual Volume（VVOL）と従来のLUNでの永続的予約をサポートしています。ONTAP 9 .15.1以降では、VVOLを使用して永続的予約を作成することもできます。この機能のサポートは、ONTAP Tools for VMware vSphere 9で実装されています。クラスタ化されたWindows仮想マシンのグループであるWindows Server Failover Cluster（WSFC）でのみサポートされます。

セキュリティ

更新	説明
FPolicy永続的ストアの作成と設定の簡易化	コマンドを使用すると、FPolicy永続ストアを作成し、ボリュームの作成と設定を同時に自動化できます `persistent-store create`。 この拡張 `persistent-store create`コマンドでは、autosize-modeパラメータを使用することもできます。autosize-modeパラメータを使用すると、使用済みスペースの量に応じてボリュームのサイズを拡張または縮小できます。
RDMAニヨルNFSv3ノサホオト	NFS over RDMA構成でNFSv3がサポートされるようになりました。
FPolicyでのNFS 4.1プロトコルのサポート	FPolicyでNFS 4.1プロトコルがサポートされるようになりました。

更新	説明
FPolicyでのProtobufエンジン形式のサポート	Protobufは、Googleが開発した言語に依存しないメカニズムで、構造化データをシリアル化するために使用されます。XMLに比べてサイズが小さく、高速で、シンプルなので、FPolicyのパフォーマンスが向上します。 Protobuf外部エンジン形式を使用できます。Protobufに設定すると、通知メッセージがGoogle Protobufを使用してバイナリ形式でエンコードされます。外部エンジン形式をProtobufに設定する前に、FPolicyサーバでもProtobuf逆シリアル化がサポートされていることを確認してください。
SSH接続の動的許可	ONTAP 9.15.1には、動的許可の初期フレームワークが搭載されています。動的許可では、管理ユーザにセキュリティ信頼スコアを割り当て、管理ユーザが不審な操作を行った際に追加の許可チェックを要求できるので、ONTAPシステム管理のセキュリティが強化されます。動的許可は、Data-Centricなゼロトラスト セキュリティ アーキテクチャの一部として活用できます。
S3ストレージ、FlexCache、クラスタ ピアリング暗号化でTLS 1.3をサポート	ONTAP 9 1.3は管理アクセス用にTLS .11.1以降でサポートされていますが、S3ストレージ、FlexCache、およびクラスタピアリングの暗号化でONTAP 9 .15.1でサポートされるようになりました。FabricPool、Microsoft Azureページブロブストレージ、SnapMirrorクラウドなどの一部のアプリケーションでは、9.15.1リリースで引き続きTLS 1.2が使用されます。
マルチ管理者検証用に拡張されたルール保護されたコマンドセット	管理者は、マルチ管理者検証ルールを作成して、クラスタ構成、LUN削除、システム構成、IPsecおよびSAMLのセキュリティ構成、ボリュームSnapshot処理、vServer構成、およびその他のコマンドを保護できます。
SMTPとTLSを使用したAutoSupportメッセージの配信	NetAppへのAutoSupportメッセージの転送にはHTTPSが推奨されますが、暗号化されていないSMTPも使用できます。ONTAP 9 .15.1では、SMTPでTLSを使用できるようになりました。SMTPSプロトコルは、Eメールトラフィックとオプションのメールサーバクレデンシャルを暗号化することで、セキュアな転送チャネルを確立します。明示的なTLSが使用されるため、TCP接続の作成後にTLSがアクティブになります。メッセージのコピーがローカルメールアドレスに送信される場合は、同じ設定が使用されます。

Storage Efficiency

更新	説明
ボリュームスペース指標のレポートに対する変更	使用中のメタデータのみを表示する2つの新しいカウンタが導入されました。また、既存のカウンタのいくつかが調整され、メタデータが削除されてユーザデータのみが表示されるようになりました。これらの変更を組み合わせることで、2種類のデータに分けられたメトリックがより明確に表示されます。お客様はこれらのカウンタを使用して、実際のユーザデータのみを考慮してメタデータを合計から割り引いて、より正確なチャージバックモデルを実装できます。

更新	説明
CPUまたは専用オフロードプロセッサによるStorage Efficiency	ONTAPは、AFF A70、AFF A90、AFF A1Kの各プラットフォームでストレージ効率化とデータコンパクションを実現します。プラットフォームに応じて、圧縮はメインCPUまたは専用のオフロードプロセッサを使用して実行されます。Storage Efficiencyは自動的に有効になるため、設定は必要ありません。

ストレージリソース管理の機能拡張

更新	説明
FlexCacheライトバックのサポート	キャッシュボリュームでライトバックが有効な場合、書き込み要求は元のボリュームではなくローカルキャッシュに送信されるため、エッジコンピューティング環境や書き込み負荷の高いワークロードのキャッシュのパフォーマンスが向上します。
ファイルシステム分析のパフォーマンスの強化	ONTAPでは、ボリュームの容量に5～8%の空きがないと、ファイルシステム分析を有効にできません。これにより、ボリュームやファイルシステム分析に関する潜在的なパフォーマンスの問題が軽減されます。
FlexCloneボリュームの暗号化キー	FlexCloneボリュームには、FlexVolボリューム（ホスト）の暗号化キーとは関係のない専用の暗号化キーが割り当てられます。

System Manager

更新	説明
System ManagerでのSnapLockバックアップ関係の設定のサポート	SnapLockバックアップ関係は、ソースとデスティネーションの両方でONTAP 9 .15.1以降を実行している場合、System Managerを使用して設定できます。
System Managerダッシュボードのパフォーマンスの強化	System Managerダッシュボードの[Health]、[Capacity]、[Network]、[Performance]の各ビューの情報には、レイテンシやパフォーマンスの問題の特定とトラブルシューティングに役立つパフォーマンス指標の強化など、より詳細な説明が表示されます。

アップグレード

更新	説明
自動無停止アップグレード時におけるHAパートナーノードへのLIFの移行のサポート	自動無停止アップグレードの実行中に他のバッチグループへのLIFの移行が失敗した場合、LIFは同じバッチグループ内のHAパートナーノードに移行されます。

ONTAP 9.14.1の新機能

ONTAP 9 14.1の新機能について説明します。

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート"。
- の更新について説明します。 "ONTAP REST API"

ONTAPを最新バージョンにアップグレードするには、を参照してくださいONTAPをアップグレードする準備。

データ保護

更新	説明
SVMルートボリュームでNVEをサポート	SVMルートボリュームは、NetAppボリューム暗号化による一意のキーを使用して暗号化できます。
長期保持スナップショットに対してスナップショットロックを設定する機能およびコンプライアンスクロックを再初期化するには	SnapLockライセンスがあるクラスタでは、SnapLock SnapMirror以外のデスティネーションボリュームで作成されたSnapshotに対して、長期保持のSnapshotの改ざん防止Snapshotロックを設定できます。また、SnapLockボリュームが存在しない場合はコンプライアンスクロックを初期化できます。
SnapMirror Active SyncはSCIS3永続的予約とWindowsフェイルオーバークラスタリングをサポート	SCSI3永続予約とSnapMirrorアクティブ同期用のウィンドウフェイルオーバークラスタリングは、デバイスにアクセスする複数のノードを同時に他のノードへのアクセスをブロックすることで、異なるアプリケーション環境のクラスタリングの一貫性と安定性を確保します。
整合グループを使用してボリューム単位のSnapshotをコピー	整合性グループを使用して非同期SnapMirror Snapshotやボリューム単位のSnapshotをデスティネーション整合性グループにレプリケートすることで、ディザスタリカバリをさらに強化できます。
SVMディザスタリカバリ関係での非同期データ保護の整合性グループのサポート	SVMディザスタリカバリ用に設定されたSVMでは、SVMに整合グループが含まれている場合、整合グループの情報をセカンダリサイトにレプリケートできます。
"20個のファンアウトターゲットに対するSnapMirror非同期のサポート"	ONTAP 9 14.1を使用すると、A700以降のシステムでサポートされるSnapMirror非同期ファンアウトターゲットの数が16から20に増加します。
暗号化されたソースからの非暗号化キャッシュの作成	ONTAP 9.14.0以降では、FlexCacheで暗号化されたソースから暗号化されていないFlexCacheボリュームを作成できます。以前のバージョンのONTAPでは、キャッシュのソースが暗号化されているとFlexCacheの作成に失敗しました。
整合グループのCLIサポート	ONTAP CLIを使用して整合グループを管理します。

ファイル アクセス プロトコル

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

S3オブジェクトストレージ

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

SAN

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

セキュリティ

更新	説明
SSHユーザに対するCisco Duo多要素認証のサポート	SSHユーザは、サインイン時の2番目の認証要素としてCisco Duoを使用して認証できます。
"OAuth 2.0サポートの強化"	ONTAP 9.14.1では、ONTAP 9.14.0から提供されていた標準的なトークンベースの認証とOAuth 2.0のサポートが拡張されます。Active DirectoryまたはLDAPに、グループとロールのマッピングを組み合わせて許可を設定できます。送信者限定アクセス トークンもサポートされ、相互TLS（mTLS）に基づいてセキュリティが確保されます。Auth0とKeycloakに加えて、Microsoft Windows Active Directory Federation Service（ADFS）がアイデンティティ プロバイダ（IdP）としてサポートされます。
"OAuth 2.0許可フレームワーク"	Open Authorization（OAuth 2.0）フレームワークが追加され、ONTAP REST APIクライアントのトークンベース認証が可能になります。これにより、REST APIスクリプトやAnsibleを実装した自動化ワークフローを使用して、ONTAPクラスタをよりセキュアに管理できます。発行者、オーディエンス、ローカル検証、リモート イントロスペクション、Remote user claim、プロキシのサポートなど、OAuth 2.0の標準機能がサポートされます。クライアント許可は、自己完結型OAuth 2.0スコープを使用するか、ローカルのONTAPユーザをマッピングすることで設定できます。サポートされるアイデンティティ プロバイダ（IdP）には、複数の並行サーバを使用するAuth0とKeycloakが含まれます。
調整可能な自律型ランサムウェア対策アラート	新しいファイル拡張子が検出されたとき、またはARPスナップショットが作成されたときに通知を受信し、ランサムウェアイベントの可能性に関する事前の警告を受け取るように、Autonomous Ransomware Protectionを設定します。
レイテンシ低減のためにFPolicyで永続的ストアをサポート	FPolicyを使用して永続的ストアを作成し、SVM内の非同期で必須でないポリシーのファイル アクセス イベントをキャプチャできます。永続的ストアは、クライアントI/O処理をFPolicy通知処理から分離して、クライアントのレイテンシを低減するのに役立ちます。同期および非同期で必須の設定はサポートされていません。
SMBを使用するFlexCacheボリュームでFPolicyをサポート	NFSかSMBを使用するFlexCacheボリュームでFPolicyがサポートされます。前のバージョンでは、SMBを使用するFlexCacheでFPolicyはサポートされていませんでした。

Storage Efficiency

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

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

ストレージリソース管理の機能拡張

更新	説明
プロアクティブなFlexGroupリバランシング	FlexGroupボリュームで、ディレクトリ内の増大中のファイルをリモートのコンスティチュエントへ自動的に移動し、ローカルのコンスティチュエント上のI/Oボトルネックを軽減する機能がサポートされました。
FlexGroupボリュームでのSnapshotタギング	でタグやラベル（コメント）を追加、変更、削除することで、Snapshotを識別したり、FlexGroupボリューム内のSnapshotが誤って削除されたりしないようにすることができます。
FabricPoolでのクラウドへの直接書き込み	FabricPoolに、FabricPool内のボリュームにデータを書き込む機能が追加されました。これにより、階層化スキャンを待たずにデータを直接クラウドに移動できます。
FabricPoolでのアグレッシブ先読み	FabricPool は、FabricPool がサポートするすべてのプラットフォームのボリューム上のファイルの積極的な先読み機能を提供します。

SVM管理の機能拡張

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

System Manager

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

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

ONTAP 9.13.1の新機能

ONTAP 9で利用できる新しい機能について説明します。13.1

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート"。
- の更新について説明します。 "ONTAP REST API"

ONTAPのアップグレードについては、を参照してくださいONTAPをアップグレードする準備。

データ保護

更新	説明
"マルチ管理者認証"	クラスタ管理者は、クラスタでマルチ管理者検証を明示的に有効にして、一部のSnapLock処理を実行する前にクォーラムの承認が必要になるようにすることができます。

更新	説明
"ボリュームの移動やジオメトリなど、整合性グループの管理のサポートが強化されました。"	整合グループ間でボリュームを移動したり、階層整合グループのジオメトリを変更したり、整合グループの容量に関する分析情報を取得したりできます。System Managerでは、新しいNASボリュームまたはNVMeネームスペースを使用して整合グループを作成できます。
"SnapMirror Synchronousを使用したNDMPのリストア"	SnapMirror Synchronousでは、NDMPのリストアがサポートされます。
SnapMirrorアクティブ同期の強化	• "SnapMirrorのアクティブな同期関係が確立された整合性グループに、システムを停止することなくボリュームを追加します。" • "SnapMirror Active SyncでNDMPリストアを使用する"です。
"単一の整合グループでの非同期SnapMirrorのサポート"	整合グループでは非同期SnapMirror構成がサポートされるため、単一の整合グループのSnapMirrorバックアップを作成できます。

ファイル アクセス プロトコル

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

ネットワーク

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

S3オブジェクトストレージ

更新	説明
S3バケットのライフサイクル管理	S3オブジェクトの有効期限操作により、バケット内のオブジェクトが期限切れになるタイミングを定義します。この機能を使用するとオブジェクトバージョンを管理できるため、保持要件を満たしたり、S3オブジェクト ストレージ全体を効率的に管理したりできます。

SAN

更新	説明
AIXホストでのNVMe/FCのサポート	ONTAPでは、AIXホストでNVMe/FCプロトコルがサポートされます。サポートされる構成については、を参照してください"NetApp相互運用性ツール"。

セキュリティ

機能	説明
自律型ランサムウェア対策	• 自律型ランサムウェア対策による複数管理者による検証機能 • 学習モードからアクティブモードへの自動移行 • FlexGroupのサポートこれには、FlexGroupボリュームの拡張、FlexVolからFlexGroupへの変換、FlexGroupのリバランシングなどのFlexGroupボリュームおよび処理の分析とレポートが含まれます。
Active Directoryを使用したSSH公開鍵認証	Active Directory（AD）ユーザの第1の認証方式としてSSH公開鍵を使用することも、ADユーザのあとに第2の認証方式としてSSH公開鍵を使用することもできます。
SSH公開鍵を使用したX.509証明書	ONTAPでは、X.509証明書をアカウントのSSH公開鍵に関連付けることができます。これにより、SSHログイン時の証明書の有効期限切れや失効のチェックのセキュリティが強化されます。
FPolicyファイル アクセス失敗通知	FPolicyは、アクセス拒否イベントの通知をサポートしています。権限がないためにファイル操作が失敗した場合（NTFS権限による失敗、UNIXモードビットによる失敗、NFSv4 ACLによる失敗など）、通知が生成されます。
TOTP（Time-based One-Time Password）を使用した多要素認証	TOTP（Time-based One-Time Password）を使用して多要素認証を行うローカル ユーザ アカウントをセットアップします。TOTPは常に2番目の認証方式として使用されます。第1の認証方法として、SSH公開鍵またはユーザパスワードを使用できます。

Storage Efficiency

更新	説明
System Managerでのプライマリデータ削減比率に関するレポートの変更	System Managerに表示されるプライマリデータ削減率の計算に、Snapshotによるスペース削減率は含まれなくなりました。使用済み論理スペースと使用済み物理スペースの比率のみが表示されます。ONTAPの以前のリリースでは、プライマリデータ削減率に、Snapshotによるスペース削減のメリットが大幅に含まれていました。そのため、ONTAP 9.13.1にアップグレードすると、報告されるプライマリ比率が大幅に低くなります。スナップショットを使用したデータ削減率は、引き続き**Capacity**の詳細ビューで確認できます。

更新	説明
温度に基づくストレージ効率	温度に基づくストレージ効率化では、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率が向上します。システムをONTAP 9にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでは、シーケンシャルパッキングが自動的に有効になります。13.1.
ロンリスヘエスノテキヨウ	論理スペースの適用はSnapMirrorデスティネーションでサポートされます。
Storage VM容量制限のサポート	Storage VM（SVM）に容量制限を設定し、SVMがしきい値に近づいたときにアラートを有効にすることができます。

ストレージリソース管理の機能拡張

更新	説明
inodeの最大数の増加	ボリュームのサイズが680GBを超えても、ONTAPでは引き続き自動的にinodeが追加されます（ボリューム スペース32KBあたり1 inodeの割合で追加）。ONTAP は、最大値 2,040,109,451 に達するまで inode を追加し続けます。
FlexClone作成時のSnapLockタイプの指定のサポート	読み取り / 書き込みボリュームのFlexCloneを作成するときに、3つのSnapLockタイプ（Compliance、Enterprise、またはNon-SnapLock）のいずれかを指定できます。
ファイルシステム分析のデフォルトでの有効化	新しいボリュームでファイルシステム分析をデフォルトで有効にするように設定します。
FlexGroupボリュームとのSVMディザスタ リカバリ ファンアウト関係	FlexGroupを備えたSVM DRのファンアウトの制限は削除されました。FlexGroupを使用したSVM DRでは、8サイトへのSnapMirrorファンアウト関係がサポートされます。
単一のFlexGroupリバランシング処理	単一のFlexGroupリバランシング処理を、指定した日時に開始するようにスケジュールを設定できます。
FabricPoolの読み取りパフォーマンス	FabricPoolは、クラウド上のデータに対する、シングルおよびマルチストリーム ワークロード用のシーケンシャル読み取りのパフォーマンスと、階層化のスループットを向上させます。この向上により、バックエンドのオブジェクト ストアへのGETおよびPUTの送信を高速化できます。オンプレミスのオブジェクト ストアがある場合は、オブジェクト ストア サービスのパフォーマンス ヘッドルームを考慮し、FabricPoolのPUTを調整すべきかどうかを判断する必要があります。
アダプティブQoSポリシー テンプレート	アダプティブQoSポリシー テンプレートを使用すると、スループットの下限をSVMレベルで設定できます。

SVM管理の機能拡張

更新	説明
SVMのデータ移動	最大200個のボリュームを含むSVMの移行のサポートが強化されます。

System Manager

ONTAP 9.12.1 以降、System Manager はNetAppコンソールと統合されています。詳細はこちらSystem Manager とNetAppコンソールの統合 。

更新	説明
レポート作成時のプライマリデータ削減比率の変更	System Managerに表示されるプライマリデータ削減率の計算に、Snapshotによるスペース削減率は含まれなくなりました。使用済み論理スペースと使用済み物理スペースの比率のみが表示されます。ONTAPの以前のリリースでは、プライマリデータ削減率に、Snapshotによるスペース削減のメリットが大幅に含まれていました。そのため、ONTAP 9.13.1にアップグレードすると、報告されるプライマリ比率が大幅に低くなります。Snapshotのデータ削減率は、引き続き容量の詳細ビューで確認できます。
改ざん防止スナップショットロック	System Managerを使用してSnapLock以外のボリューム上のSnapshotをロックし、ランサムウェア攻撃から保護することができます。
外部キー管理ツールのサポート	System Managerを使用して外部キー管理ツールを管理し、認証キーと暗号化キーを保存、管理できます。
ハードウェアの問題のトラブルシューティング	System Managerユーザは、[Hardware]ページで、ASAプラットフォームやAFF Cシリーズ プラットフォームなどの追加のハードウェア プラットフォームを可視化できます。AFF Cシリーズ プラットフォームは、最新パッチ リリースのONTAP 9.12.1、ONTAP 9.11.1、およびONTAP 9.10.1でもサポートされます。この可視化によってプラットフォームの問題や懸念事項が明らかになり、ユーザがハードウェアの問題を迅速にトラブルシューティングできます。

ONTAP 9.12.1の新機能

ONTAP 9で利用できる新しい機能について説明します。12.1

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート" 。
- の更新について説明します。 "ONTAP REST API"

ONTAPのアップグレードについては、を参照してくださいONTAPをアップグレードする準備。

データ保護

更新	説明
SnapMirror Synchronousによる大容量FlexVolのサポート	SnapMirror Synchronous構成でサポートされるFlexVolの最大サイズが100TBから300TBに拡張されました。ソースクラスタとデスティネーションクラスタの両方で_ ONTAP 9.12.1P2以降_が実行されている必要があります。
SnapMirror Synchronousでのファイルサイズ とLUNサイズの拡張のサポート	SnapMirror Synchronous構成でサポートされるファイルとLUNの最大サイズが16TBから128TBに拡張されました。ソース クラスタとデスティネーション クラスタの両方でONTAP 9.12.1P2以降が実行されている必要があります。
整合グループのサポートの強化	• 整合性グループへのボリュームの追加と削除、整合性グループのクローニング（Snapshotからのクローニングを含む）を実行できます。 • 整合グループではアプリケーションのタグ付けがサポートされるため、データの保護と管理のプロセスを合理化できます • ONTAP REST APIでは、NFS / SMBボリュームまたはNVMeネームスペースを使用した整合グループの設定がサポートされます
SnapMirror Synchronous NDO	SnapMirror Synchronousで、HAのテイクオーバーとギブバック、ボリューム移動、その他のメンテナンス関連処理からなるノンストップ オペレーション（NDO）がサポートされます。この機能は、AFF / ASAプラットフォームでのみ使用できます。
ONTAP Mediator 1.5でのSnapMirrorビジネス継続性のサポート	ONTAP Mediator 1.5では、SnapMirrorアクティブ同期関係を監視できます。
SnapMirrorアクティブ同期継続性の強化	SnapMirror Active Syncは、Snapshotからの部分的なLUNリストアをサポートしています。また、SnapMirrorのアクティブな同期機能により、SnapMirror関係にないボリュームでもQoSが拡張されます。
SnapMirror非同期のデータウェアハウス再構築インジケータ	SnapMirror非同期では、ディザスタリカバリのリハーサル後にData Warehouseのリビルドにかかる時間を示すインジケータが表示されます。これには、完了したパーセンテージが表示されます。
最小保持期間を「未指定」に設定するSnapLockオプション絶対保持期間	SnapLockには、絶対保持期限が「unspecified」に設定されている場合に最小保持期限を設定するオプションがあります。
スナップショットの改ざん防止	SnapLock以外のボリュームでSnapshotをロックして、ランサムウェア攻撃から保護できます。スナップショットをロックすると、誤ってまたは悪意を持って削除されないようになります。

ファイル アクセス プロトコル

更新	説明
AES暗号化を使用してKerberosベースの通信のセキュリティを構成する	新しいSMBセキュリティオプションを使用すると、Active Directory（AD）KDCとのKerberosベースの通信にAdvanced Encryption Standard（AES）暗号化タイプを優先してRC4とDESを無効にできます。

更新	説明
NASデータへのS3クライアントアクセス	S3クライアントは、再フォーマットすることなくNFSクライアントやSMBクライアントと同じNASデータにアクセスできるため、オブジェクトデータを必要とするS3アプリケーションを簡単に提供できます。
NFS拡張属性	NFSv4.2に対応したNFSサーバでは、属性対応クライアントからNFS拡張属性（xattrs）を格納および取得できます。
NFSv4.2のスパースファイルとスペースリザベーションのサポート	NFSv4.2クライアントでは、スパースファイル用にスペースをリザーブできます。スペースの割り当てを解除したり、ファイルから予約を解除したりすることもできます。

ネットワーク

更新	説明
LIFサービス	サービスを使用して、監査ログをリモートsyslogサーバに転送するために使用するLIFを制御できます。 `management-log-forwarding`

S3オブジェクトストレージ

更新	説明
S3操作のサポートを強化	次のAmazon S3 APIアクションがサポートされています。 • `CopyObject` • `UploadPartCopy` • `BucketPolicy`（GET、PUT、DELETE）

SAN

更新	説明
AFFおよびFASプラットフォームの最大LUNサイズの拡張	ONTAP 9.12.1P2以降では、AFFおよびFASプラットフォームでサポートされるLUNの最大サイズが16TBから128TBに拡張されました。
"NVMeの上限の引き上げ"	NVMeプロトコルでサポートされる機能は次のとおりです。 • 1つのStorage VMと1つのクラスタに8Kのサブシステムを配置 • 12ノードクラスタNVMe/FCはポートあたり256台のコントローラをサポートし、NVMe/TCPはノードあたり2、000台のコントローラをサポートします。
NVMe/TCPのサポートによるセキュアな認証	NVMeホストとコントローラの間で、DHHMAC-CHAP認証プロトコルを使用したNVMe/TCP経由のセキュアな一方向認証および双方向認証がサポートされます。
MetroCluster IPでのNVMeのサポート	4ノードMetroCluster IP構成ではNVMe / FCプロトコルがサポートされます。

セキュリティ

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

機能	説明
自律型ランサムウェア対策の相互運用性の強化	自律型ランサムウェア対策は、次の構成で使用できます。 • SnapMirrorで保護されているボリューム • SnapMirrorで保護されているSVM • 移行に対応したSVM（SVMのデータ移動）
多要素認証（MFA）でのFIDO2とPIV（どちらもYubikeyで使用される）を使用したSSHのサポート	SSH MFAでは、ユーザ名とパスワードによるハードウェア支援型の公開鍵 / 秘密鍵交換を使用できます。Yubikeyは、MFAセキュリティを強化するためにSSHクライアントに接続する物理トークン デバイスです。
改ざん不能のロギング	ONTAPの内部ログはすべてデフォルトで改ざん不能になっているため、不正な管理者アカウントで悪意のある操作を隠蔽することはできません。
イベントのTLS転送	TLSプロトコルを使用してEMSイベントをリモートsyslogサーバに送信できるため、集約型外部監査ロギングのためのネットワークを介した保護が強化されます。

Storage Efficiency

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

ストレージリソース管理の機能拡張

更新	説明
FlexGroupリバランシング	無停止のFlexGroupボリュームの自動リバランシングを有効にして、FlexGroupコンスティチュエント間でファイルを再配分することができます。 FlexVolからFlexGroupへの変換後は、FlexGroupの自動リバランシングを使用しないことを推奨します。代わりに、ONTAP 9 .10.1以降の停止を伴う遡及的ファイル移動機能を使用するには、コマンドを入力し `volume rebalance file-move`ます。詳細情報とコマンド構文については、"ONTAP コマンドリファレンス" 。
SnapLock for SnapVaultによるFlexGroupボリュームのサポート	SnapLock for SnapVaultによるFlexGroupボリュームのサポート

SVM管理の機能拡張

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

System Manager

ONTAP 9.12.1 以降、System Manager はNetAppコンソールと統合されています。コンソールを使用すると、管理者は使い慣れたシステム マネージャー ダッシュボードを維持しながら、単一のコントロール プレーンからハイブリッド マルチクラウド インフラストラクチャを管理できます。System Manager にサインインする場合、管理者はNetAppコンソールの System Manager インターフェイスにアクセスするか、System Manager に直接アクセスするかを選択できます。詳細はこちらSystem Manager とNetAppコンソールの統合 。

更新	説明
System ManagerによるSnapLockのサポート	System Managerでは、コンプライアンスクロックの初期化、SnapLockボリュームの作成、WORMファイルのミラーリングなどのSnapLock処理がサポートされます。
ケーブル配線のハードウェア可視化	System Managerユーザは、クラスタ内のハードウェアデバイス間のケーブル接続に関する接続情報を表示して、接続の問題をトラブルシューティングできます。
System Managerへのログイン時にCisco Duoを使用した多要素認証のサポート	Cisco DuoをSAMLアイデンティティプロバイダ（IdP）として設定すると、ユーザがSystem Managerにログインするときにに Cisco Duoを使用して認証できるようになります。
System Managerのネットワーク機能拡張	System Managerでは、ネットワークインターフェイスの作成時にサブネットとホームポートをより細かく制御できます。System Managerでは、RDMA接続経由のNFSの設定もサポートされます。

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

ONTAP 9.11.1の新機能

ONTAP 9 .11.1の新機能について説明します。

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート"。
- の更新について説明します。 "ONTAP REST API"

ONTAPを最新バージョンにアップグレードするには、を参照してくださいONTAPをアップグレードする準備。

データ保護

更新	説明
クラスタカイフキイサアハ	クラスタ化された外部キー管理サーバは、クラスタ化されたKMIPサーバソリューションを提供するNetAppパートナー向けにサポートされるようになりました。これにより、プライマリとセカンダリのKMIPサーバを追加して、暗号化キーデータの重複を防止できます。サポートされているパートナーについては、を参照して"Interoperability Matrix Tool"ください。
System ManagerのSnapMirror非同期ポリシー	System Managerを使用して、ボリュームやStorage VMを保護する際に、事前に作成されたカスタムのミラーとバックアップポリシーを追加したり、従来のポリシーを表示したり、保護ポリシーで定義されている転送スケジュールを上書きしたりできます。また、System Managerを使用して、ボリュームとStorage VMの保護関係を編集することもできます。 ONTAP 9.8P12以降のONTAP 9.8パッチ リリースを実行していて、System ManagerからSnapMirrorを設定した場合、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする際は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチ リリースをアップグレードに使用してください。
SnapMirror Cloudによる単一ディレクトリのリストア	admin権限レベルのクラスタ管理者が、クラウド エンドポイントから単一ディレクトリのリストア処理を実行できます。リストア元のバックアップ エンドポイントを特定するためにソース エンドポイントのUUIDを指定する必要があります。複数のバックアップでデスティネーションと同じ名前を使用できるため、 `cloud_endpoint_name`restoreコマンドではバックアップに関連付けられたUUIDを指定する必要があります。コマンドを使用すると、を取得 `source_endpoint_uuid`できます `snapmirror show`。
SnapMirrorアクティブ同期のサポートの強化	• SnapMirrorアクティブ同期で、ホストとしてAIXがサポートされます • SnapMirrorアクティブ同期で単一ファイルのSnapRestoreがサポートされるため、SnapMirrorアクティブ同期構成のLUNまたは通常のファイルを個別にリストアできます
SVMデータ レプリケーションのクイック再同期	SVMデータ レプリケーションのクイック再同期を使用すると、ストレージ管理者は、データ ウェアハウスの完全な再構築を省略できるため、ディザスタ リカバリのリハーサルからより迅速にリカバリできます。
MetroClusterでのSVMデータ レプリケーションのサポート	MetroCluster構成の両側でSVM-DRソースがサポートされます。
2フェーズ・コンシステンシ・グループのスナップショット作成	REST APIでは、整合グループで2段階のSnapshot処理がサポートされるため、Snapshotをコミットする前に事前確認を実行できます。

ファイル アクセス プロトコル

更新	説明
TLSv1.3のサポート	ONTAPでは、HTTPSおよびREST API管理プロトコルでTLS 1.3がサポートされます。TLS 1.3は、SP / BMCやクラスタ ピアリング暗号化ではサポートされません。
LDAP高速バインドのサポート	LDAPサーバでサポートされている場合は、LDAP高速バインドを使用して、ONTAP管理者ユーザをすばやく簡単に認証できます。

ネットワーク

更新	説明
Link Layer Discovery Protocol（LLDP）	クラスタ ネットワークでLLDPがサポートされます。これにより、Cisco Discovery Protocol（CDP）をサポートしていないクラスタ スイッチともONTAPを連携できます。
LIFサービス	新しいクライアント側のLIFサービスでは、アウトバウンドのAD、DNS、LDAP、NISの要求にどのLIFを使用するかをより細かく制御できます。

S3オブジェクトストレージ

更新	説明
S3オブジェクト操作のサポートの追加	ONTAP APIでサポートされるアクションは `CreateBucket`、`DeleteBucket` `DeleteObjects`です。さらに、`ONTAP S3`では、オブジェクトのバージョン管理と、 `GetBucketVersioning`での関連付けられた操作がサポートされます `PutBucketVersioning` `ListBucketVersions`。

SAN

更新	説明
iSCSI LIFフェイルオーバー	新しいiSCSI LIFフェイルオーバー機能では、SFOパートナーのフェイルオーバー時およびローカル フェイルオーバー時にiSCSI LIFを自動および手動で移行できます。iSCSI LIFフェイルオーバーは、オールSANアレイ（ASA）プラットフォームで使用できます。
LUNからNVMeネームスペース、NVMeネームスペースからLUNへの無停止での移行	ONTAP CLIを使用して、またはをインプレース変換し既存のLUNをNVMeネームスペースにキソンノNVMeネエムスへエスヲLUNニます。

セキュリティ

更新	説明
自律型ランサムウェア対策（ARP）の機能拡張	ARP検出アルゴリズムが強化され、追加のマルウェアの脅威を検出できるようになりました。また、自律型ランサムウェア対策のアクティブ化に新しいライセンス キーが使用されます。ONTAP 9.10.1からアップグレードしたONTAPシステムの場合は、以前のライセンス キーでも同じ機能を利用できます。

更新	説明
マルチ管理者認証	マルチ管理者認証が有効になっている場合、ボリュームやスナップショットの削除などの特定の操作は、指定された管理者の承認後にのみ実行できます。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。

Storage Efficiency

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

ストレージリソース管理の機能拡張

更新	説明
ファイルシステム分析におけるSVMレベルのアクティビティ追跡	アクティビティ追跡はSVMレベルで集計され、読み取り/書き込みIOPSとスループットを追跡することで、データに関する実用的な分析情報を瞬時に提供します。
ファイルアクセス時間の更新を有効にする	有効にすると、現在のアクセス時間がユーザが指定した期間を超えた場合にのみ、FlexCache元のボリュームでアクセス時間が更新されます。
非同期ディレクトリの削除	非同期削除は、ストレージ管理者がボリュームに対する権限をNFSクライアントとSMBクライアントに許可した場合に使用できます。非同期削除が有効になっている場合、Linuxクライアントではmvコマンドを使用でき、Windowsクライアントではrenameコマンドを使用してディレクトリを削除し、非表示のディレクトリに移動でき`.ontaptrashbin`ます。
SnapLockでのFlexGroupボリュームのサポート	SnapLockでは、FlexGroupボリュームに格納されたデータがサポートされます。FlexGroupボリュームは、SnapLock ComplianceモードとSnapLock Enterpriseモードでサポートされます。SnapLockでは、FlexGroupボリュームでのSnapLock for SnapVault、イベントベースの保持、およびリーガルホールドの処理はサポートされていません。

SVM管理の機能拡張

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

System Manager

更新	説明
SnapMirror非同期ポリシーを管理します。	ボリュームやStorage VMを保護する場合は、System Managerを使用して、事前に作成されたカスタムのミラーとバックアップポリシーを追加したり、従来のポリシーを表示したり、保護ポリシーで定義されている転送スケジュールを上書きしたりできます。また、System Managerを使用して、ボリュームとStorage VMの保護関係を編集することもできます。 ONTAP 9.8P12以降のONTAP 9.8パッチ リリースを使用していて、System Managerを使用してSnapMirrorを設定していて、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする場合は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチ リリースをアップグレードに使用してください。
ハードウェアの可視化	System Managerのハードウェア可視化機能は、現在のすべてのAFFおよびFASプラットフォームをサポートしています。
システム分析情報	System Managerの[Insights]ページには、容量やセキュリティに関する追加の分析情報のほか、クラスタやStorage VMの構成に関する新しい分析情報が表示されるため、システムの最適化に役立ちます。
ユーザビリティの向上	• 新しく作成したボリュームは、デフォルトでは共有できません。デフォルトのアクセス権限（NFS経由のエクスポート、SMB / CIFS経由の共有、権限レベルの指定など）を指定できます。 • SANの簡易化：System Managerでイニシエータグループを追加または編集するときに、グループ内のイニシエータの接続ステータスを表示して、LUNデータにアクセスできるように接続されているイニシエータをグループに含めることができます。
アドバンストローカル階層（アグリゲート）処理	System Manager 管理者は、System Manager からの推奨事項を受け入れたくない場合は、ローカル層の構成を指定できます。また、既存のローカル階層のRAID構成を編集することもできます。 ONTAP 9.8P12以降のONTAP 9.8パッチ リリースを使用していて、System Managerを使用してSnapMirrorを設定していて、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする場合は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチ リリースをアップグレードに使用してください。
監査ログの管理	System Managerを使用して、ONTAP監査ログを表示および管理できます。

関連情報

- "snapmirror show"

ONTAP 9.10.1の新機能

ONTAP 9 10.1の新機能について説明します。

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート"。
- の更新について説明します。 "ONTAP REST API"

ONTAPのアップグレードについては、を参照してくださいONTAPをアップグレードする準備。

データ保護

更新	説明
SnapLockの保持期間を最大100年に設定	ONTAP 9 .10.1より前のリリースでは、サポートされる最大保持期間は2071年1月19日です。ONTAP 9 10.1以降、SnapLock EnterpriseおよびComplianceでは、3058年10月26日までの保持期間と100年までの保持期間がサポートされます。保持期限を延長すると、古いポリシーが自動的に変換されます。
同じアグリゲートにSnapLockボリュームとSnapLock以外のボリュームを作成する機能	ONTAP 9 .10.1以降では、SnapLockボリュームとSnapLock以外のボリュームを同じアグリゲートに配置できるため、SnapLockボリューム用に個別にSnapLockアグリゲートを作成する必要はありません。
整合グループ	ボリュームとLUNを整合グループに編成してデータ保護ポリシーを管理し、複数のストレージボリュームにまたがるワークロードの書き込み順序に忠実であることを確認します。
パブリッククラウドでバックアップをアーカイブ	SnapMirror Cloudは、長期保持のために、AWSおよびMS Azureの低コストのパブリッククラウドオブジェクトストレージクラスへのONTAPバックアップの階層化をサポートしています。
セキュアなネットログオンチャネル通信のためのAESサポート	Netlogon認証サービスを使用してWindowsドメインコントローラに接続する場合は、Advanced Encryption Standard（AES）を使用してセキュアなチャネル通信を行うことができます。
SMBドメイントンネル認証でのKerberos	Kerberos認証は、NTLMに加えて、ONTAP管理用のドメイントンネル認証にも使用できます。これにより、Active Directoryのクレデンシャルを使用してONTAP CLIおよびSystem Manager GUIにログインする際の安全性が向上します。
チャネルバインディングによるLDAP通信のセキュリティ強化	LDAPチャネルバインドは、Active Directoryとネームサービスの両方のLDAP接続でデフォルトでサポートされています。これにより、中間者攻撃に対する保護が強化されます。

ファイル アクセス プロトコル

更新	説明
NFS over RDMA（NVIDIAのみ）	NFS over RDMAはRDMAアダプタを使用します。ストレージ システムとホスト システムのメモリ間でデータが直接コピーされるため、CPUの中断やオーバーヘッドを回避できます。NFS over RDMAにより、サポート対象のNVIDIA GPUを搭載したホストでNVIDIA GPUDirect Storageを使用してワークロードをGPUで高速化することができます。

ネットワーク

更新	説明
RDMAクラスタインターコネクト	A400またはASA A400ストレージシステムとX1151AクラスタNICを使用すると、マルチノードクラスタでハイパフォーマンスワークロードを高速化し、クラスタ内トラフィックにRDMAを活用できます。
システムSVMのLIFでステータスadminをdownに設定するには、確認が必要です	これにより、クラスタの適切な運用に欠かせないLIFが誤って停止するのを防ぐことができます。CLIでこの動作を呼び出すスクリプトがある場合は、確認手順に合わせてスクリプトを更新する必要があります。
ネットワーク配線の問題の自動検出と修復に関する推奨事項	ポートの到達可能性の問題が検出された場合は、ONTAP修復処理を実行して問題を解決することを推奨します。
Internet Protocol Security（IPsec;インターネットプロトコルセキュリティ）証明書	IPSecポリシーでは、認証用の証明書に加えて、事前共有キー（PSK）がサポートされます。
LIFのサービスポリシー	ファイアウォールポリシーは廃止され、LIFのサービスポリシーに置き換えられました。アウトバウンドNTP要求に使用するLIFをより細かく制御できるように、新しいNTP LIFサービスポリシーも追加されました。

S3オブジェクトストレージ

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

SAN

更新	説明
NVMeネームスペース	ONTAP CLIを使用して、ネームスペースのサイズを拡張または縮小できます。System Managerでは、ネームスペースのサイズを拡張できます。
TCPでのNVMeプロトコルのサポート	NVMe（Non-Volatile Memory express）プロトコルを、TCPネットワークを介したSAN環境で使用できます。

セキュリティ

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

Storage Efficiency

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

ストレージリソース管理の機能拡張

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

SVM管理の機能拡張

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

System Manager

更新	説明
System Managerのログでパフォーマンステレメトリログを有効にする	管理者は、System Managerでパフォーマンスの問題が発生した場合にテレメトリログを有効にし、サポートに連絡して問題を分析できます。
NetAppライセンスファイル	すべてのライセンスキーは、個別の28文字のライセンスキーではなくNetAppライセンスファイルとして提供されるため、1つのファイルを使用して複数の機能のライセンスを取得できます。
ファームウェアの自動更新	System Manager管理者は、ファームウェアを自動的に更新するようにONTAPを設定できます。
リスク軽減のための推奨事項をレビューし、Digital Advisorから報告されるリスクを承認する	System Managerユーザは、Digital Advisorによって報告されるリスクを確認し、リスクの軽減に関する推奨事項を確認できます。9.10.1以降では、リスクを承認することもできます。
管理者によるEMSイベント通知の受信の設定	System Manager管理者は、対応が必要なシステムの問題が通知されるように、イベント管理システム（EMS）のイベント通知の配信方法を設定しておくことができます。
証明書の管理	System Manager管理者は、信頼された認証局、クライアント / サーバ証明書、ローカル（オンボード）認証局を管理できます。
System Managerを使用した過去の容量利用の確認と将来の容量ニーズの予測	Digital AdvisorとSystem Managerが統合されているため、管理者はクラスタの容量使用状況の履歴データを表示できます。
System Managerを使用して、Cloud Backup Serviceを使用してStorageGRIDにデータをバックアップする	Cloud Managerをオンプレミスに導入している場合は、Cloud Backup Service管理者がStorageGRIDにバックアップできます。AWSまたはAzureでCloud Backup Serviceを使用してオブジェクトをアーカイブすることもできます。

更新	説明
ユーザビリティの向上	ONTAP 9.10.1以降では、次のことが可能になります。 • 親ボリュームではなくLUNへのQoSポリシーの割り当て（VMware、Linux、Windows） • LUNのQoSポリシー グループの編集 • LUNの移動 • LUNのオフライン化 • ONTAPイメージのローリング アップグレードの実行 • ポートセットの作成とigroupへのバインド • ネットワーク配線の問題の自動検出と修復に関する推奨事項 • Snapshotディレクトリへのクライアントアクセスを有効または無効にする • Snapshotを削除する前に再利用可能なスペースを計算 • SMBキョウユウノケイソクテキカヨウセイノフィールドヘンコウヘノアクセス • より正確な表示単位を使用した容量測定値の表示 • WindowsとLinuxでのホスト固有のユーザとグループの管理 • AutoSupport設定の管理 • 個別操作でのボリューム サイズの変更

ONTAP 9.9.1の新機能

ONTAP 9 .9.1で提供される新しい機能について説明します。

最近のONTAP 9リリースの既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、を参照して "ONTAP 9 リリース ノート"ください。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

- 新しい機能と強化された機能について説明します "ONTAP MetroClusterの機能"。
- 学ぶ "AFF、 ASA、 FASシステムおよびサポート対象スイッチに対する新規および強化されたサポート"。
- の更新について説明します。 "ONTAP REST API"

ONTAPを最新バージョンにアップグレードするには、を参照してくださいONTAPをアップグレードする準備。

データ保護

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

ファイル アクセス プロトコル

更新	説明
"LDAPリファーラル追跡の機能拡張"	LDAPリファーラル追跡は、LDAPの署名と封印、暗号化されたTLS接続、およびLDAPSポート636経由の通信でサポートされます。
"任意のポートでLDAPSをサポート"	LDAPSは任意のポートに設定できます。デフォルトはポート636です。
"デフォルトで有効になるNFSv4.xのバージョン"	NFSv4.0、NFSv4.1、NFSv4.2がデフォルトで有効になります。
"ラベル付きNFSv4.2をサポート"	NFSv4.2が有効になっている場合は、強制アクセス制御（MAC: Mandatory Access Control）ラベル付きNFSがサポートされます。この機能により、ONTAP NFSサーバはMACに対応し、クライアントから送信された属性を格納および取得し `sec_label`ます。

ネットワーク

更新	説明
"クラスタの耐障害性"	• 2ノードスイッチレスクラスタのポートの監視と回避（従来はスイッチ構成でのみ使用可能） • クラスタネットワーク経由でデータを提供できないノードの自動フェイルオーバー • パケット損失が発生しているクラスタパスを表示する新しいツール

更新	説明
"仮想IP（VIP）LIFの拡張機能"	• Border Gateway Protocol（BGP;ボーダーゲートウェイプロトコル）のAutonomous System Number（ASN;自律システム番号）は、4バイトの非負整数をサポートします。 • Multi-Exit Discriminator（MED）を使用すると、パスの優先順位付けをサポートした高度なルート選択が可能になります。MEDは、BGPアップデートメッセージのオプション属性です。 • VIP BGPは、BGPピアグループ化を使用してデフォルトルートを自動化し、設定を簡素化します。

S3オブジェクトストレージ

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

SAN

更新	説明
Foreign LUN Import（FLI）	NetAppサポート サイトのSAN LUN Migrateアプリケーションを使用して、FLI Interoperability Matrixに記載されていない外部アレイを評価できます。
NVMe-oFリモート パス アクセス	フェイルオーバー時に直接パス アクセスが失われた場合でも、リモートI/Oを使用してシステムをリモート パスにフェイルオーバーしてデータ アクセスを継続できます。
ASAでの12ノード クラスタのサポート	AFF ASA構成で、12ノード クラスタがサポートされます。ASAクラスタには、さまざまな種類のASAシステムを混在させることができます。
ASAでのNVMe-oFプロトコル	AFF ASAシステムで、NVMe-oFプロトコルもサポートされるようになりました。
igroupの機能拡張	• 既存のigroupで構成されるigroupを作成できます。です。 • igroupまたはホストイニシエータのエイリアスとして機能するigroupまたはホストイニシエータに説明を追加できます。 • igroupを2つ以上のLUNに同時にマッピングできます。
単一LUNのパフォーマンスの向上	AFFの単一LUNのパフォーマンスが大幅に向上し、仮想環境への導入を簡易化するのに最適です。たとえば、A800ではランダムリードIOPSが最大400%向上します。

セキュリティ

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

Storage Efficiency

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

ストレージリソース管理の機能拡張

更新	説明
System Managerのファイルシステム分析（FSA）管理の機能拡張	FSAで検索やフィルタリングを行ったり、FSAの推奨事項に基づく操作を実行したりするための機能がSystem Managerに追加されました。
ネガティブ ルックアップ キャッシュをサポート	FlexCacheボリュームで発生した「file not found」エラーをキャッシュして、元のボリュームの呼び出しに起因するネットワーク トラフィックを削減します。
FlexCacheディザスタ リカバリ	キャッシュ間でクライアントを無停止で移行できます。
FlexGroupボリュームでのSnapMirrorカスケードとファンアウトをサポート	FlexGroupボリュームでのSnapMirrorカスケード関係とSnapMirrorファンアウト関係がサポートされました。
FlexGroupボリュームのSVMディザスタ リカバリをサポート	FlexGroupボリュームのSVMディザスタ リカバリがサポートされました。これにより、SnapMirrorを使用してSVMの設定とデータをレプリケート、同期して冗長性を確保できます。
FlexGroupボリュームの論理スペースのレポート作成と適用をサポート	FlexGroupボリュームのユーザによって消費される論理スペースを表示、制限できます。
qtreeでのSMBアクセスをサポート	SMBが有効なFlexVolおよびFlexGroupボリュームのqtreeでのSMBアクセスがサポートされました。

System Manager

更新	説明
Digital Advisorから報告されたリスクがSystem Managerに表示される	System Managerを使用して、Active IQデジタルアドバイザ（別名デジタルアドバイザ）にリンクします。このアドバイザは、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を報告します。
ローカル階層を手動で割り当てる	System Managerでは、ボリュームおよびLUNを作成および追加するときに、ローカル階層を手動で割り当てることができます。
非同期ディレクトリの削除	System Managerでは、低レイテンシの非同期ディレクトリ削除機能を使用してディレクトリを削除できます。

更新	説明
Ansible Playbookの生成	System Managerユーザが、UIを通じて一部のワークフローのAnsible Playbookを生成し、それを自動化ツールで使用してボリュームやLUNを繰り返し追加または編集できます。
ハードウェアの可視化	ONTAP 9.8で初めて導入されたハードウェア可視化機能が、すべてのAFFプラットフォームでサポートされるようになりました。
Digital Advisorの統合	System Managerユーザは、クラスタに関連するサポートケースを表示してダウンロードできます。また、NetAppサポートサイトで新しいサポートケースを送信するために必要なクラスタの詳細もコピーできます。System Managerユーザは、Digital Advisorからアラートを受信して、新しいファームウェア更新が利用可能になったときに通知することができます。その後、System Managerを使用してファームウェアイメージをダウンロードし、アップロードできます。
Cloud Managerの統合	System Managerユーザは、Cloud Backup Serviceを使用してパブリッククラウドエンドポイントにデータをバックアップする保護を設定できます。
データ保護プロビジョニングワークフローの機能拡張	System Managerユーザは、データ保護の設定時に、SnapMirrorデスティネーションとigroupの名前を手動で指定できます。
ネットワークポート管理の強化	[ネットワークインターフェイス]ページでは、ホームポートのインターフェイスを表示および管理する機能が強化されています。
システム管理の機能拡張	• ネストされたigroupのサポート • 1回のタスクで複数のLUNをigroupにマッピングし、処理中にWWPNエイリアスを使用してフィルタリングできます。 • NVMe-oF LIFの作成中に、両方のコントローラで同じポートを選択する必要がなくなりました。 • 各ポートのトグル ボタンでFCポートを無効にできます。
System ManagerでのSnapshotに関する情報の表示の強化	• System Managerユーザは、SnapshotのサイズとSnapMirrorラベルを表示できます。 • Snapshotが無効になっている場合、Snapshotリザーブはゼロに設定されます。
ストレージ階層の容量と場所の情報に関するSystem Managerの表示機能を強化	• 新しい[* **Tiers**列には、各ボリュームが配置されているローカル階層（アグリゲート）が表示されます。] • System Managerには、ローカル階層（アグリゲート）レベルに加え、クラスタレベルの使用済み物理容量と使用済み論理容量が表示されます。 • 新しい容量表示フィールドを使用すると、容量を監視したり、容量に近づいているボリュームや使用率が低いボリュームを追跡したりできます。
EMS緊急アラートおよびその他のエラーと警告をSystem Managerに表示する	24時間以内に受信したEMSアラートの数、およびその他のエラーや警告は、System Managerの[Health]カードに表示されます。

ONTAPの制限とデフォルトに対する変更

ONTAP 9リリースで実装された制限とデフォルトの一部の変更点について説明します。NetAppは、ONTAPの各リリースで最も重要なデフォルトと制限の変更をお客様が理解できるように努めています。

ONTAPノテフオルトノヘンコウ

新しいONTAPリリースにアップグレードする前に、ONTAPのデフォルト設定に対する変更が自動化やビジネスの運用に影響する可能性があることを確認しておく必要があります。

機能	デフォルトの変更	リリースで変更...
ボリュームのデフォルト	NAS プロトコルに割り当てられたONTAPクラスター上の新しく作成された SVM に作成されたボリュームでは、ファイル システム分析 (FSA) がデフォルトで有効になっています。	ONTAP 9.17.1
HTTP 厳格なトランスポート セキュリティ (HSTS)	9.17.1 では HSTS がデフォルトで有効になっています。	ONTAP 9.17.1
NASの監査	および `file-session-io-grouping-duration`パラメータの最大制限 `file-session-io-grouping-count`が拡張され、オプションで選択できる統合NAS監査イベント通知の数が少なくなりました。これにより、SVMのIO速度が向上し、デスティネーションボリュームへのストレージへの影響が軽減されます。nfs_file_session_io_grouping_count_max：20000～120000 nfs_file_session_io_grouping_duration_max：600～3600	ONTAP 9 .16.1
FASシステムのノードあたりの最大ボリューム数	コントローラあたり200GBを超えるRAMを搭載したFASシステムでは、ノードあたりのサポートされるボリュームの最大数が1、000から2、500に増加します。以前のバージョンのONTAPでは"Data Protection Optimized（DPO）"、ONTAP FASシステムのサポートをノードあたり1、000~2、500個に増やすためにライセンスが必要でした。	ONTAP 9 .16.1
負荷共有ミラー	負荷共有ミラー関係を作成する場合、SVM でストレージ制限を有効にすることはできません。	ONTAP 9 .16.1
`vserver object-store-server user show`コマンド	ONTAP 9 .15.1より前のリリースでは `vserver object-store-server user show`、コマンドからS3ユーザのシークレットキーが返されていました。コマンドからS3ユーザのシークレットキーデータが返されなくなります。	ONTAP 9 .15.1
NASの監査	NAS監査設定では、デフォルトですべての監査ログレコードを保持できます。rotate-limitパラメータの値を変更すると、監査ログがサポートするボリュームに合わせて適切にサイジングされます。	ONTAP 9 .15.1

機能	デフォルトの変更	リリースで変更...
スペースの割り当て	新しく作成したLUNに対しては、スペース割り当てがデフォルトで有効になります。以前のバージョンのONTAP（9.14.1以前）では、スペース割り当てがデフォルトで無効になっていました。	ONTAP 9 .15.1
NVMe/TCPによるホストの自動検出	NVMe/TCPプロトコルを使用するコントローラのホスト検出は、デフォルトで自動化されています。	ONTAP 9 .14.1
Kerberosベースの通信用のAES暗号化	認証用のAES暗号化は、SMBサーバとのKerberosベースの通信ではデフォルトで有効になっています。AES暗号化がサポートされていない環境では、AES暗号化を手動で無効にできます。	ONTAP 9 .13.1
RAIDアグリゲート	ONTAP 9.12.1以降では、いずれかのアグリゲートがデグレード状態の場合、24時間後にシステムコントローラはデフォルトでシャットダウンされません。ユーザがオプションを変更した場合、 `raid.timeout`システムコントローラは時間が経過してもシャットダウンし続け `raid.timeout`ます。	ONTAP 9 12.1
TLS 1.1をデフォルトで無効にする	ONTAPの新規インストールでは、TLS 1.1はデフォルトで無効になっています。ONTAP 9 1.1が有効な状態のままになるため、TLS 1.1以降にアップグレードしたシステムは影響を受けません。ただし、FIPSが有効になっているクラスタをアップグレードする場合、ONTAP 9 .11.1以降のFIPSではTLS 1.1がサポートされないため、TLS 1.1は自動的に無効になります。デフォルトで無効になっている場合、TLS 1.1は必要に応じて手動で有効にできます。	ONTAP 9 .12.0
TLS 1.0がデフォルトで無効	ONTAPの新規インストールでは、TLS 1.0はデフォルトで無効になっています。ONTAP 9 .8以降にアップグレードしたシステムですでにTLS 1.0が有効になっている場合は、アップグレード後にTLS 1.0が有効な状態になるため、影響はありません。ただし、FIPSが有効になっているクラスタをアップグレードする場合、ONTAP 9 8以降のFIPSではTLS 1.0がサポートされないため、TLS 1.0は自動的に無効になります。デフォルトで無効になっている場合、TLS 1.0は必要に応じて手動で有効にできます。	ONTAP 9.8

ONTAPの制限に対する変更

新しいONTAPリリースにアップグレードする前に、ONTAP制限に対する変更が自動化やビジネスの運用に影響する可能性があることを確認しておく必要があります。

機能	セイケンヘンコウ	リリースで変更...
qtreeの拡張パフォーマンス監視	1つのONTAPクラスタで最大50、000個のqtreeに対して拡張パフォーマンス監視を有効にすることができます。	ONTAP 9 .16.1
SnapMirrorアクティブ同期	SnapMirrorのアクティブな同期で整合グループ内の80個のボリュームをサポート	ONTAP 9 .15.1

機能	セイケンヘンコウ	リリースで変更...
SnapMirror非同期	SnapMirror非同期保護を使用する整合グループでは、整合グループで最大80個のボリュームがサポートされます。	ONTAP 9 .15.1
ファイルシステム分析	ONTAPでは、パフォーマンスの問題を軽減するために、ファイルシステム分析を有効にする際に、ボリュームの容量の5~8%を空けておく必要があります。	ONTAP 9 .15.1
SVMのデータ移動	SVMのデータ移動が可能なSVMあたりのサポートされるボリュームの最大数が400に増え、サポートされるHAペアの数が12に増えました。	ONTAP 9 .14.1
FlexGroupリバランシング	FlexGroupのリバランシング処理で設定可能な最小ファイルサイズが4KBから20MBに拡張されました。	• ONTAP 9 .14.1 • ONTAP 9.13.1P1 • ONTAP 9.12.1P10
FlexVolとFlexGroupのボリューム サイズの制限	AFFプラットフォームとFASプラットフォームでサポートされるFlexVolとFlexGroupのボリューム コンスティチュエントの最大サイズが、100TBから300TBに引き上げられました。	ONTAP 9.12.1P2
LUNのサイズの制限	AFFプラットフォームとFASプラットフォームでサポートされるLUNのサイズ上限が、16TBから128TBに引き上げられました。SnapMirror構成（同期および非同期の両方）でサポートされるLUNの最大サイズが16TBから128TBに拡張されました。	ONTAP 9.12.1P2
FlexVol volumeサイズ制限	AFFおよびFASプラットフォームでサポートされる最大ボリュームサイズが100TBから300TBに拡張されました。SnapMirror同期構成でサポートされるFlexVolの最大サイズが100TBから300TBに拡張されました。	ONTAP 9.12.1P2
ファイルサイズの上限	AFFおよびFASプラットフォームでサポートされるNASファイルシステムの最大ファイルサイズが16TBから128TBに拡張されました。SnapMirror同期構成でサポートされる最大ファイルサイズが16TBから128TBに拡張されました。	ONTAP 9.12.1P2
クラスタノホリユウムセイケン	コントローラがCPUとメモリを最大限に活用できるようになり、クラスタの最大ボリューム数を15、000から30、000に増やします。	ONTAP 9 12.1
FlexVolのSVM-DR関係	FlexVolのSVM-DR関係の最大数が64個から128個に増えました（クラスタあたりのSVM数は128台）。	ONTAP 9 .11.1
SnapMirror同期	HAペアあたりのSnapMirror同期処理の最大数が200から400に増加しました。	ONTAP 9 .11.1
NAS FlexVolボリューム	NAS FlexVolボリュームのクラスタ制限が12、000から15、000に増加しました。	ONTAP 9 10.1
SAN FlexVolボリューム	SAN FlexVolボリュームのクラスタ数の上限が12、000から15、000に引き上げられました。	ONTAP 9 10.1

機能	セイケンヘンコウ	リリースで変更...
FlexGroupを備えたSVM-DR	• FlexGroupでは、最大32個のSVM-DR関係がサポートされます。 • SVM-DR関係にある1つのSVMでサポートされる最大ボリューム数は300で、これにはFlexVolとFlexGroupコンスティチュエントの数が含まれます。 • FlexGroupのコンスティチュエントの最大数は20以下にする必要があります。 • SVM-DRの最大ボリューム数は、ノードあたり500、クラスタあたり1000（FlexVolボリュームとFlexGroupコンスティチュエントを含む）です。	ONTAP 9 10.1
監査を有効にしたSVM	クラスタでサポートされる監査を有効にしたSVMの上限数が、50個から400個に増えました。	ONTAP 9 .9.1
SnapMirror同期	HAペアあたりのサポートされるSnapMirror同期エンドポイントの最大数が80から160に拡張されました。	ONTAP 9 .9.1
FlexGroup SnapMirrorトポロジ	FlexGroupボリュームでは、AからB、AからCなど、2つ以上のファンアウト関係がサポートされます。FlexVolボリュームと同様に、FlexGroupのファンアウトでは、最大8つのファンアウト関係と、AからBからCのように最大2レベルのカスケードがサポートされます。	ONTAP 9 .9.1
SnapMirror同時転送	ボリュームレベルの非同期同時転送の最大数が100から200に増加しました。クラウド間のSnapMirror転送は、ハイエンドシステムでは32件から200件、ローエンドシステムでは6件から20件に増加しています。	ONTAP 9.8
FlexVolホリユウムノセイケン	ASAプラットフォームでは、FlexVolボリュームで消費されるスペースが100TBから300TBに増加しました。	ONTAP 9.8

ONTAP 9リリースのサポート

ONTAP 9 .8リリース以降、NetAppではONTAPリリースを暦年に2回提供しています。計画は変更される可能性がありますが、新しいONTAPリリースは暦年の第2四半期と第4四半期に提供する予定です。この情報は、最新のONTAPリリースを利用するためのアップグレード期間を計画する際に使用します。

バージョン	リリース日
9.17.1	2025年9月
9.16.1	2025年1月

バージョン	リリース日
9.15.1	2024年7月
9.14.1	2024年1月
9.13.1	2023年6月
9.12.1	2023年2月
9.11.1	2022年7月
9.10.1	2022年1月
9.9.1	2021年6月

サポート レベル

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

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

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

開始する

ONTAPの詳細

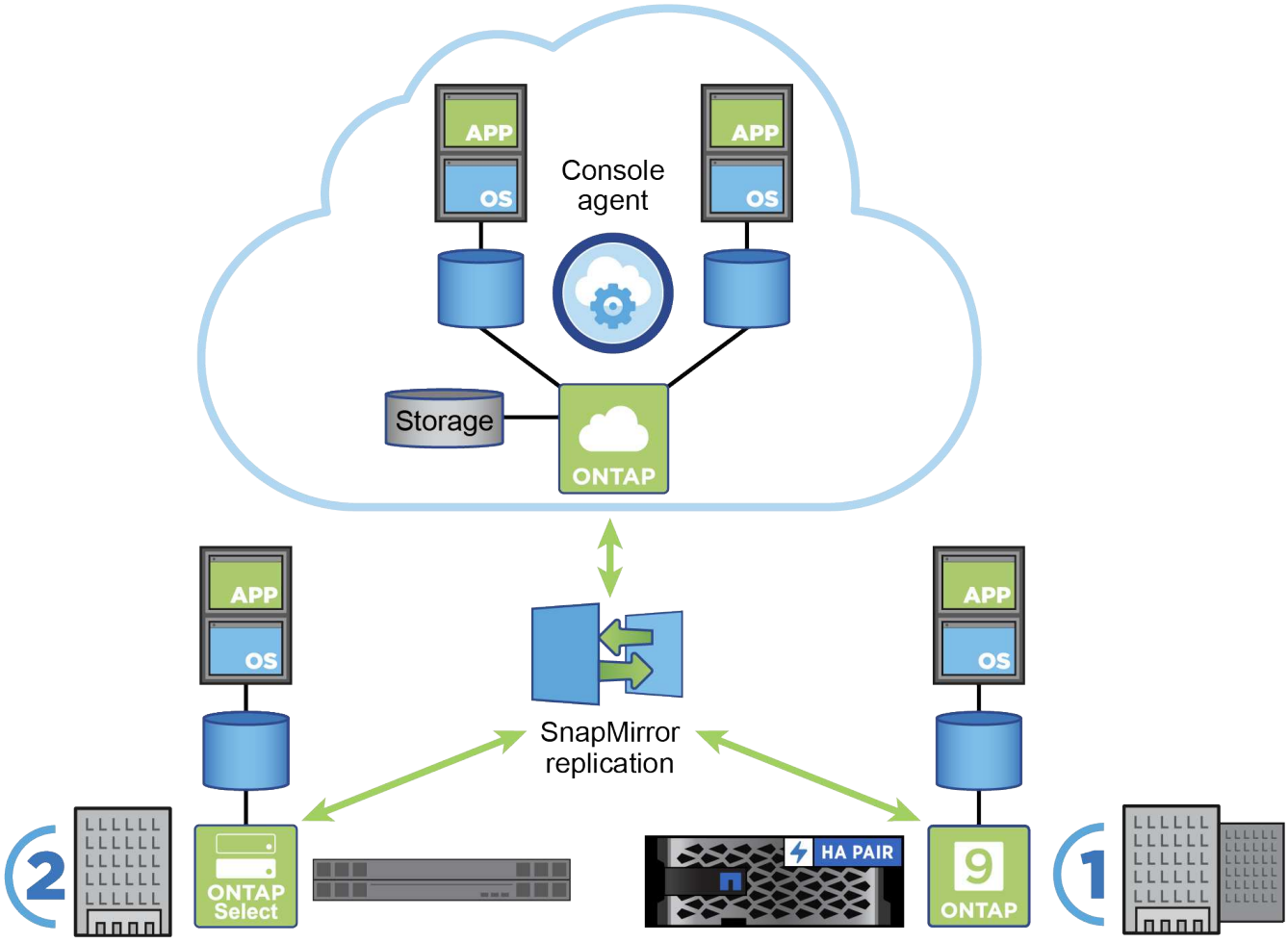
ONTAPプラットフォーム

ONTAPデータ管理ソフトウェアは、ブロックデータやファイルデータの読み取りと書き込みを行うアプリケーションにユニファイドストレージを提供します。高速フラッシュから低価格の回転式メディア、クラウドベースのオブジェクトストレージまで、さまざまなストレージ構成が用意されています。

ONTAPの実装は次の環境で実行されます。

- * NetAppエンジニアリング システム*: "AFF、AFX、 ASA、およびFASストレージシステム"
- * ONTAPストレージ パーソナリティ*: "AFXおよびASA r2ストレージシステム"特定のプロトコルに重点を置いた分散型ONTAPストレージを提供する専用のONTAPパーソナリティを実行します。
- コモディティハードウェア： "ONTAP Select"
- プライベート、パブリック、またはハイブリッド クラウド: "Cloud Volumes ONTAP" 、 "NetApp ONTAP対応の Amazon FSX" 、 "Azure NetApp Files" 、 そして "Google Cloud NetAppボリューム"
- 業界最高のコンバージドインフラを提供する特殊な実装 "FlexPod データセンター"

これらの実装を組み合わせることで、_インテリジェントデータインフラストラクチャ_の基本的なフレームワークが形成され、データ管理に対する共通のソフトウェア定義アプローチと、プラットフォーム間での高速かつ効率的なレプリケーションが実現します。



ONTAPユーザインターフェイス

ONTAPデータ管理ソフトウェアには、ONTAPクラスタの管理に使用できる複数のインターフェイスが用意されています。これらのインターフェイスオプションを使用すると、さまざまなレベルのアクセスや機能を提供し、環境に応じてONTAPクラスタを柔軟に管理できます。

これらのインターフェイスのいずれかを使用して、ONTAPクラスタの管理やデータ管理処理を実行できます。

ONTAPシステムマネージャ

ONTAP System Managerは、Webベースのユーザインターフェイスで、シンプルでわかりやすい方法でクラスタを管理します。ストレージ構成、データ保護、ネットワークのセットアップと管理などの一般的な操作を管理できます。System Managerでは、リスクとクラスタのパフォーマンスを監視し、クラスタの問題に対処して問題を未然に先回りするのに役立つ分析情報も提供されます。"詳細"です。

ONTAP 9.7は、ONTAP System Managerにとって重要なジャンクションとなりました。このリリースでは、NetAppからONTAP System Managerの2つのバージョンが提供され、ONTAP 9.7より前のバージョンに加えて、設計が刷新され、より合理的でわかりやすいバージョンが導入されました。ONTAP 9.7以降、再設計されたバージョンはONTAPシステムマネージャとして引き継がれ、旧バージョンはSystem Managerクラシックに名称が変更された。System Manager Classicの最終更新はONTAP 9.7で行われました。System Manager

Classicを使用している場合は、そのドキュメントを参照 "別 々 に"できます。

NetAppコンソール

ONTAP 9.12.1 以降では、使い慣れた System Manager ダッシュボードを維持しながら、 NetAppコンソールの Web ベース インターフェイスを使用して、単一のコントロール プレーンからハイブリッド マルチクラウド インフラストラクチャを管理できます。コンソールを使用すると、クラウド ストレージ (NetApp Backup and Recovery など) を作成および管理したり、NetApp のデータ サービス (Cloud Backup など) を使用したり、多数のオンプレミスおよびエッジ ストレージ デバイスを制御したりできます。オンプレミスのONTAPシステムをコンソールに追加すると、単一のインターフェースからすべてのストレージとデータ資産を管理できるようになります。 "詳細" 。

ONTAPコマンドラインインターフェイス

は、"ONTAPコマンドラインインターフェイス（CLI）"クラスタ、ノード、SVMなどをを使用して操作できるテキストベースのインターフェイスです"コマンド"。CLIコマンドはに基づいて使用でき"ロールタイプ"ます。ONTAP CLIには、SSHまたはクラスタ内のノードへのコンソール接続を介してアクセスできます。

ONTAP REST API

ONTAP 9.6以降では、プログラムを使用してクラスタ処理を管理および自動化できるRESTful APIにアクセスできます。APIを使用して、ボリューム、Snapshot、アグリゲートの作成と管理、クラスタのパフォーマンスの監視など、ONTAPのさまざまな管理タスクを実行します。ONTAP REST APIには、curlなどのユーティリティを使用するか、Python、PowerShell、Javaなど、RESTクライアントをサポートする任意のプログラミング言語を使用して直接アクセスできます。 "詳細"です。

ONTAPIは、ONTAP REST APIに先行する独自のONTAP APIです。ONTAPIを使用している場合は、 "ONTAP REST APIへの移行" 。

NetAppのツールキットとフレームワーク

NetAppには、ONTAP REST APIを抽象化し、自動化コードの作成を容易にする特定の開発言語および環境用のクライアントツールキットが用意されています。https://docs.netapp.com/us-en/ontap-automation/get-started/ontap_automation_options.html#client-software-toolkits["詳細"^]です。

これらのツールキットに加えて、フレームワークを使用して自動化コードを作成および展開できます。 "詳細"です。

ONTAP System Manager とNetAppコンソールを統合する

NetAppコンソールの System Manager を使用して、 ONTAP 9.10.1 以降のリリースを管理できます。この統合により、使い慣れた System Manager ユーザー インターフェイスを維持しながら、統合されたコントロール プレーンを使用してハイブリッド マルチクラウド インフラストラクチャを効率的に監視できます。

コンソールを使用すると、クラウド ストレージ (Cloud Volumes ONTAPなど) を作成および管理したり、NetAppデータ サービス (Cloud Backup など) を使用したり、多数のオンプレミスおよびエッジ ストレージ デバイスを制御したりできます。

コンソールでは、クラスターを検出して管理するための 2 つの方法が提供されています。

- System Manager による管理のための直接検出 (ONTAP 9.12.1 以降)
- コンソール エージェントによる検出。

コンソール エージェントは、環境にインストールされるソフトウェアです。これにより、System Manager を通じて管理機能にアクセスし、データ レプリケーション、バックアップとリカバリ、データ分類、データ階層化などの機能を提供するNetAppクラウド サービスにアクセスできるようになります。

詳細はこちら"NetAppコンソールを使用したオンプレミスのONTAPクラスタ管理" 。

手順

1. NetAppコンソールにログインします。
   a. コンソール ログインがある場合はそれを使用します。
   b. 初めての場合は、 「NetAppサポート サイトの資格情報を使用してログイン」を選択し、コンソール ログイン ページで資格情報を入力します。
2. コンソール エージェントまたは直接検出を使用して、コンソールでオンプレミス クラスターを検出します。詳細については、リンク: オンプレミスのONTAPクラスターの検出 を参照してください。
   a. 。 "直接検出されたクラスターを管理する" 。
   b. 。 "コンソールエージェントで検出されたクラスターを管理する" 。
3. System Manager を使用してオンプレミス クラスターを管理します。 [作業環境システム] ページでクラスターを選択し、[サービス] リストから [システム マネージャー] をクリックします。
   a. 詳細はこちら"直接検出されたクラスターを管理する" 。
   b. 。 "コンソールエージェントで検出されたクラスターを管理する" 。

NetAppコンソールとONTAP 9.12.1

注: ONTAP 9.12.1 を使用している場合は、 NetAppコンソールを試すように求めるメッセージが表示されます。

+ クラスターがNetAppコンソールに接続されている場合は、ログイン プロンプトが表示されます。

1. * NetAppコンソールに進む* をクリックして、コンソールへのリンクに進みます。

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

2. コンソールのログイン ページで、* NetAppサポート サイトの資格情報を使用してログイン* を選択し、資格情報を入力します。

   すでにコンソールを使用しており、メールとパスワードを使用してログインしている場合は、代わりにそのログイン オプションを引き続き使用する必要があります。

   "NetAppコンソールへのログインの詳細" 。

3. プロンプトが表示されたら、新しいNetAppコンソール アカウントの名前を入力します。

ほとんどの場合、コンソールはクラスターのデータに基づいて自動的にアカウントを作成します。

4. クラスタのクラスタ管理者のクレデンシャルを入力します。

結果

System Manager が表示され、コンソールからクラスターを管理できるようになります。

NetAppコンソールの詳細はこちら

- "NetAppコンソールの概要"
- "NetAppコンソールからNetApp AFFおよびFASシステムを管理します"

クラスタストレエシ

ONTAP の現在のバージョンは、もともとはネットアップのスケールアウトクラスタストレージアーキテクチャ用に開発されたものです。これは、ONTAPのデータセンター実装で一般的に使用されるアーキテクチャです。この実装ではONTAPのほとんどの機能が実行されるため、ONTAPテクノロジを構成する概念の理解から始めることをお勧めします。

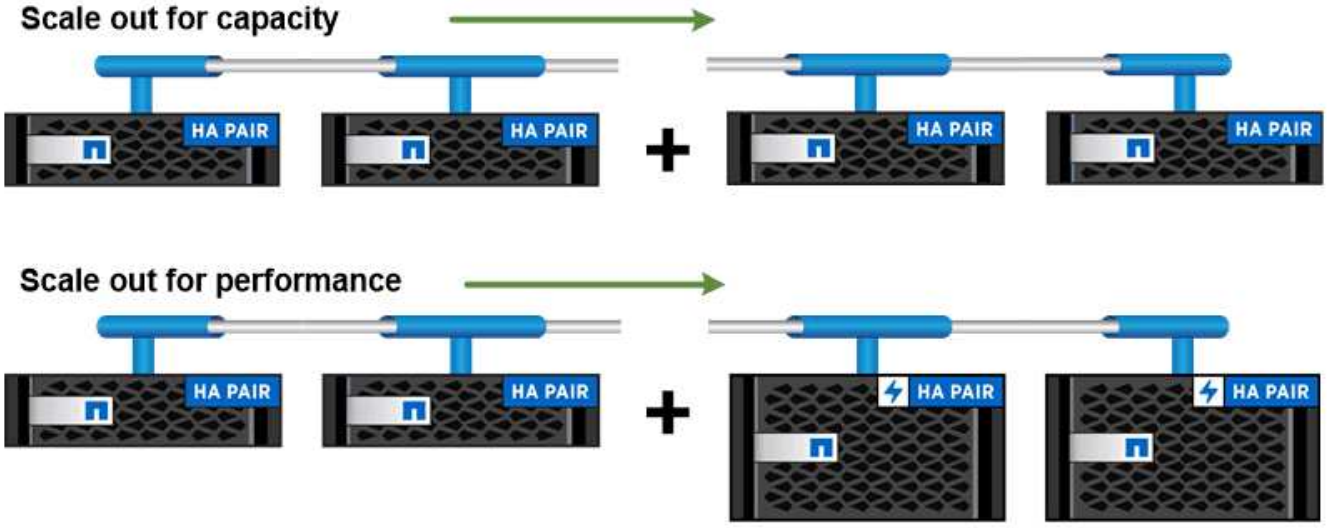
データセンターアーキテクチャでは通常、 ONTAPデータ管理ソフトウェアを実行する専用のAFF、 ASA 、またはFASシステムが採用されます。各コントローラ、そのストレージ、ネットワーク接続、そしてコントローラ上で実行されるONTAPインスタンスは、_ノード_と呼ばれます。

ノードはハイアベイラビリティ（HA）用にペアリングされます。これらのペア（SANの場合は最大12ノード、NASの場合は最大24ノード）を合わせてクラスタを構成します。ノードは、専用のプライベートクラスタインターコネクトを介して相互に通信します。

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

HAペアの各ノードで使用するストレージアレイモデルは同じでなければなりません。それ以外の場合は、サポートされている任意のコントローラを組み合わせて使用できます。スケールアウトできるのは、同等のストレージアレイモデルを使用するノードを追加して容量を増やすか、ハイエンドのストレージアレイを使用するノードを追加してパフォーマンスを高めることです。

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



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

ハイアベイラビリティペア

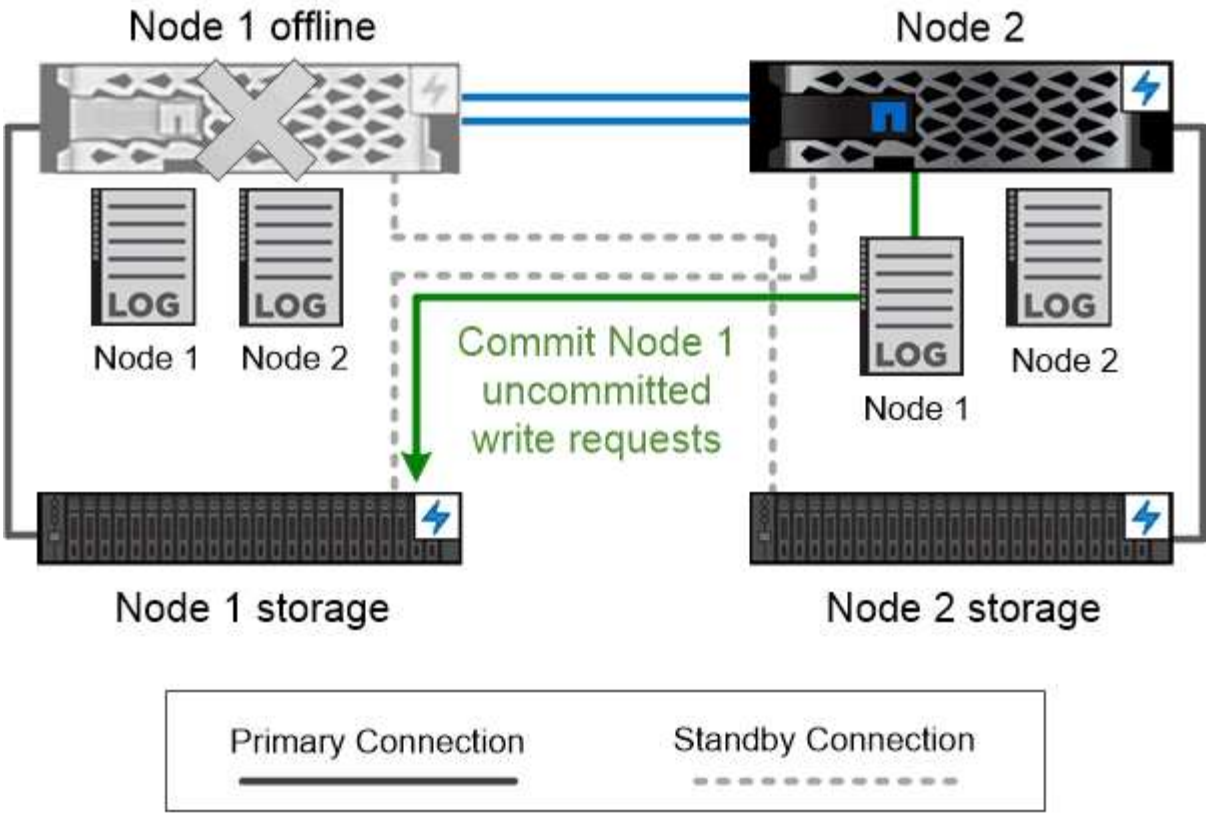
クラスタノードは、フォールトトレランスとノンストップオペレーションを実現するために、 _high-availability （ HA ）ペア _ で構成されます。ノードに障害が発生した場合や定期的なメンテナンスのためにノードを停止する必要がある場合、パートナーはそのストレージをテイクオーバーしてデータの提供を継続できます。ノードがオンラインに戻ったときに、 partner_ギ ブバック _storage を提供します。

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

HAペアは、フォールト トレラントなノードです。ペアになっているノードがさまざまな方法で通信し、パートナーが機能しているかを継続的にチェックしたり、パートナーの不揮発性メモリのログ データをミラーリングしたりできます。一方のノードへの書き込み要求が発生した場合、両方のノードのNVRAMに要求が記録されたのち、クライアントまたはホストに応答が返されます。フェイルオーバーの際は、障害が発生したノードのコミットされていない書き込み要求が稼働しているパートナーによってディスクにコミットされてデータの一貫性が維持されます。存続しているノードは、以前は障害が発生したノードのNVRAMのミラーとして機能していたNVRAMパーティションへの書き込みを記録し続けます。

もう一方のコントローラのストレージメディアへの接続により、テイクオーバー時に各ノードがもう一方のストレージにアクセスできるようになります。ネットワークパスのフェイルオーバーメカニズムにより、クライアントとホストは稼働しているノードと引き続き通信できます。

可用性を確保するには、フェイルオーバー時の追加のワークロードに対応できるように、どちらかのノードのパフォーマンス容量利用率を50%に抑える必要があります。同じ理由で、1つのノードに設定できるNAS仮想ネットワークインターフェイスの最大数の50%を超えないようにすることもできます。



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

*_ 仮想 ONTAP 実装でのテイクオーバーとギブバック _ *

ONTAP Selectのような仮想化された「shared-nothing」 ONTAP実装では、ノード間でストレージは共有されません。一方のノードが停止した場合、そのノードのデータの同期ミラーリングされたコピーを使用してパートナーがデータの提供を継続します。パートナーはノードのストレージはテイクオーバーせず、データ提供機能だけをテイクオーバーします。

AutoSupportとデジタルアドバイザ

ONTAPは、Webポータルとモバイルアプリを使用して、人工知能によるシステムの監視とレポートを提供します。ONTAPのAutoSupportコンポーネントは、Active IQデジタルアドバイザ（デジタルアドバイザとも呼ばれる）によって分析されるテレメトリを送信します。

Digital Advisorは、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体にわたってデータインフラを最適化します。SupportEdgeと有効な契約を結んでいるNetAppのすべてのお客様が、デジタルアドバイザによるデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Digital Advisorでできることは次のとおりです。

- アップグレードを計画する。Digital Advisorは、新しいバージョンのONTAPにアップグレードすることで解決できる環境内の問題を特定し、Upgrade Advisorコンポーネントがアップグレードの計画を支援します。
- システムの健全性を表示します。デジタルアドバイザのダッシュボードが健全性に関する問題を報告し、問題の修正を支援します。システム容量を監視して、ストレージスペースが不足しないようにします。
- パフォーマンスの管理Digital Advisorでは、System Managerよりも長い期間のシステムパフォーマンスが表示されます。パフォーマンスに影響している構成やシステムの問題を特定します。
- 効率を最大化Storage Efficiencyの指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定できます。
- インベントリと構成を表示します。Digital Advisorは、完全なインベントリおよびソフトウェアとハードウェアの構成情報を表示します。サービス契約の有効期限を確認して、サポート期間を維持できます。

関連情報

"NetAppのドキュメント：デジタルアドバイザ"

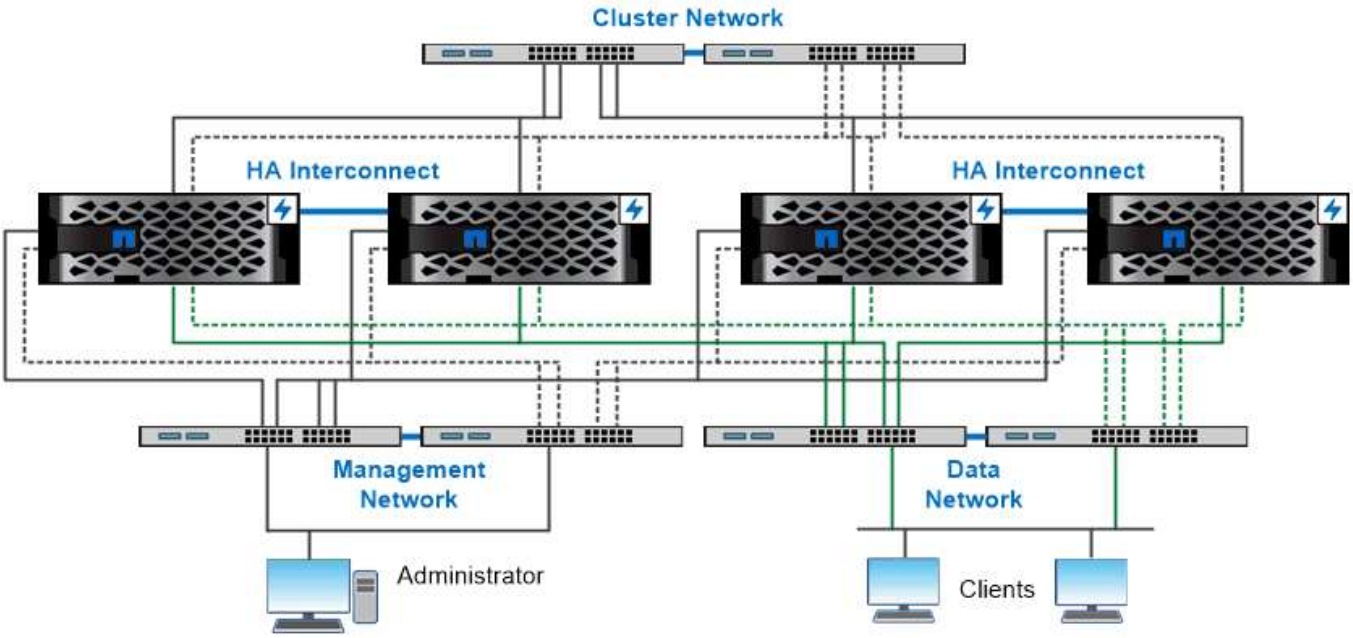
"Digital Advisorを起動"

"SupportEdgeサービス"

ネットワークアーキテクチャ

ネットワークアーキテクチャの概要

通常、ONTAPデータセンター実装のネットワークアーキテクチャは、クラスタインターコネクト、クラスタ管理用の管理ネットワーク、およびデータネットワークで構成されます。NIC（ネットワークインターフェイスカード）は、イーサネット接続用の物理ポートを提供します。HBA（ホストバスアダプタ）は、FC接続用の物理ポートを提供します。



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

論理ポート

各ノードに搭載されている物理ポートに加え、 _logical ports_を 使用してネットワークトラフィックを管理できます。論理ポートはインターフェイスグループまたはVLANです。

インターフェイスグループ

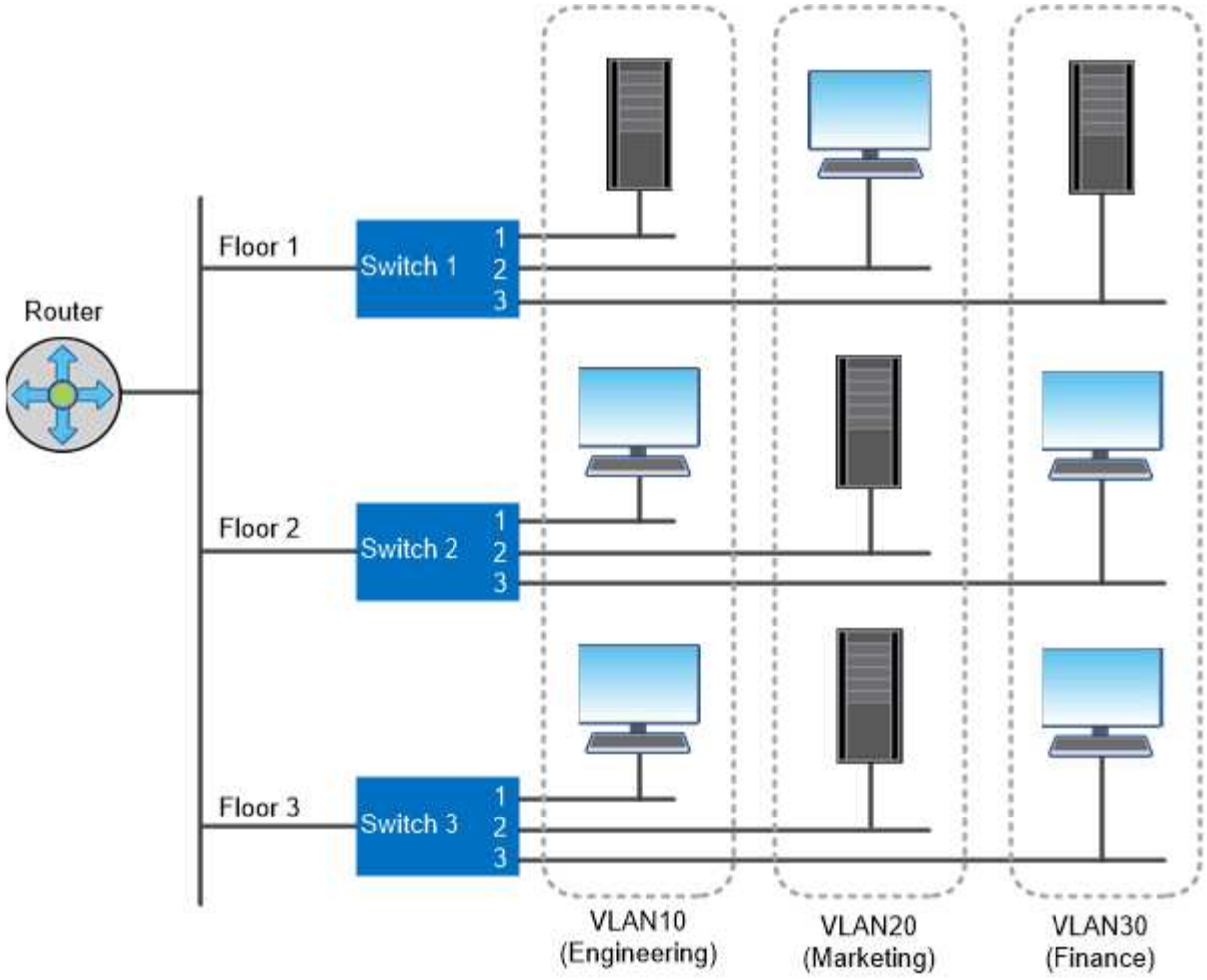
_インタフェースグループ_複数の物理ポートを1つの論理「トランクポート」に結合します。1つのスロットで障害が発生してビジネスクリティカルなトラフィックが停止しないようにするには、異なるPCIスロットのNICのポートで構成されるインターフェイスグループを作成します。

インターフェイスグループには、シングルモード、マルチモード、またはダイナミックマルチモードがあります。各モードでは、フォールトトレランスのレベルが異なります。どちらのタイプのマルチモードインターフェイスグループも、ネットワークトラフィックの負荷分散に使用できます。

VLAN

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

エンドステーションは、エンジニアリングやマーケティングなどの部門ごと、またはrelease1やrelease2などのプロジェクトごとにグループ化できます。VLANではエンドステーションの物理的な近接性は無関係であるため、エンドステーションは地理的に離れた場所に配置できます。



You can use VLANs to segregate traffic by department.

業界標準のネットワークテクノロジのサポート

ONTAPは、すべての主要な業界標準ネットワークテクノロジをサポートしています。主なテクノロジには、IPspace、DNSロードバランシング、SNMPトラップなどがあります。

ブロードキャストドメイン、フェイルオーバーグループ、およびサブネットについては、をNASパスのフェイルオーバー参照してください。

IPspace

IPspace を使用すると、クラスタ内の仮想データサーバごとに個別の IP アドレススペースを作成できます。これにより、管理上分離されたネットワークドメインに属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

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

DNSロオトハランシンク

DNS ロードバランシング _ を使用すると、使用可能なポートにユーザネットワークトラフィックを分散できます。DNSサーバは、インターフェイスにマウントされているクライアントの数に基づいて、トラフィック用のネットワークインターフェイスを動的に選択します。

SNMPトラツフ

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

FIPS準拠

ONTAPは、すべてのSSL接続で連邦情報処理標準（FIPS）140-2に準拠しています。SSL FIPSモードをオンまたはオフにしたり、SSLプロトコルをグローバルに設定したり、RC4などの弱い暗号を無効にしたりできます。

RDMAの概要

ONTAPのリモート ダイレクト メモリ アクセス（RDMA）ソリューションは、レイテンシの影響を受けやすい広帯域幅のワークロードをサポートします。RDMAを使用すると、ストレージ システムとホスト システムのメモリ間でデータが直接コピーされるため、CPUの中断やオーバーヘッドを回避できます。

NFS over RDMA

ONTAP 9 .10.1以降では、サポート対象のNVIDIA GPUを搭載したホストでGPUアクセラレーションワークロードにNVIDIA GPUDirect Storageを使用できるように設定できます"NFS over RDMA"。

RDMA は SMB プロトコルではサポートされていません。

クラスタインターコネクトRDMA

クラスタインターコネクトRDMAは、レイテンシを低減し、フェイルオーバー時間を短縮し、クラスタ内のノード間の通信を高速化します。

X1151Aクラスタ NICを使用する場合、ONTAP 9 .10.1以降では、特定のハードウェアシステムでクラスタインターコネクトRDMAがサポートされます。X91153A NICでは、ONTAP 9 13.1以降でクラスタインターコネクトRDMAもサポートされます。各ONTAPリリースでサポートされるシステムについては、表を参照してください。

システム	サポートされる**ONTAP**バージョン
• AFF A50用 • AFF A30用 • AFF A20用 • AFF C80用 • AFF C60用 • AFF C30用 • ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1以降
• AFF A1K用 • AFF A90用 • AFF A70用 • ASA A1K • ASA A90 • ASA A70 • FAS90 • FAS70	ONTAP 9.15.1以降
• AFF A900用 • ASA A900 • FAS9500	ONTAP 9.13.1以降
• AFF A400 • ASA A400	ONTAP 9.10.1以降

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

クライアントプロトコル

ONTAPは、業界標準の主要なクライアントプロトコル（NFS、SMB、FC、FCoE、iSCSI、 NVMe、S3、

NFS

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

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

ファイルアクセスは、UNIX形式のアクセス権、NTFS形式のアクセス権、またはその両方を組み合わせて制御できます。

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

SMB

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

SMB 1.0も使用できますが、ONTAP 9 .3以降のリリースではデフォルトで無効になっています。

FC

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

LUNは仮想ディスクを表し、1つ以上のLUNがONTAPボリュームに格納されます。FC、FCoE、およびiSCSIの各プロトコルを使用して同じLUNにアクセスできますが、複数のクライアントから同じLUNにアクセスできるのは、それらのクライアントが書き込みの競合を防止するクラスタに属している場合のみです。

FCoE

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

iSCSI

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

NVMe/FCとNVMe/TCP

NVMeは、フラッシュベースのストレージと連携するように特別に設計された最新のブロックプロトコルです。スケーラブルなセッションを提供し、レイテンシの大幅な低減と並列処理能力の向上を実現するため、インメモリデータベースや分析など、低レイテンシで高スループットのアプリケーションに適しています。

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

S3

ONTAP 9 .8以降では、ONTAPクラスタでONTAP Simple Storage Service（S3）サーバを有効にすることで、S3バケットを使用してオブジェクトストレージにデータを提供できるようになりました。

ONTAPでは、S3オブジェクトストレージを提供する次の2つのオンプレミスユースケースシナリオがサポートされています。

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

> ONTAP S3は、既存のクラスタで追加のハードウェアや管理作業を行わずにS3機能を利用する場合に適しています。300TBを超える環境では、引き続きNetApp StorageGRIDソフトウェアがNetAppのオブジェクトストレージ向け主力ソリューションとなります。詳細はこちらをご覧ください "StorageGRID"。

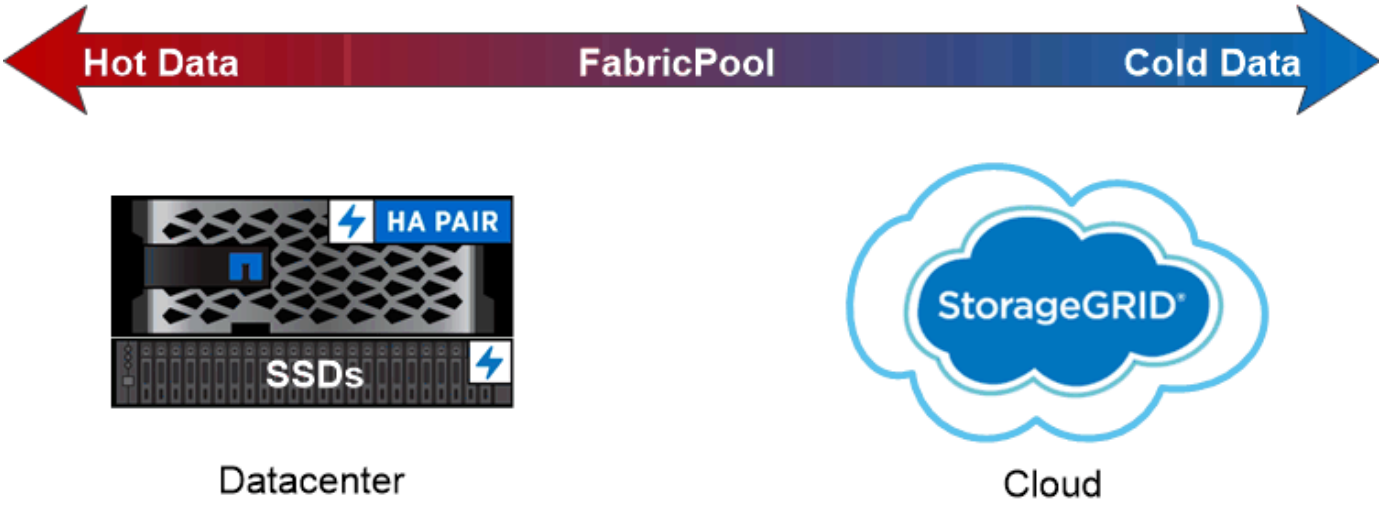
ディスクとローカル階層

ディスクと**ONTAP**ローカル階層

_Local Tiers_は_aggregates_とも呼ばれ、ノードで管理されるディスクの論理コンテナです。ローカル階層を使用すると、パフォーマンス要件が異なるワークロードを分離したり、アクセスパターンが異なるデータを階層化したり、規制要件に準拠するためにデータを分離したりできます。

> ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。

- レイテンシを最小限に抑え、パフォーマンスを最大限に高める必要があるビジネスクリティカルなアプリケーションの場合は、SSDのみで構成されるローカル階層を作成します。
- アクセスパターンに応じてデータを階層化する場合は、_hybrid local tier _を作成し、作業データセットにはフラッシュを導入して高性能なキャッシュを利用しながら、アクセス頻度が低いデータには低コストのHDDやオブジェクトストレージを使用することができます。
  - は、"Flash Pool _"SSDとHDDの両方で構成されます。
  - は"_ FabricPool _"、オブジェクトストアが接続されたオールSSDローカル階層で構成されます。
- 規制要件に準拠するためにアクティブなデータからアーカイブデータを分離する必要がある場合は、大容量HDDまたはパフォーマンスHDDと大容量HDDで構成されるローカル階層を使用できます。



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

MetroCluster構成でのローカル階層の使用

MetroCluster構成を使用している場合は、ドキュメントの初期設定手順、およびローカル階層とディスク管理に関するガイドラインに従って"MetroCluster"ください。

関連情報

- "ローカル階層の管理"
- "ディスクの管理"
- "RAID構成の管理"
- "Flash Pool階層の管理"
- "FabricPoolクラウド階層の管理"

ONTAP RAIDグループとローカル階層

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

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

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

サイジングに関する推奨事項の上位にRAIDグループを作成することで、パリティディスクのオーバーヘッドコストを分散させることができます。これは特に、容量ドライブよりもはるかに信頼性が高いSSDの場合に当

てはまります。HDDを使用するローカル階層の場合は、ディスクストレージを最大化する必要性と、大規模なRAIDグループのリビルド時間が長くなるなどの相反する要因のバランスを取る必要があります。

ミラーされたローカル階層とミラーされないローカル階層

raid_raid_を使用するONTAPと、異なるSyncMirrorグループに格納されているコピー（*plexes*）のローカル階層のデータを同期的にミラーリングできます。プレックスを使用すると、RAIDタイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や、RAIDグループのディスクへの接続が失われた場合でも、データ損失を防ぐことができます。

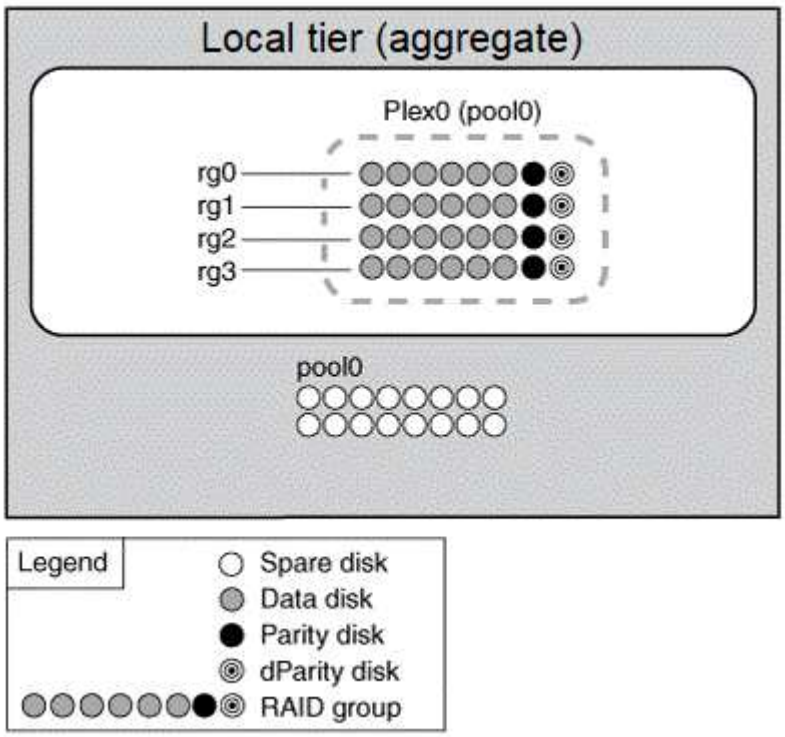
ローカル層を作成するときに、ローカル層をミラーリングするかミラーリングしないかを指定できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

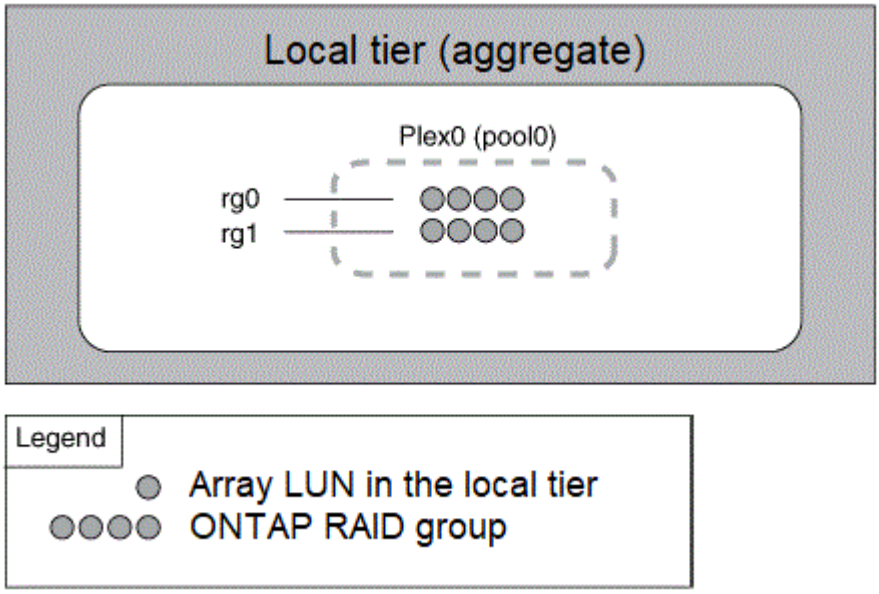
ミラーされていないローカル階層の仕組み

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

次の図は、ディスクで構成され、1つのプレックスにグループ化された、ミラーされていないローカル階層を示しています。ローカル階層には、rg0、rg1、rg2、rg3の4つのRAIDグループがあります。各RAIDグループには、6本のデータディスク、1本のパリティディスク、および1本のdparity（ダブルパリティ）ディスクがあります。ローカル階層で使用されるすべてのディスクは'同じプールであるpool0から提供されます



次の図は、アレイLUNで構成されたミラーされていないローカル階層を1つのプレックスにグループ化した状態を示しています。このノードには、rg0とrg1の2つのRAIDグループがあります。ローカル階層で使用されるすべてのアレイLUNは'同じプールであるpool0から提供されます



ミラーされたローカル階層の機能

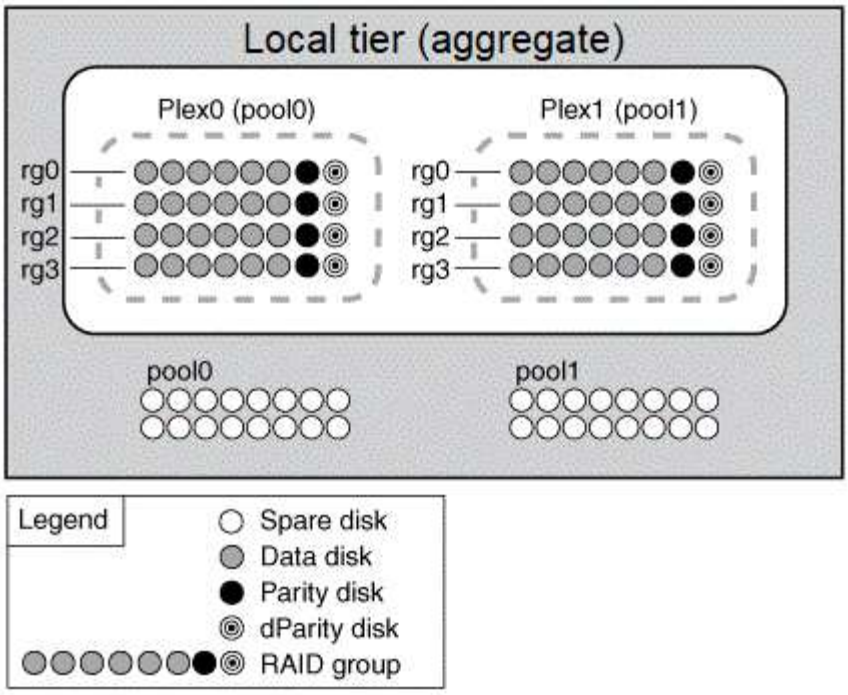
ミラーされたローカル階層には、2つの_プレックス_（データのコピー）があります。これらの階層では、SyncMirror機能を使用してデータを複製し、冗長性を確保します。

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

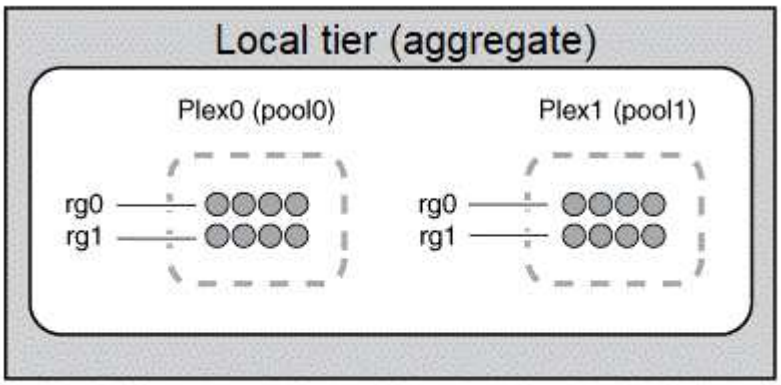
この構成では、ローカル階層のRAIDレベルで保護されるディスク数よりも多くのディスクで障害が発生した場合や接続が失われた場合に、障害の原因を修正しながら影響を受けないプレックスがデータの提供を継続するため、データ損失に対する保護が強化されます。問題のあるプレックスが修正されると、2つのプレックスが再同期され、ミラー関係が再確立されます。

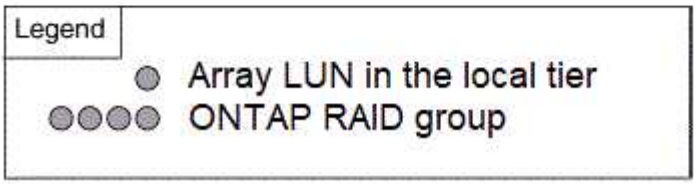
システム上のディスクとアレイLUNは、との `pool1`2つのプールに分割されます `pool0`。plex0はpool0からストレージを取得し、plex1はpool1からストレージを取得します。

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



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





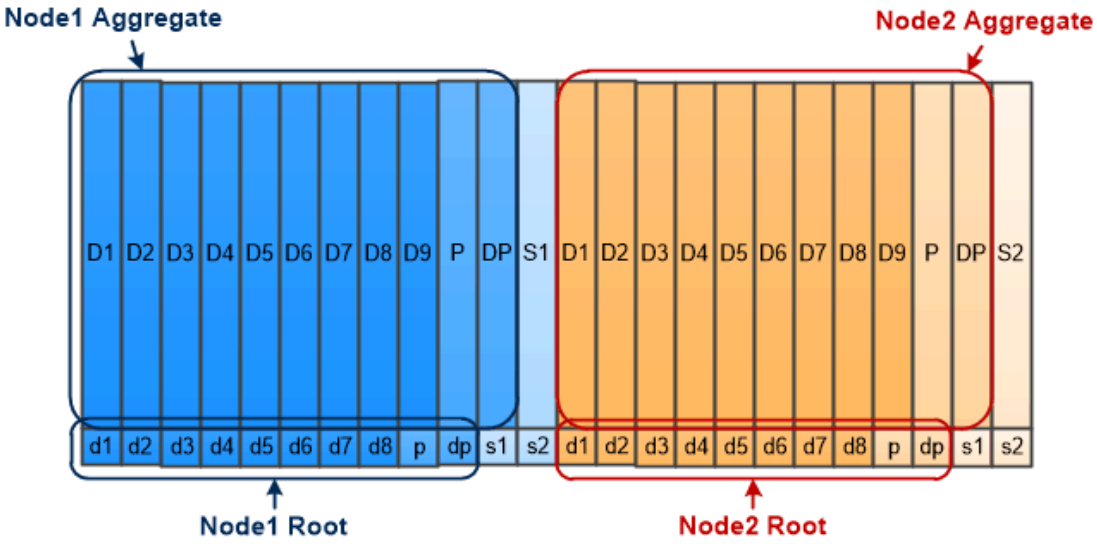
ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。

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

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

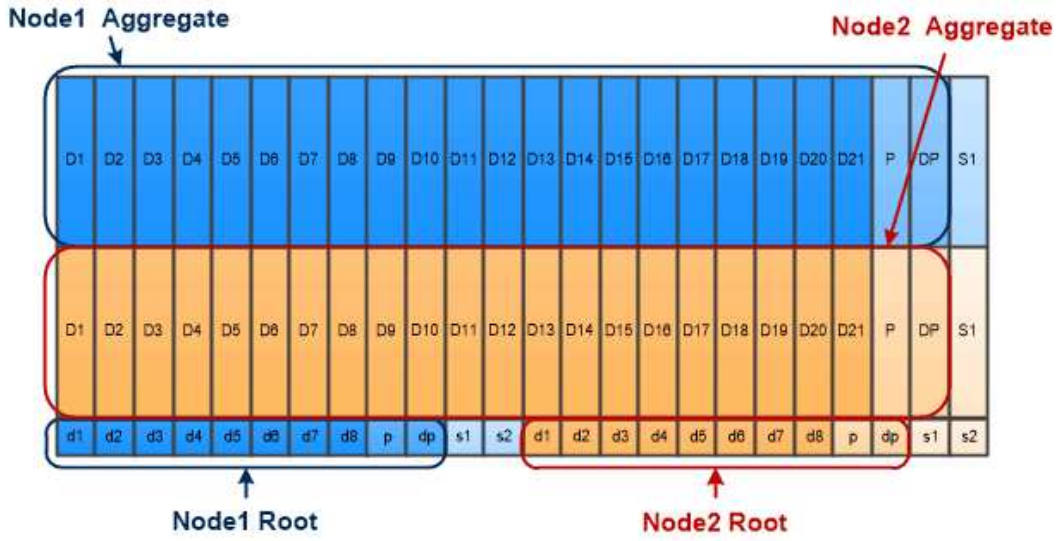
RAID-DPタイプのルートアグリゲートは、通常、1本のデータディスクと2本のパリティディスクで構成されます。これは、アグリゲート内の各 RAID グループ用に 2 つのディスクがパリティディスクとしてすでにリザーブされている場合、ストレージシステムファイルの料金を支払う「パリティ税」として相当します。

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



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

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



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

どちらのタイプのルート / データパーティショニングも、 ONTAP のアドバンストドライブパーティショニング（ ADP ）機能の一部です。どちらも工場出荷時に構成され、エントリレベルのFAS2xxx、FAS9000、FAS8200、FAS80xx、およびAFFシステムではルート/データパーティショニング、AFFシステムでのみルート/データ/データパーティショニングが使用されます。

詳細については、をご覧ください "アドバンストドライブパーティショニング"。

ドライブがパーティショニングされてルートアグリゲート用に使用される

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

ルートアグリゲートに使用されているドライブの数を把握しておくと、ルートパーティション用にリザーブされているドライブ容量と、データアグリゲートで使用可能な容量を判断するのに役立ちます。

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

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

All Flash FASプラットフォームおよびSSDのみが接続されたFASプラットフォームでは、システム初期化時にコントローラに接続されたすべてのドライブがパーティショニングされます（ノードあたり最大24個）。システムの構成後に追加されたドライブはパーティショニングされません。

ボリューム、**qtree**、ファイル、**LUN**

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

1つのアグリゲートに複数のFlexVolを割り当てて、それぞれ異なるアプリケーションやサービス専用にすることができます。FlexVol volumeの拡張と縮小、FlexVol volumeの移動、FlexVol volumeの効率的なコピーの作成が可能です。qtree _ を使用して FlexVol ボリュームをより管理しやすい単位にパーティショニングした

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

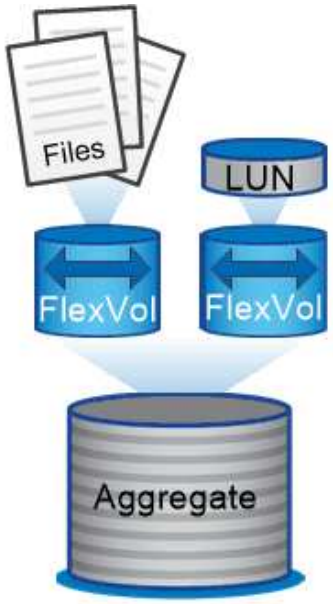
ボリュームには、NAS環境ではファイルシステムが格納され、SAN環境ではLUNが格納されます。LUN （論理ユニット番号）は、 SAN プロトコルによって対処される a_logical unit_ というデバイスの識別子です。

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

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

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

これらのボリュームはデータの格納には使用できません。



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

*_ FlexGroup volumes _ *

企業によっては、単一のネームスペースにペタバイト規模のストレージが必要になる場合があります。これは、FlexVol volumeの100TB容量をはるかに超えています。

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

FlexGroupボリュームの場合、メンテナンスや管理のオーバーヘッドは必要ありません。FlexGroupボリュームを作成してNASクライアントと共有するだけです。残りはONTAPが行います。

ストレージ仮想化

ストレージ仮想化の概要

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

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

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

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

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

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

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

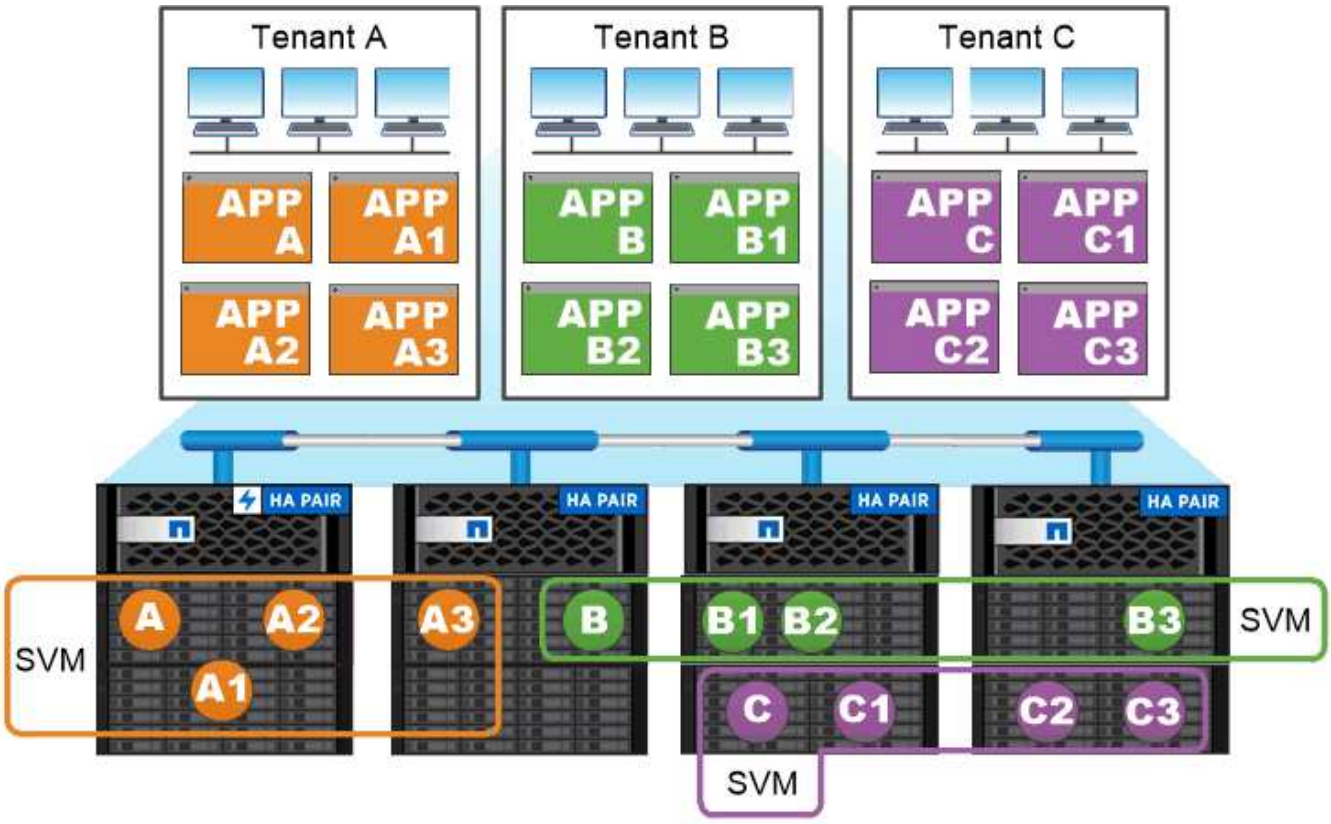
ONTAPがミドルウェアに似ている理由

ONTAPがストレージ管理タスクに使用する論理オブジェクトは、適切に設計されたミドルウェアパッケージでよく知られている目標を達成します。具体的には、管理者を低レベルの実装の詳細から保護し、ノードやポートなどの物理特性の変更から構成を切り離すことです。管理者は、ストレージインフラ全体ではなくいくつかのフィールドを再設定して、ボリュームやLIFを簡単に移動できるようにすることが基本的な考え方です。

SVMのユースケース

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

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



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

クラスタと**SVM**の管理

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

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

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

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

*_ ロールベースアクセス制御 (RBAC) _ *

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

ネームスペースとジャンクションポイント

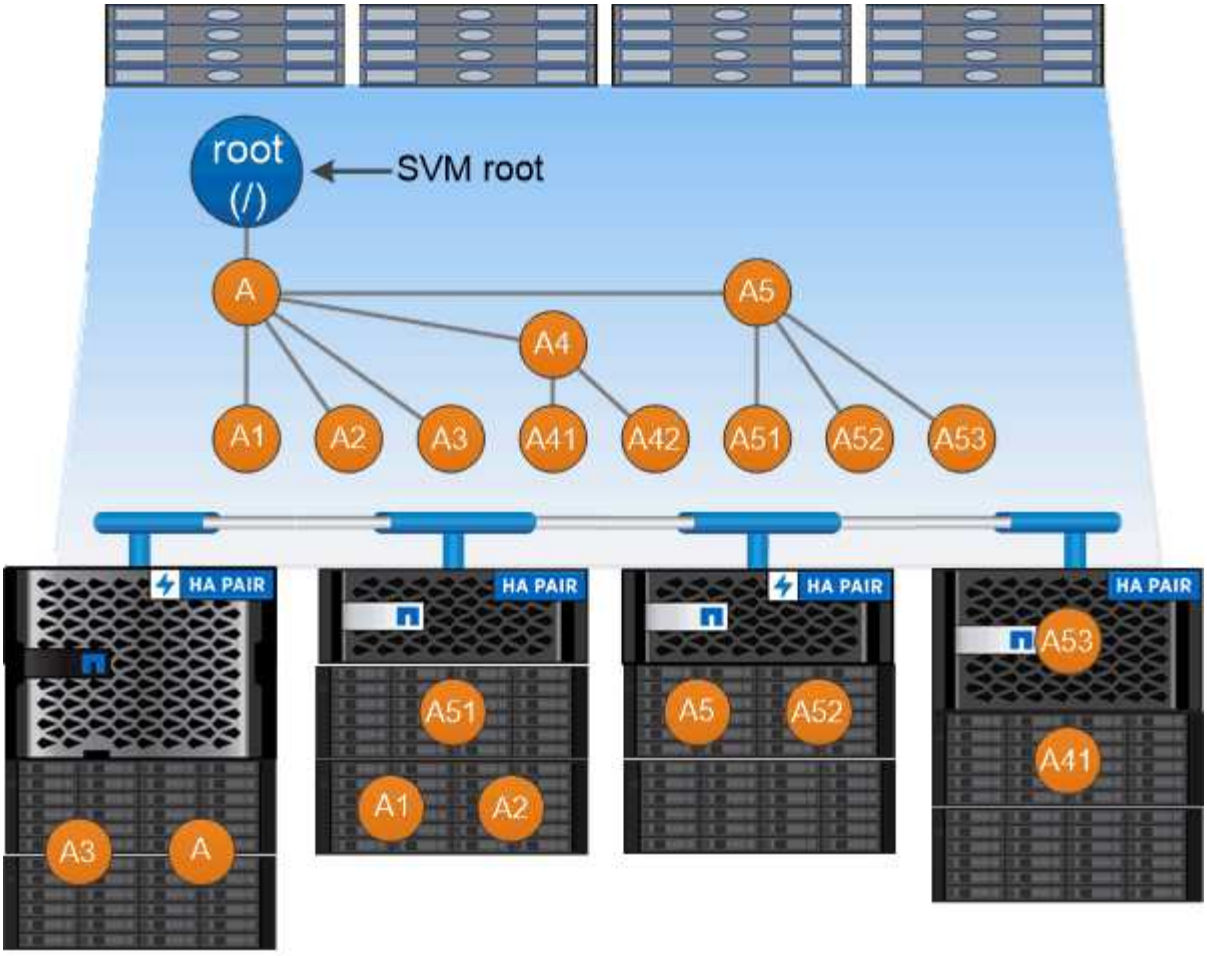
nas_namespace _ は、 _junction points_to によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限があるクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

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

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

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

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



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

例

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

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

パスのフェイルオーバー

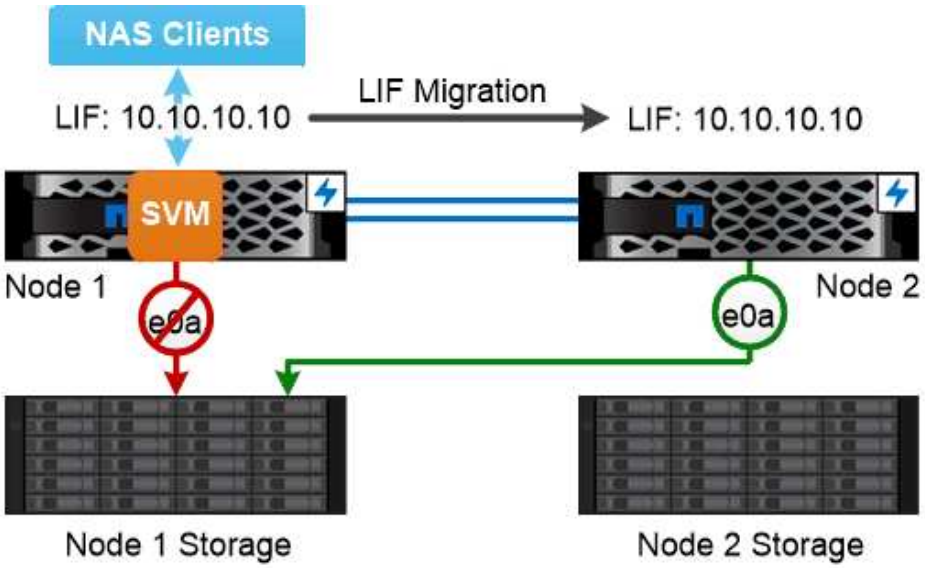
パスノフェイルオーバーノガイヨウ

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

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

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

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



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

- _ サブネット _ *

a_subnet_ は、ブロードキャストドメイン内の IP アドレスのブロックを予約します。これらのアドレスは同じレイヤ3ネットワークに属し、LIFの作成時にブロードキャストドメイン内のポートに割り当てられます。LIFアドレスを定義するときに、IPアドレスとネットワークマスクを指定するよりもサブネット名を指定する方が簡単でエラーも少なくなります。

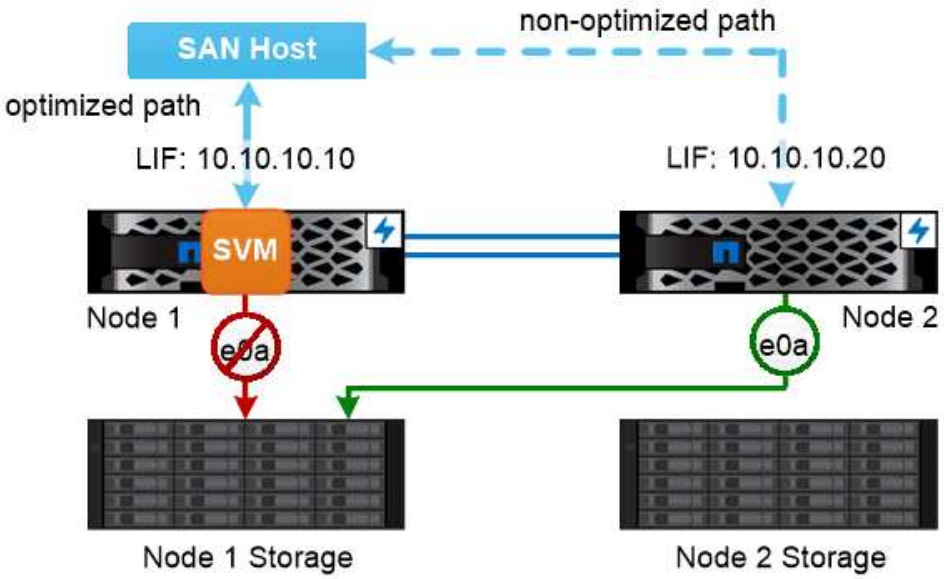
SANパスのフェイルオーバー

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

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

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

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



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

*_ SAN 環境でのボリュームの移動 _ *

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

つまり、ボリュームを別のHAペアのノードに移動する場合は、デスティネーションHAペアのレポートノードをLUNマッピングに追加する必要があります。その後、MPIOセットアップで新しいパスを指定できます。ボリュームの移動が完了したら、ソースHAペアのレポートノードをマッピングから削除できます。

ノードでの作業量が使用可能なリソースを超えると、ワークロードのパフォーマンスがレイテンシの影響を受け始めます。ノードが過負荷になった場合は、使用可能なリソースを増やす（ディスクまたはCPUをアップグレードする）か、負荷を軽減する（必要に応じてボリュームまたはLUNを別のノードに移動する）ことで対処できます。

また、ONTAP _ storage Quality of Service（QoS）_を使用して、重要なワークロードのパフォーマンスが競合するワークロードによって低下しないようにすることもできます。

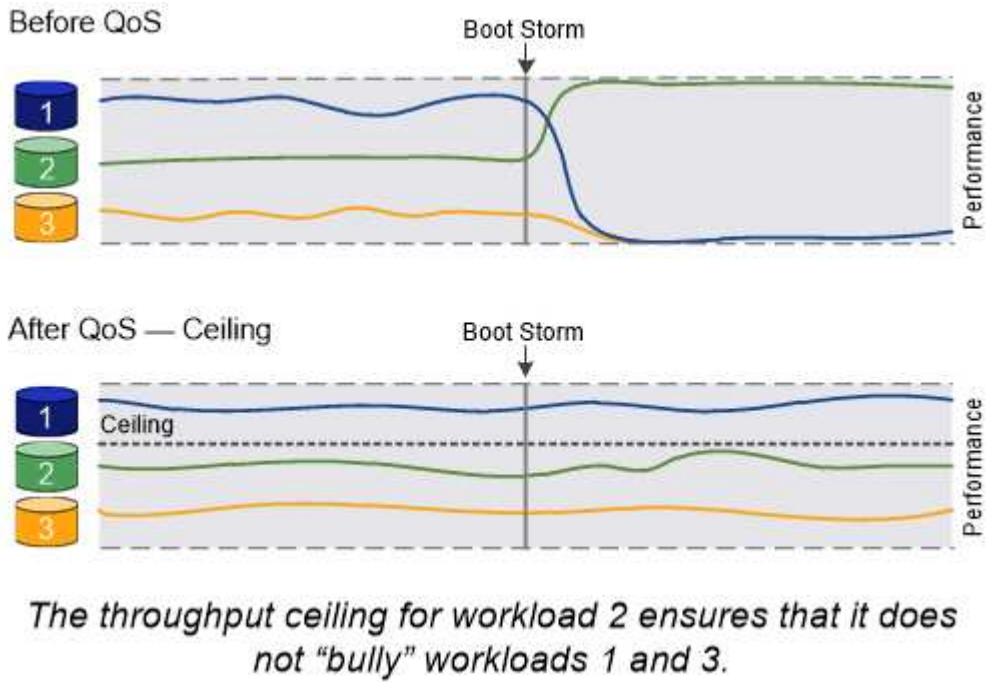
- 競合するワークロードに対して QoS スループットの上限を設定すると、そのワークロードによるシステムリソースへの影響を制限できます（最大 QoS ）。
- 重要なワークロードに対して QoS スループットの下限を設定すると、競合するワークロードによる要求に関係なく、必要な最小スループットを確保できます（最小 QoS ）。
- 同じワークロードに対してQoSの上限と下限を設定できます。

スループットの上限

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

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

ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を10%までは超えることができます。バーストに対処するために、上限を50%まで超過することがあります。



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

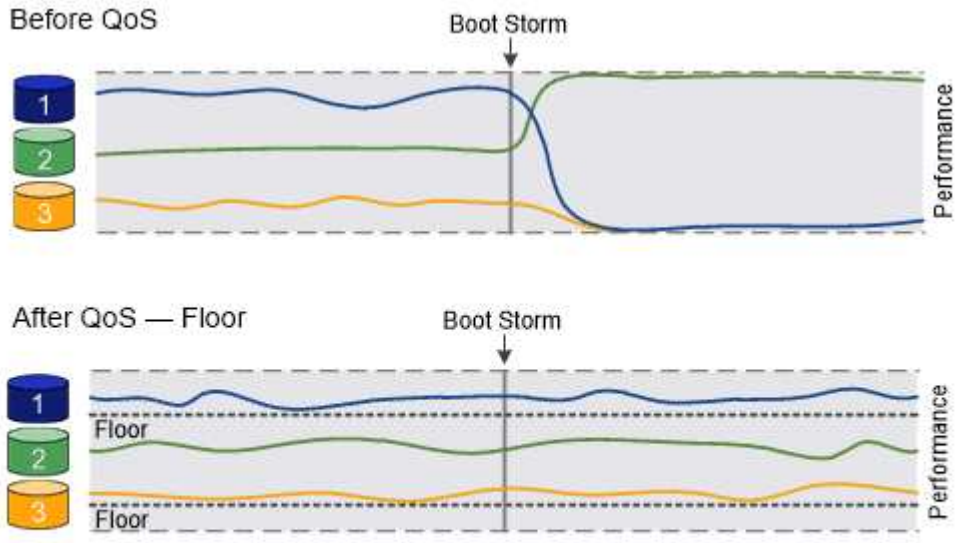
スループットの下限

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

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

ワークロードは、ボリューム、LUN、またはONTAP 9 .3以降のfileのI/O処理を表します。スループットの下限が定義されたポリシーグループは、SVMには適用できません。下限はポリシーグループの作成時に指定できます。また、ワークロードを監視したあとで指定することもできます。

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



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

アダプティブ**QoS**

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

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

アダプティブQoSは、主にスループットの上限の調整に使用しますが、下限の管理（ワークロードサイズが増加した場合）にも使用できます。ワークロードのサイズは、ストレージオブジェクトに割り当てられたスペー

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

ONTAP 9.5以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9.4以前のスループットの下限ではサポートされません。

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

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

レプリケーション

スナップショット

従来、ONTAPレプリケーションテクノロジはディザスタリカバリ（DR）とデータアーカイブのニーズに対応してきました。クラウドサービスの登場に伴い、ONTAPレプリケーションは、NetAppデータファブリック内のエンドポイント間のデータ転送に適用されるようになりました。これらすべての用途の基盤となるのが、ONTAPのSnapshotテクノロジです。

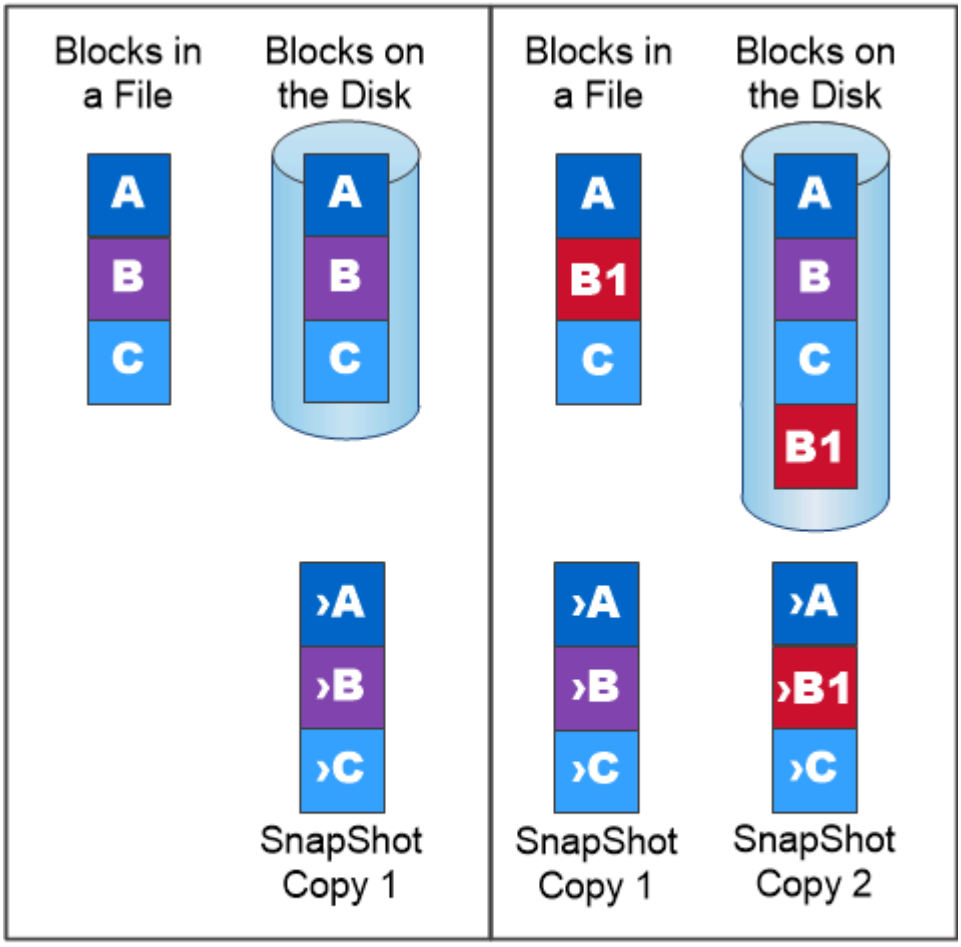
a_snapshot_（旧称_Snapshotコピー_）は、ボリュームのポイントインタイムイメージの読み取り専用です。スナップショットが作成されると、アクティブファイルシステムとスナップショットは同じディスクブロックを参照します。したがって、スナップショットは追加のディスクスペースを使用しません。イメージには最後のSnapshotが作成されてからのファイルへの変更のみが記録されるため、時間の経過とともに消費されるストレージスペースは最小限で済み、パフォーマンスのオーバーヘッドもわずかです。

Snapshotの効率性は、ONTAPの中核となるストレージ仮想化テクノロジである_Write Anywhere File Layout（WAFL）によるものです。_ WAFLは、データベースと同様に、メタデータを使用してディスク上の実際のデータブロックを参照します。ただし、データベースとは異なり、WAFLは既存のブロックを上書きしません。更新されたデータは新しいブロックに書き込まれ、メタデータが変更されます。

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

Snapshotを使用すると、個 々 のファイルやLUNをリカバリしたり、ボリュームの内容全体をリストアしたりできます。ONTAPは、Snapshot内のポインタ情報をディスク上のデータと比較して、ダウンタイムや大幅なパフォーマンスコストを発生させることなく、欠落または破損したオブジェクトを再構築します。

a_snapshotポリシー：ボリュームのSnapshotの作成方法を定義します。このポリシーは、Snapshotを作成するタイミング、保持するコピーの数、Snapshotに名前を付ける方法、およびSnapshotにレプリケーション用のラベルを付ける方法を指定します。たとえば、毎日午前12時10分にSnapshotを1つ作成し、最新の2つのコピーを保持して「daily」（タイムスタンプが付加された）という名前を付け、レプリケーション用に「daily」というラベルを付けることができます。



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

SnapMirrorディザスタリカバリとデータ転送

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

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

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

ONTAP 9 .10.1以降では、SnapMirror S3を使用してS3バケット間のデータ保護関係を作成できます。デスティネーションバケットは、ローカルまたはリモートのONTAPシステムに配置することも、ONTAP以外のシス

テム（StorageGRIDやAWSなど）に配置することもできます。

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

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

ベースライン転送が完了すると、SnapMirrorは新しいSnapshotのみをミラーに転送します。更新は、設定したスケジュールに従って非同期に行われます。保持期間は、ソース上のSnapshotポリシーをミラーリングします。プライマリサイトで災害が発生した場合は最小限のシステム停止でデスティネーションボリュームをアクティブ化し、サービスの復旧後にソースボリュームを再アクティブ化できます。

ベースラインの作成後はSnapMirrorでSnapshotのみが転送されるため、無停止で高速なレプリケーションが可能です。フェイルオーバーのユースケースが示すように、ミラーリングされたストレージからデータを効率的に提供するには、セカンダリシステムのコントローラがプライマリシステムのコントローラと同等またはほぼ同等である必要があります。

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

- _ SnapMirror を使用したデータ転送 _ *

SnapMirrorを使用して、NetAppデータファブリック内のエンドポイント間でデータをレプリケートすることもできます。SnapMirrorポリシーの作成時に、1回限りのレプリケーションと定期的なレプリケーションのどちらかを選択できます。

SnapMirrorクラウドによるオブジェクトストレージへのバックアップ

_ SnapMirror cloud_は、データ保護ワークフローをクラウドに移行したいONTAPユーザ向けに設計されたバックアップおよびリカバリテクノロジです。従来のテープバックアップアーキテクチャから脱却した組織は、長期的なデータ保持とアーカイブの代替リポジトリとしてオブジェクトストレージを使用できます。SnapMirror Cloudは、永久増分バックアップ戦略の一環として、ONTAPからオブジェクトストレージへのレプリケーションを提供します。

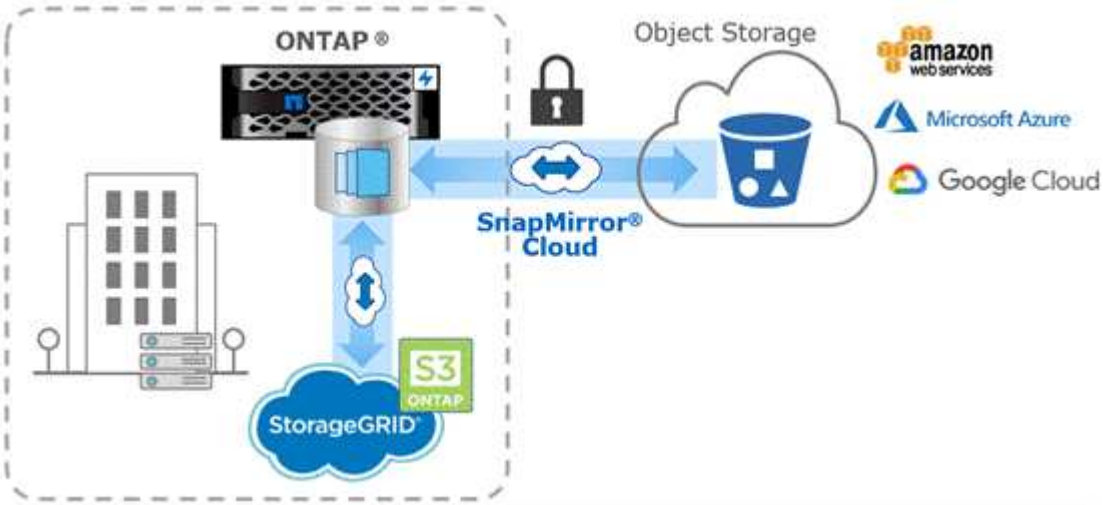
SnapMirrorクラウドレプリケーションは、ONTAPのライセンス機能です。SnapMirrorクラウドは、SnapMirrorレプリケーションテクノロジファミリーの拡張としてONTAP 9.8で導入されました。SnapMirrorはONTAPからONTAPへのバックアップによく使用されますが、SnapMirrorクラウドでは同じレプリケーションエンジンを使用して、ONTAPのSnapshotをS3準拠のオブジェクトストレージバックアップに転送します。

バックアップのユースケースをターゲットにしたSnapMirror Cloudは、長期保持とアーカイブの両方のワークフローをサポートしています。SnapMirrorと同様に、SnapMirrorの初回クラウドバックアップでボリュームのベースライン転送が実行されます。以降のバックアップでは、SnapMirror Cloudによってソースボリュームのスナップショットが生成され、変更されたデータブロックのみを含むSnapshotがオブジェクトストレージターゲットに転送されます。

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

ONTAP System Managerを使用してSnapMirrorクラウド構成を管理するだけでなく、SnapMirrorクラウドバックアップを管理するためのいくつかのオーケストレーションオプションを使用できます。

- SnapMirrorクラウドレプリケーションのサポートを提供する複数のサードパーティバックアップパートナー。参加ベンダーは、から入手でき"ネットアップのブログ"ます。
- ONTAP環境向けのNetAppネイティブ ソリューションであるNetAppバックアップおよびリカバリ
- データ保護ワークフロー向けのカスタムソフトウェアを開発したり、自動化ツールを活用したりするためのAPI



SnapVaultアーカイブ

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

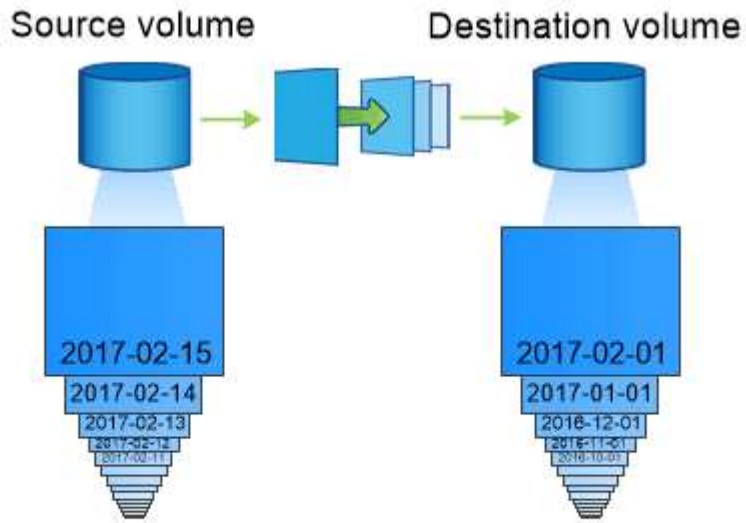
_ SnapVault _は、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのスナップショットレプリケーションを行うために設計されたアーカイブテクノロジです。SnapMirror関係では、通常、ソースボリューム内のSnapshotのみがデスティネーションに含まれますが、SnapVaultデスティネーションでは、より長期間にわたって作成されたポイントインタイムSnapshotが保持されます。

たとえば、ビジネスに関する政府会計規制に準拠するために、データの月次スナップショットを20年間にわたって保持することができます。SnapVaultストレージからデータを提供する必要はないため、デスティネーションシステムでは低速で低コストのディスクを使用できます。

SnapMirrorと同様に、SnapVaultは初回起動時にベースライン転送を実行します。ソースボリュームのSnapshotが作成され、そのコピーおよびコピーが参照するデータブロックがデスティネーションボリュームに転送されます。SnapMirrorとは異なり、SnapVaultではベースラインに古いSnapshotは含まれません。

更新は、設定したスケジュールに従って非同期に行われます。関係のポリシーで定義するルールによって、更新に含める新しいSnapshotと保持するコピーの数が決まります。ポリシーで定義されたラベル（「毎月」など）は、ソースのSnapshotポリシーで定義された1つ以上のラベルと一致する必要があります。そうしないと、レプリケーションが失敗します。

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



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

ONTAP 9 .7以前でのみディスクツーディスクであったSnapMirrorおよびSnapVaultのデータ保護関係に加えて、より低コストで長期的なデータ保持を実現できるバックアップソリューションがいくつか登場しました。

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

ONTAP 9.8以降では、SnapMirror Cloudで、ONTAPインスタンスからオブジェクトストレージエンドポイントへのSnapshotの非同期レプリケーションを実行できます。SnapMirrorのクラウドレプリケーションには、データ保護ワークフローのオーケストレーションと管理を行うための、ライセンスが必要です。SnapMirrorのクラウド関係は、ONTAPシステムからオンプレミスとパブリッククラウドのオブジェクトストレージターゲット（AWS S3、Google Cloud Storage Platform、Microsoft Azure Blob Storageなど）への移行がサポートされ、ベンダーのバックアップソフトウェアで効率性が向上します。サポートされる認定アプリケーションやオブジェクトストレージベンダーの一覧については、NetAppの担当者にお問い合わせください。

クラウドネイティブのデータ保護に関心がある場合は、 NetAppコンソールを使用して、オンプレミスのボリュームとパブリック クラウドのCloud Volumes ONTAPインスタンス間のSnapMirrorまたはSnapVault関係を構成できます。

コンソールは、Software as a Service (SaaS) モデルを使用してCloud Volumes ONTAPインスタンスのバックアップも提供します。ユーザーは、 NetApp Backup and Recovery を使用して、 Cloud Volumes ONTAPインスタンスを S3 および S3 準拠のパブリック クラウド オブジェクト ストレージにバックアップできます。

"Cloud Volumes ONTAP のドキュメント"

"NetAppコンソールのドキュメント"

"NetAppコンソール"

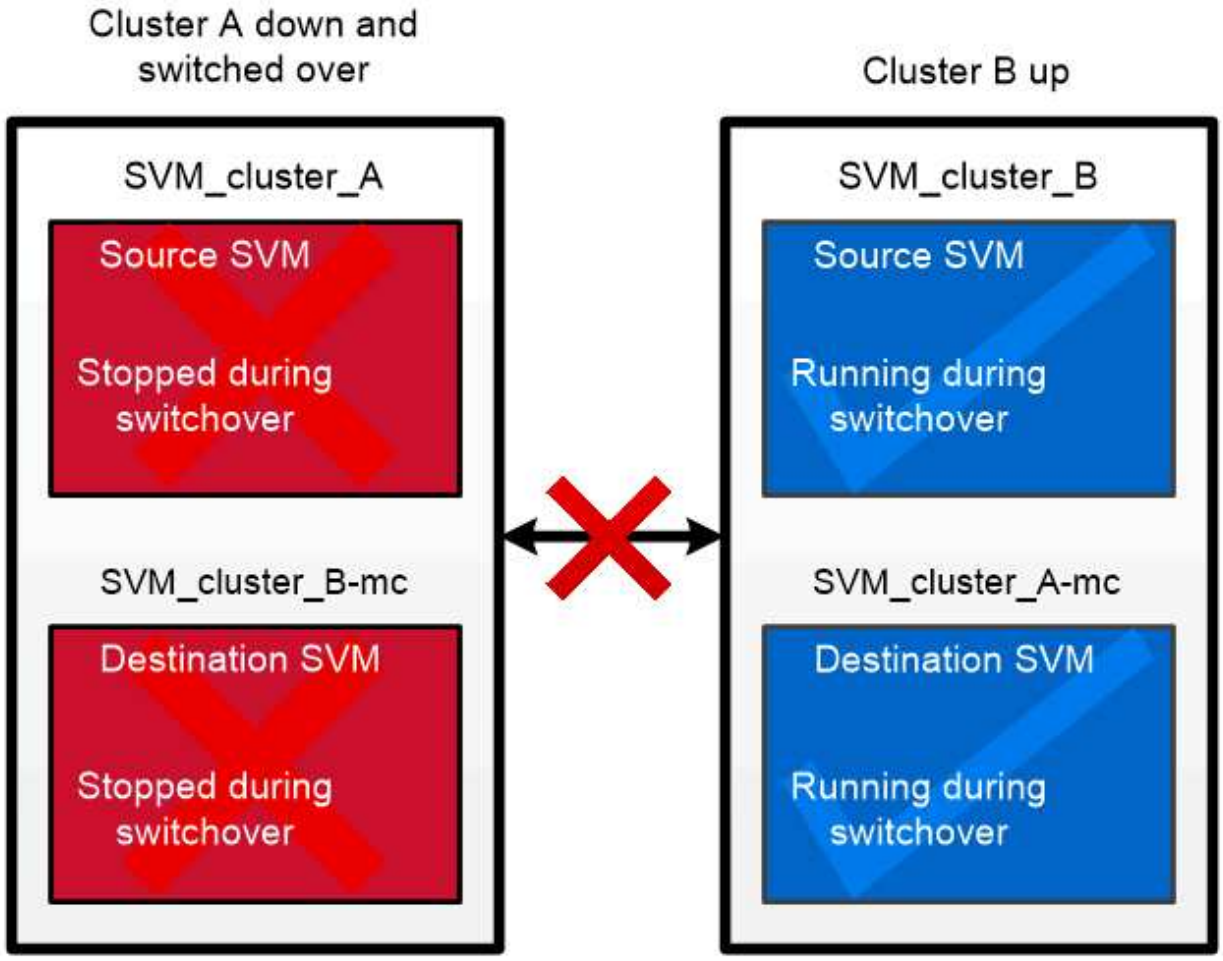
MetroClusterの継続的可用性

MetroCluster構成は、物理的に分離された2つのミラークラスタを実装することでデータを保護します。各クラスタが、もう一方のクラスタのデータとSVMの設定を同期的にレプリケートします。一方のサイトで災害が発生した場合、管理者は、ミラーされたSVMをアクティブ化し、サバイバーサイトからデータの提供を開始できます。

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

どちらの場合も、クラスタ間でピア関係を確立する必要があります。

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



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

*_ MetroCluster 以外の実装で SyncMirror を使用する _ オプションで MetroCluster 以外の実装で SyncMirror を使用することにより 'RAID タイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や 'RAID グループのディスクへの接続が失われた場合のデータ損失を防ぐことができますこの機能はHAペアに対してのみ使用できます。

アグリゲートデータは、別 々 のディスクシェルフに格納されたプレックスにミラーリングされます。いずれかのシェルフが使用できなくなった場合、障害の原因を修正しながら、影響を受けていないプレックスが引き続きデータを提供します。

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

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

Storage Efficiency

ONTAPのStorage Efficiencyの概要

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

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

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

- * シンプロビジョニング *

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

- * 重複排除 *

  重複排除ボリュームに必要な物理ストレージの量を3つの方法で削減します。

- ゼロブロック重複排除

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

- インライン重複排除

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

- バックグラウンド重複排除

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

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

- * 圧縮 *

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

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

- 圧縮

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

- * FlexCloneボリューム、ファイル、LUN *

  FlexCloneテクノロジSnapshotメタデータを活用して、ボリューム、ファイル、LUNの書き込み可能なポイントインタイムコピーを作成します。コピーはデータブロックを親と共有し、変更がコピーまたはその

親に書き込まれるまでメタデータに必要な分以外ストレージを消費しません。変更が書き込まれると、差分のみが保存されます。

従来の手法でコピーを作成すると数分から数時間かかりますが、FlexCloneテクノロジを使用すれば大規模なデータセットのコピーもほぼ瞬時に作成できます。

- 温度に敏感なストレージ効率

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

  ONTAP 9.8で導入されたTemperature-Sensitive Storage Efficiency（TSSE）は、新しく作成したシンプロビジョニングAFFボリュームで自動的に有効になります。ハードウェアオフロードプロセッサを使用するONTAP 9.15.1で導入されたでは、この機能は有効になっていません"AFF A70、AFF A90、およびAFF A1Kプラットフォーム"。

- * CPUまたは専用オフロード・プロセッサーのストレージ効率*

  ONTAP 9.15.1以降では、"CPUまたは専用オフロードプロセッサのストレージ効率"特定のAFFおよびFASプラットフォームでは自動的に有効になり、構成は必要ありません。これらのプラットフォームでは、温度に敏感なストレージ効率は使用されません。圧縮は、データがコールドになるのを待たずに開始され、メイン CPU または専用のオフロード プロセッサを使用して実行されます。これらのプラットフォームでは、連続する物理ブロックの順次パッキングも使用して、圧縮データのストレージ効率をさらに向上させます。

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

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

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

NetAppは、オンプレミスのONTAPと同じStorage Efficiency機能をクラウドでも提供しています。オンプレミスのONTAPからクラウドにデータを移行する際には、既存のストレージ効率化が維持されます。たとえば、ビジネスクリティカルなデータが含まれるSQLデータベースを、オンプレミス システムからクラウドに移行するとします。NetAppコンソールでデータ レプリケーションを使用してデータを移行し、移行プロセスの一環として、クラウド内のスナップショットに対して最新のオンプレミス ポリシーを有効にすることができます。

シンプロビジョニング

ONTAPは、Snapshotに加えて、さまざまなStorage Efficiencyテクノロジを提供しています。主なテクノロジには、シンプロビジョニング、重複排除、圧縮、 FlexClone ボリューム、ファイル、 LUN の割り当てが可能です。Snapshotと同様に、すべてONTAPのWrite Anywhere File Layout（WAFL）上に構築されています。

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

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

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

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

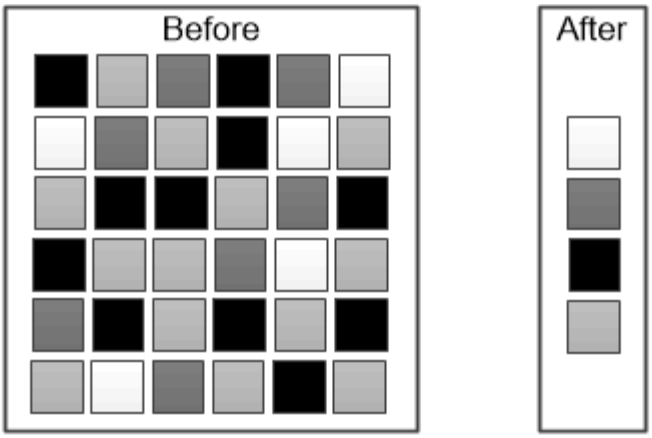
シンプロビジョニングを使用すると、使用しない可能性があるストレージを購入することなく、ストレージを大量に消費するユーザのニーズを満たすことができます。ストレージスペースは消費されるまで割り当てられないため、アグリゲートに含まれる5、000個のボリュームそれぞれに名目上1GBのサイズを割り当てることで、2TBのアグリゲートを「オーバーコミット」できます。

ライトユーザとヘビーユーザの比率が10：1であること、およびアグリゲートの空きスペースをアクティブに監視しているかぎり、スペース不足によってボリュームへの書き込みが失敗することはありません。

重複排除

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

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



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

圧縮

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

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

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

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

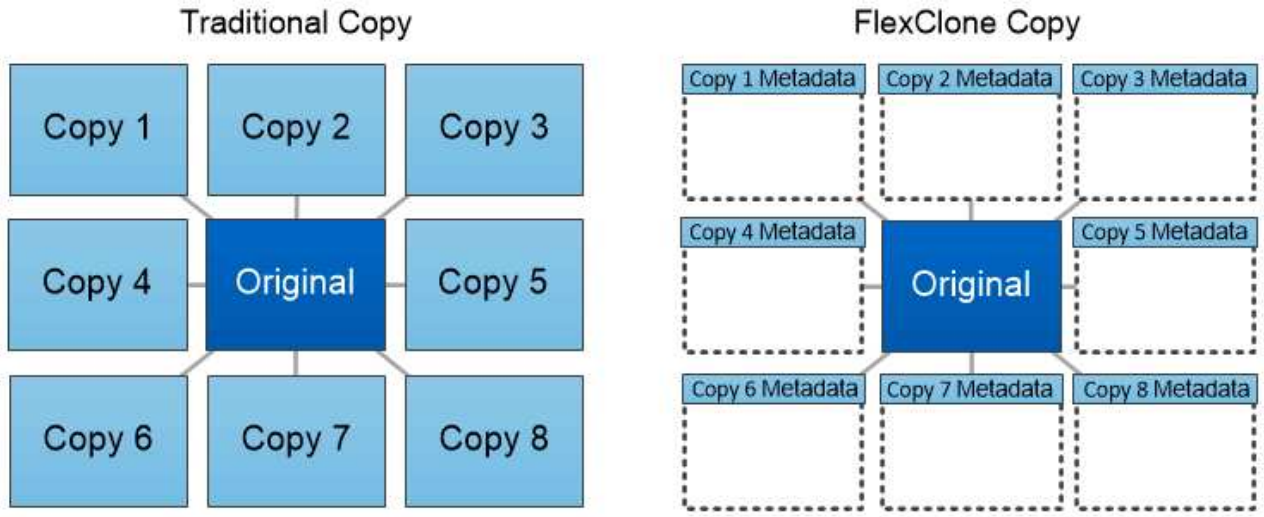
FlexCloneボリューム、ファイル、**LUN**

_snapshot_technology FlexCloneは、Snapshotメタデータを参照して、ボリュームの書き込み可能なポイントインタイムコピーを作成します。コピーはデータブロックを親と共有し、変更がコピーに書き込まれるまでメタデータに必要な分以外ストレージを消費しません。FlexCloneファイルとFlexClone LUNは同じテクノロジを使用しますが、元のスナップショットは必要ありません。

従来型のコピーの作成には数分から数時間かかることがありますが、FlexCloneソフトウェアを使用すると、大規模なデータセットでもほぼ瞬時にコピーできます。そのため、同一のデータセットの複数のコピー（仮想

デスクトップ環境など）やデータセットの一時的なコピー（本番環境のデータセットに対してアプリケーションをテストする）が必要な状況に最適です。

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



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

ONTAP System Manager での容量測定

システム容量は、物理スペースと論理スペースのどちらかで測定できます。ONTAP 9 .7以降では、System Managerで物理容量と論理容量の両方を測定できます。

次の説明では、2つの測定値の違いについて説明します。

- 物理容量：物理スペースは、ボリュームまたはローカル階層で使用されているストレージの物理ブロックを表します。Storage Efficiency機能（重複排除や圧縮など）によってデータが削減されるため、通常、使用済み物理容量の値は使用済み論理容量の値よりも小さくなります。
- 論理容量：論理スペースは、ボリュームまたはローカル階層で使用可能なスペース（論理ブロック）です。論理スペースとは、重複排除や圧縮の結果を考慮せずに理論上のスペースをどのように使用できるかを指します。使用済み論理スペースの値は、使用済み物理スペースの量に、設定されているStorage Efficiency機能（重複排除や圧縮など）による削減量を加えた値になります。この測定値にはSnapshot、クローン、その他のコンポーネントが含まれ、データ圧縮などの物理スペースの削減量が反映されていないため、使用済み物理容量よりも多く表示されることがあります。したがって、合計論理容量がプロビジョニング済みスペースよりも大きくなる可能性があります。

System Managerでは、容量表現にルートストレージ階層（アグリゲート）の容量は考慮されません。

使用済み容量の測定値

使用済み容量の測定値は、次の表で説明するように、使用しているSystem Managerのバージョンによって表示されます。

System Manager のバージョン	容量に使用される用語	参照される容量のタイプ
9.9.1以降	使用済み論理容量	使用済み論理スペース（Storage Efficiency の設定が有効になっている場合）
9.7および9.8	使用済み	使用済みの論理スペース（ Storage Efficiency の設定が有効になっている場合 ）
9.5 および 9.6 （クラシックビュー）	使用済み	使用済みの物理スペース

容量の測定条件

容量の定義には次の用語が使用されます。

- 割り当て容量：Storage VM内のボリュームに割り当てられているスペースの量。
- 使用可能：Storage VMまたはローカル階層でデータの格納やボリュームのプロビジョニングに使用できる物理スペースの量。
- ボリューム間の容量：Storage VM上のすべてのボリュームの使用済みストレージと使用可能なストレージの合計。
- クライアントデータ：クライアントデータに使用されているスペースの量（物理または論理）。
  - ONTAP 9.13.1以降では、クライアントデータで使用されている容量を*論理使用済み*と呼び、Snapshotで使用されている容量が別 々 に表示されます。
  - ONTAP 9.12.1以前では、クライアントデータで使用されている容量がSnapshotで使用されている容量に追加された容量を*論理使用済み*と呼びます。
- * Committed *：ローカル階層のコミット済み容量。
- データ削減：取り込まれたデータのサイズと格納されたデータのサイズの比率。
  - ONTAP 9 .13.1以降、データ削減機能では、重複排除や圧縮など、ほとんどのストレージ効率化機能の結果が考慮されますが、Snapshotやシンプロビジョニングはデータ削減率に含まれません。
  - ONTAP 9.12.1以前では、データ削減比率は次のように表示されます。
    - [容量]*パネルに表示されるデータ削減値は、使用済みの物理スペースに対するすべての使用済み論理スペースの総削減率であり、Snapshotやその他のStorage Efficiency機能を使用することによるメリットも含まれます。
    - 詳細パネルを表示すると、概要パネルに表示された*「全体」の比率と、クライアントデータのみで使用されている物理的な使用済みスペースと比較した、クライアントデータのみで使用されている論理スペースの比率（スナップショットおよびクローンなし）の両方が表示されます。
- 使用済み論理容量：
  - ONTAP 9.13.1以降では、クライアントデータで使用されている容量を*論理使用済み*と呼び、Snapshotで使用されている容量が別 々 に表示されます。
  - ONTAP 9.12.1以前では、クライアントデータで使用されている容量がSnapshotで使用されている容量に追加された容量を「* Logical Used *」と呼びます。
- * Logical Used %*：現在の使用済み論理容量に対するプロビジョニング済みサイズの割合（Snapshotリザ

ーブを除く）。この値にはボリュームでの効率化による削減も含まれるため、100%を超える場合があります。

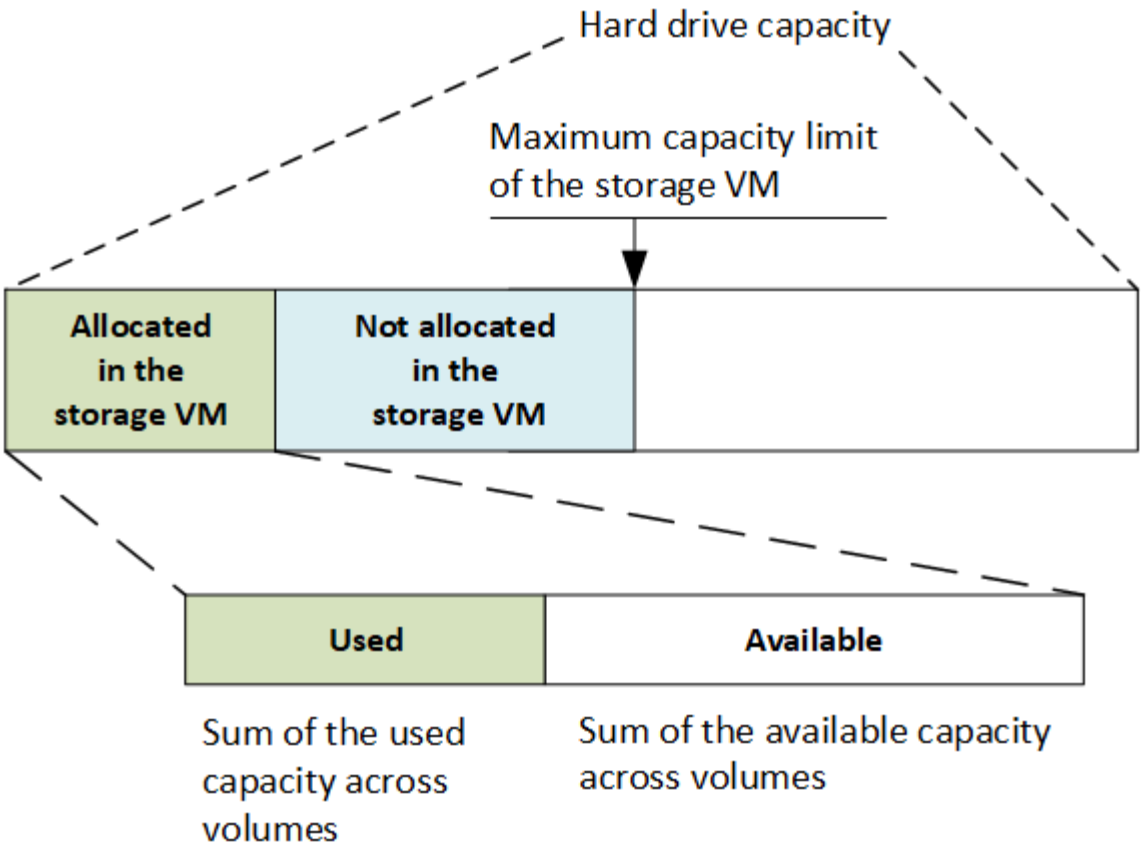
- 最大容量：Storage VM上のボリュームに割り当てられる最大スペース。
- 使用済み物理容量：ボリュームまたはローカル階層の物理ブロックで使用されている容量。
- * Physical Used %*：ボリュームの物理ブロックで使用されている容量の、プロビジョニングされたサイズに対する割合。
- プロビジョニングされた容量：Cloud Volumes ONTAPシステムから割り当てられ、ユーザやアプリケーションのデータを格納できる状態にあるファイルシステム（ボリューム）。
- * Reserved *：ローカル階層ですでにプロビジョニングされているボリューム用にリザーブされているスペースの量。
- 使用済み：データが格納されているスペースの量。
- * usedおよびreserved *：使用済みの物理スペースとリザーブスペースの合計です。

Storage VMの容量

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

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

次のグラフは、ボリューム間の容量の測定値と最大容量の関係を示しています。



ONTAP 9 .13.1以降では、クラスタ管理者が使用できます"Storage VMの最大容量制限を有効にする"。ただし、データ保護、SnapMirror関係、またはMetroCluster構成のボリュームを含むStorage VMに対してストレージ制限を設定することはできません。また、Storage VMの最大容量を超えるようにクォータを設定することはできません。

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

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

容量の測定単位

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

- .10.1以降では、ONTAP 9 Managerにストレージ容量の単位がKiB、MiB、GiB、TiB、およびPiBとして表示されます。
- ONTAP 9 .10.0以前では、これらの単位は、System ManagerにKB、MB、GB、TB、およびPBとして表示されます。

System Managerでスループットに使用される単位は、ONTAPのすべてのリリースで、KB/秒、MB/秒、GB/秒、TB/秒、およびPB/秒のままです。

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

関連情報

"System Managerでクラスタ、階層、SVMの容量を監視する"

"ボリュームの論理スペースのレポートと適用"

ONTAPの温度に敏感なストレージ効率について学ぶ

ONTAP は、ボリュームのデータへのアクセス頻度を評価し、その頻度をそのデータに適用される圧縮度にマッピングすることで、温度に敏感なストレージ効率 (TSSE) の利点を実現します。あまりアクセスされないコールド データは大きなデータ ブロックで圧縮され、頻繁にアクセスされて上書きされるホット データは小さなデータ ブロックで圧縮されるため、プロセスが効率化されます。

TSSE はONTAP 9.8 で導入され、新しく作成されたシンプロビジョニングされたAFFボリュームで自動的に有効になります。Temperature Sensitive Storage Efficiencyは、既存のAFFボリュームと、シンプロビジョニングされた非AFF DPボリュームで有効にできます。

温度に敏感なストレージ効率は、次のプラットフォームには適用されません。

プラットフォーム	**ONTAP**のバージョン
• AFF A1K用 • AFF A90用 • AFF A70用 • FAS90 • FAS70	9.15.1以降
• AFF A50用 • AFF A30用	9.16.1以降

これらのプラットフォームは"CPUまたは専用オフロードプロセッサのストレージ効率"。圧縮は、ホット データまたはコールド データに基づかず、メイン CPU または専用のオフロード プロセッサを使用して実行されます。

> 時間が経つにつれて、ボリューム内で使用されるスペースの量は、8K アダプティブ圧縮と比較して TSSE でより顕著になる可能性があります。この動作は、TSSE と 8K アダプティブ圧縮のアーキテクチャ上の違いにより予想されるものです。

「デフォルト」モードと「効率的」モードの導入

ONTAP 9 .10.1以降では、AFFシステムにのみ_default_and_efficient_volume-levelのStorage Efficiencyモードが導入されています。この2つのモードでは、ファイル圧縮（デフォルト）（新しいAFFボリュームの作成時のデフォルトモード）と、自動アダプティブ圧縮を使用してコールドデータやアクセス頻度の低いデータに対して圧縮による削減効果を高める温度重視のStorage Efficiency（効率的）のどちらかを選択できます。

ONTAP 9 .10.1以降にアップグレードする場合、既存のボリュームには、ボリュームで現在有効になっている圧縮のタイプに基づいてStorage Efficiencyモードが割り当てられます。アップグレードの実行中、圧縮が有効なボリュームにはデフォルトモードが割り当てられ、温度に基づくStorage Efficiencyが有効なボリュームには効率モードが割り当てられます。圧縮が有効になっていない場合、Storage Efficiencyモードは空白のままです。

"温度に基づくストレージ効率化は明示的に設定する必要があります"自動アダプティブ圧縮を有効にするには、ONTAP 9 .10.1を使用します。ただし、AFFプラットフォームでは、データコンパクション、自動重複排除スケジュール、インライン重複排除、ボリューム間インライン重複排除、ボリューム間バックグラウンド重複排除などの他のStorage Efficiency機能が、デフォルトモードと効率モードのどちらでもデフォルトで有効になります。

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

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

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

- ONTAP 9.12.1P4以降
- ONTAP 9.13.1以降

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

既存のボリュームでは、温度に基づくStorage Efficiencyは自動的には有効になりませんが、手動で効率化モードに変更できます。"Storage Efficiencyモードを変更します"

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

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

ONTAP 9 .13.1以降では、温度に左右されるストレージ効率化機能によって、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率がさらに向上します。システムをONTAP 9にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでは、シーケンシャルパッキングが自動的に有効になります。13.1シーケンシャルパッキングを有効にした後は、を実行する必要があります"既存のデータを手動で再パックします"。

専用オフロード プロセッサのストレージ効率は、連続する物理ブロックの順次パッキングを実行し、32k のデータ圧縮に専用オフロード プロセッサを使用します。 32k 圧縮では、スペースの節約がボリューム レベルで実現される 8k アダプティブ圧縮を使用するプラットフォームとは異なり、集約レベルでスペースの節約が実現されます。専用オフロード プロセッサ ストレージ効率を使用するプラットフォームでは、温度に敏感なストレージ効率 (TSSE) は使用されません。つまり、圧縮はホット データまたはコールド データに基づいていません。これにより、パフォーマンスに影響を与えることなく、すぐにスペースを節約できます。

専用オフロード プロセッサ ストレージ効率は、次のプラットフォームおよびONTAPバージョンでデフォルトで有効になっています。

AFF A20 プラットフォームは、専用オフロード プロセッサのストレージ効率をサポートしていません。 AFF A20 プラットフォームの場合、 SnapMirrorテクノロジーを使用して移行されたデータは、メイン CPU を使用して 32k インライン圧縮に自動的に変換されます。

プラットフォーム	**ONTAP**のバージョン
• AFF A1K用 • AFF A90用 • AFF A70用 • FAS90 • FAS70	9.15.1以降
• AFF A50用 • AFF A30用	9.16.1以降

次のプラットフォームでは、ストレージ効率は自動的に有効になり、構成は必要ありません。これは、他のプラットフォームから移動されたボリュームを含む、新しく作成されたすべてのシンプロビジョニング ボリュームと既存のデータに適用されます。スペース保証設定に関係なく重複排除は有効になります。圧縮とデータ圧縮の両方で、スペース保証を「なし」に設定する必要があります。ボリューム移動またはSnapMirrorテクノロジーを使用して移行されたデータは、自動的に 32k インライン圧縮に変換されます。

- AFF A1K用
- AFF A90用
- AFF A70用
- AFF A50用
- AFF A30用

次のプラットフォームでは、 ONTAP 9.15.1 以降にアップグレードする前にストレージ効率が有効になっていた既存のシンプロビジョニング ボリュームに対してのみ、ストレージ効率がデフォルトで有効になります。新しく作成したボリュームについては、CLIかREST APIメソッドを使用してストレージ効率化を有効にできます。ボリューム移動またはSnapMirrorテクノロジを使用して移行されたデータは、元のプラットフォームで

圧縮が有効になっている場合にのみ、32k インライン圧縮に変換されます。

- FAS90
- FAS70

コントローラをサポートされているプラットフォームにアップグレードする方法については、 "ONTAPハードウェアのアップグレードに関するドキュメント" 。

セキュリティ

クライアント認証と許可

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

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

認証

ローカルまたはリモートのユーザアカウントを作成できます。

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

ONTAPは、ローカルまたは外部のネームサービスを使用して、ホスト名、ユーザ、グループ、ネットグループ、およびネームマッピング情報を検索します。ONTAPは次のネームサービスをサポートしています。

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

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

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

許可

ONTAPでは、3つのレベルのセキュリティを評価して、SVM上にあるファイルおよびディレクトリに対して要

求された操作を実行する権限がエンティティにあるかどうかを判断します。アクセスは、セキュリティレベルの評価後に有効な権限によって決定されます。

- エクスポート（NFS）および共有（SMB）セキュリティ

  エクスポートおよび共有セキュリティは、特定のNFSエクスポートまたはSMB共有へのクライアントアクセスに適用されます。管理Privilegesを持つユーザは、SMBクライアントおよびNFSクライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルとディレクトリのセキュリティ

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

- NTFS、UNIX、およびNFSv4の標準のファイルレベルセキュリティ

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

SAMLによる認証

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

OAuth 2.0と**ONTAP REST API**クライアント

ONTAP 9.14以降では、Open Authorization（OAuth 2.0）フレームワークがサポートされています。クライアントでREST APIを使用してONTAPにアクセスする場合、認証とアクセス制御には、OAuth 2.0しか使用できません。ただし、その機能を有効にするためには、CLI、System Manager、REST APIなどの任意のONTAP管理インターフェイスを使用できます。

OAuth 2.0の標準的な機能は、いくつかの一般的な認証サーバとともにサポートされています。相互TLSベースの送信者制約付きアクセス トークンを使用することで、ONTAPのセキュリティをさらに強化できます。また、自己完結型スコープや、ONTAP RESTロールやローカル ユーザ定義との統合など、多様な認証オプションを利用できます。詳細については、を参照してください "ONTAP OAuth 2.0実装の概要" 。

カンリシヤニンシヨウト**RBAC**

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

認証

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

- ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納さ

れます。

- リモートアカウントでは、アカウント情報がActive Directoryドメインコントローラ、LDAPサーバ、またはNISサーバに格納されます。

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

RBAC

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

ウィルススキャン

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

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

- クライアントが SMB 経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、 _on_access scanning_to を使用します。ファイル処理は、外部サーバからファイルのスキャンステータスが報告されるまで中断されます。ファイルがすでにスキャンされている場合、ONTAPはファイル操作を許可します。それ以外の場合は、サーバからのスキャンを要求します。

  NFSではオンアクセススキャンはサポートされていません。

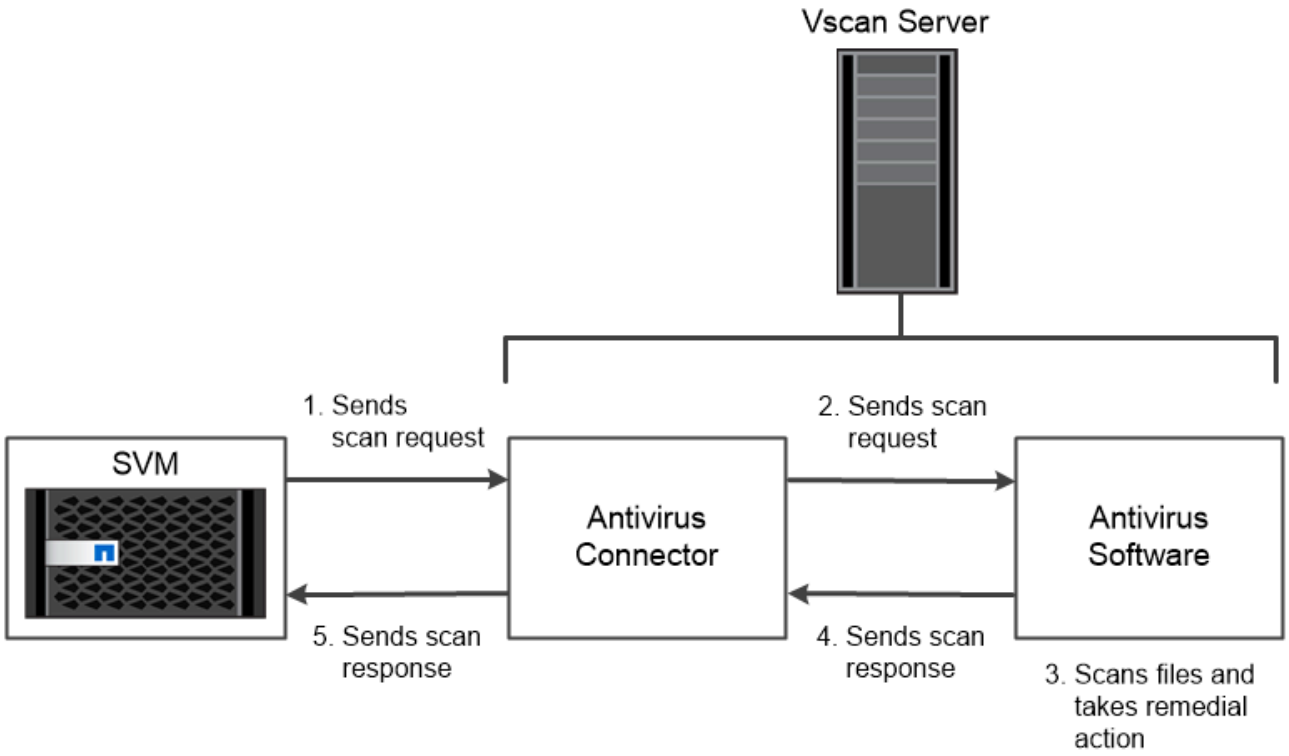
- オンデマンドスキャン _ を使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。たとえば、ピーク時を避けてスキャンを実行する場合などに便利です。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB経由で次回ファイルがアクセスされたときにそれらのファイル（ファイルが変更されていなければ）のファイルアクセスレイテンシが短縮されます。

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

通常は、SVMに対して両方のスキャンモードを有効にします。どちらのモードでも、ウィルス対策ソフトウェアはソフトウェアの設定に基づいて感染ファイルに対して修復アクションを実行します。

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

ディザスタリカバリ構成およびMetroCluster構成では、ローカルクラスタとパートナークラスタ用に個別のVscanサーバをセットアップする必要があります。



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

暗号化

ONTAPは、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないように、ソフトウェアベースとハードウェアベースの暗号化テクノロジを提供します。

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

- ハードウェアソリューション：
  - NetAppストレージ暗号化（NSE）

    NSEは、自己暗号化ドライブ（SED）を使用するハードウェアソリューションです。

  - NVMe SED

    ONTAPは、FIPS 140-2認証を取得していないNVMe SEDに対してFull Disk Encryptionを提供します。
- ソフトウェアソリューション：
  - NetAppアグリゲート暗号化（NAE）

    NAEは、アグリゲートごとに一意のキーを使用して、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェアソリューションです。

  - NetAppボリューム暗号化（NVE）

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

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

NetAppストレージ暗号化

NetAppストレージ暗号化（NSE）は、データを書き込み時に暗号化するSEDをサポートします。ディスクに保存されている暗号化キーがないと、データを読み取ることはできません。暗号化キーには、認証されたノードだけがアクセスできます。

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

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

NSEは、自己暗号化HDDとSSDをサポートしています。NetAppボリューム暗号化とNSEを併用すると、NSEドライブのデータを二重に暗号化できます。

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

NVMe自己暗号化ドライブ

NVMe SEDはFIPS 140-2認定を取得していませんが、AES 256ビット透過的ディスク暗号化を使用して保存データを保護します。

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

NetAppアグリゲート暗号化

NetAppアグリゲート暗号化（NAE）は、アグリゲートのすべてのデータを暗号化するためのソフトウェアベースのテクノロジです。NAEのメリットは、ボリュームはアグリゲートレベルの重複排除の対象となり、NVEボリュームは除外されることです。

NAEを有効にすると、アグリゲート内のボリュームをアグリゲートキーで暗号化できます。

ONTAP 9 .7以降では"NVEライセンス"、およびオンボードまたは外部のキー管理を使用している場合、新しく作成したアグリゲートとボリュームはデフォルトで暗号化されます。

NetAppボリューム暗号化

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

データ（Snapshotを含む）とメタデータの両方が暗号化されます。データへのアクセスには、ボリュームごとに1つの一意のXTS-AES-256キーが使用されます。キーは、組み込みのオンボードキーマネージャによってデータと同じシステムに保護されます。

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

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

- 暗号化キー管理ソリューションが、Federal Information Processing Standards（FIPS；連邦情報処理標準）140-2またはOASIS KMIP標準に準拠している必要があります。
- マルチクラスタソリューションが必要です。KMIPサーバでは、複数のクラスタの暗号化キーの一元管理がサポートされます。

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

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

  KMIPサーバでは、データとは別に認証キーが格納されます。

関連情報

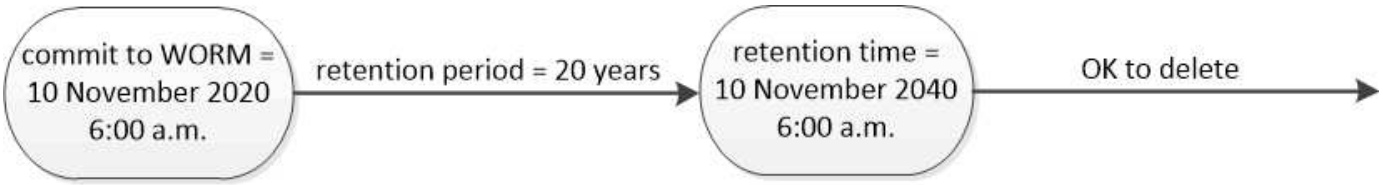
"FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"

WORMストレージ

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

1つのライセンスで、SnapLockをStrict_Complianceモードで使用したり、SEC Rule 17a-4（f）などの外部の要件を満たすために_を使用したり、Looser_Enterpriseモードで_を使用したりすることができます。また、デジタル資産の保護に関する社内で義務付けられている規制を満たすこともできます。SnapLock では、改ざん防止機能を備えた ComplianceClock _ を使用して、 WORM ファイルの保持期間が経過したかどうかを判断します。

SnapVaultで_ SnapLockを使用して、セカンダリストレージ上のSnapshotをWORM方式で保護できます。SnapMirrorを使用すると、ディザスタリカバリなどの目的で、地理的に離れた別の場所にWORMファイルをレプリケートできます。



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

ONTAPとVMware vSphere

ONTAPおよび関連するNetApp製品をVMware vSphereに統合できます。お使いのテクノロジ環境やビジネス ニーズに応じた、いくつかのオプションが用意されています。

選択された概念と用語

VMware環境でのONTAPおよび関連するNetApp製品の使用方法について理解しておくと、最初にいくつかの主要な用語と概念を理解しておくと役立ちます。

論理ユニット番号

LUNは、ストレージエリアネットワーク（SAN）内の論理ユニットを識別するために使用される番号です。これらのアドレス指定可能なデバイスは、通常、SCSI（Small Computer System Interface）プロトコルまたはそのカプセル化された派生物の1つを介してアクセスされる論理ディスクです。

VMware vSphere仮想ボリューム

仮想ボリューム（vVol）は、仮想マシンで使用されるストレージをボリュームレベルで抽象化します。これにはいくつかの利点があり、従来のLUNの代わりに使用できます。

永続的予約

永続的予約はSCSI-3でサポートされ、以前のSCSI-2予約よりも強化されています。これにより、複数のクライアント イニシエータが1つのターゲットと通信しながら、他のノードをロックアウトできます。エラー リカバリのためにバスがリセットされた場合でも、予約は維持できます。

ONTAP 9.15.1以降では、SCSI-3を使用して仮想ボリュームの永続的予約を作成できます。この機能は、Windows Serverフェイルオーバー クラスタ（WSFC）でONTAP Tools for VMware vSphere 9を使用する場合にのみサポートされます。

Windows Serverフェイルオーバー クラスタリング

Microsoft Windows Serverフェイルオーバー クラスタリング（WSFC）は、フォールト トレランスと高可用性を提供するWindows Serverオペレーティング システムの機能です。一連の（物理または仮想）サーバ ノードをクラスタとして統合することにより、障害発生時の耐障害性を確保します。WSFCは、一般にデータベース サーバ、ファイル サーバ、ネームスペース サーバなどのインフラ サービスを導入するために使用されます。

VMware vSphere Storage API - Storage Awareness

VMware vSphere Storage API - Storage Awareness（VASA）は、ストレージ アレイとvCenterを統合して管理するための一連のAPIです。このアーキテクチャは、VMware vSphereとストレージシステムの間の通信を処理する_VASA Provider_など、複数のコンポーネントに基づいています。ONTAPでは、プロバイダはONTAP Tools for VMware vSphereの一部として実装されます。

VMware vSphere Storage APIs - Array Integration

VMware vSphere Storage API – Array Integration（VAAI）は、VMware vSphere ESXiホストとストレージデバイスの間の通信を可能にする一連のAPIです。このAPIには、ストレージ処理をアレイにオフロードするためにホストが使用する一連の基本処理が含まれています。VAAIは、ストレージを大量に消費するタスクのパフォーマンスを大幅に向上させることができます。

NetApp SnapCenter

SnapCenterは、ONTAPストレージシステムを使用してアプリケーション、データベース、ホストファイルシステム、仮想マシンのデータを保護する、拡張性に優れた一元化されたプラットフォームです。Snapshot、SnapRestore、FlexClone、SnapMirror、SnapVaultなど、ネイティブのONTAPテクノロジが活用されています。

NetAppプラグインと関連テクノロジ

NetAppは、ONTAPおよび関連製品をVMware vSphereテクノロジと統合するための堅牢なサポートを提供します。

ONTAP tools for VMware vSphere

ONTAP Tools for VMware vSphereは、ONTAPとvSphereを統合するための一連のツールです。VASA APIフレームワークのプロバイダ機能を実装します。ONTAP Toolsには、vCenterプラグイン、VMware Site Recovery Manager用のStorage Replication Adapter（SRA）、自動化アプリケーションの構築に使用できるREST APIサーバも含まれています。

NFS Plug-In for VMware VAAI

NetApp NFS Plug-In for VMware VAAIでは、VAAI機能にアクセスできます。このプラグインはESXiホストにインストールできるため、ホストがONTAP上のNFSデータストアでVAAIを活用できます。クローニング、スペース リザベーション、Snapshotのオフロードなど、複数の処理を実行できます。

VMware Site Recovery Manager

VMware Site Recovery Manager（SRM）は、ディザスタ リカバリ機能を提供します。SRMは、ONTAP Tools for VMware vSphereと統合されているため、ONTAPのデータ管理機能にアクセスして活用できます。

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster（vMSC）は、a_stretched cluster_deployment.vMSCソリューションを有効にしてサポートするテクノロジです。vMSCソリューションは、NetApp MetroClusterおよびSnapMirrorのアクティブ同期（旧称SMBC）でサポートされます。これらのソリューションは、ドメインに障害が発生した場合のビジネス継続性を強化します。耐障害性モデルは、選択した構成に基づいています。

SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere（SCV）は、SnapCenterサーバと一緒に導入することも、スタンドアロン アプリケーションとして導入することもできるLinuxベースの仮想アプライアンスです。どちらの場合も、SCVはVM、データストア、VMDKのバックアップ処理とリストア処理を提供します。各処理は高速でスペース効率に優れ、クラッシュ整合性、VM整合性を備えています。

追加情報へのアクセス

VMware vSphere環境にONTAPを導入するための準備に役立つその他のリソースがいくつか用意されています。

- "ONTAP Tools for VMware vSphereのドキュメント"
- "エンタープライズアプリケーション：VMware vSphereとONTAP"
- "NetApp KB：SCSI予約とSCSI永続的予約について"
- "SnapCenter Plug-in for VMware vSphereのドキュメント"

FabricPool

NetAppをご利用のお客様の多くは、ほとんどアクセスされない大量のデータを格納しています。これは、 _COM_DATA と呼ばれます。また、お客様は頻繁にアクセスされるデータも保有しており、これを _hot_data と呼んでいます。最高のパフォーマンスを得るためには、ホットデータを最速のストレージに保存することが理想的です。コールドデータは、必要に応じてすぐに利用できるかぎり、低速のストレージに移動できます。では、データのどの部分がホットで、どの部分がコールドであるかを知るには、どうすればよいでしょうか。

FabricPoolは、ハイパフォーマンスなローカル階層とクラウド階層の間で、アクセスパターンに基づいてデータを自動的に移動するONTAPの機能です。階層化することで、高価なローカルストレージをホットデータ用に解放し、コールドデータをクラウド内の低コストのオブジェクトストレージからいつでも利用できる状態に保ちます。FabricPoolはデータアクセスを常時監視し、階層間でデータを移動することで、最高のパフォーマンスと最大限のコスト削減を実現します。

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

しかし、FabricPoolは、オンプレミスのデータをクラウドに階層化するだけのものではありません。多くのお客様がCloud Volumes ONTAPでFabricPoolを使用して、クラウドプロバイダ内の高コストのクラウドストレージから低コストのオブジェクトストレージにコールドデータを階層化しています。ONTAP 9 8以降では、またはを使用してFabricPool対応ボリュームで分析をキャプチャできます"ファイルシステム分析""温度に敏感なストレージ効率"。

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

コールドデータは、大手クラウドプロバイダのオブジェクトストレージに格納できます。また、NetApp StorageGRIDを選択してコールドデータを自社のプライベートクラウドに保持することで、パフォーマンスを最大限に高め、データを完全に管理できます。

関連情報

"FabricPool System Managerのドキュメント"

"NetAppクラウド階層化"

"NetApp TechComm TVのFabricPool関連ビデオ"

ONTAP でのクイックスタート

ONTAPの使用を開始するには、クラスタのセットアップ、ネットワークの設定、BMCに

よる自動ネットワーク設定の有効化、ローカル階層の作成、プロトコルの設定、ストレージのプロビジョニングを行う必要があります。

1 クラスタのセットアップ

にはSystem Managerを使用することを推奨しますNetApp"新しいONTAPクラスタのセットアップ"。System Managerでは、ノード管理IPアドレスの割り当てやクラスタの初期化など、クラスタセットアップのワークフローをシンプルかつ簡単に実行できます。

2 ネットワークの設定

を作成してネットワークを設定します。"ブロードキャスト ドメイン" "サブネット"必要に応じて、を作成し"IPspace"ます。

3 **BMC**の自動ネットワーク設定を有効にする

"BMCの自動ネットワーク設定を有効にする"そのため、各ノードのBMCにIPアドレスを手動で割り当てる必要はありません。

4 ローカル階層を作成する

"ローカル階層の作成"ノードの使用可能なディスクまたはSSDからデータを移動します。ハードウェアに基づいて、最適な階層構成がSystem Managerによって自動的に計算されます。

5 プロトコルを設定する

"NAS、SAN、NVMeの各プロトコルを有効にする"をクラスタに追加します。

6 ストレージのプロビジョニング

または"SAN"構成用のストレージをプロビジョニング"NAS"

次の手順

- "システムの最適化に役立つ分析情報を取得"です。
- "ONTAP管理者認証とロールベースアクセス制御（RBAC）の設定"をクリックして、管理者の機能を定義します。
- "重要なイベント管理システム（EMS）通知を送信するようにONTAPを構成する"注意が必要なシステムの問題についてすぐに通知されます。
- ONTAPを使用して、およびを使用する方法を学習します"ディザスタリカバリ用にデータをバックアップ""ランサムウェア攻撃からデータを保護"。
- "Digital AdvisorとAutoSupportの詳細"です。
- System Managerを使用して、"クラスタの健全性の監視"

ONTAPクラスタをセットアップする

ONTAPクラスタセットアップワークフローの概要

クラスタをセットアップするには、セットアップの完了、クラスタの作成とノードの結合、管理 LIF の IPv4 から IPv6 への変換、 Active IQ Config Advisorを使用したクラスタの確認、クラスタ全体のシステム時間の同期に必要な情報を収集する必要があります。

この手順は、 FAS、 AFF 、およびASAシステムに適用されます。

- AFXシステムをお持ちの場合は、"以下の手順を実行します" ONTAPクラスタをセットアップします。
- ASA r2システム（ASA A1K、 ASA A90、 ASA A70、 ASA A50、 ASA A30、 ASA A20、またはASA C30）をお持ちの場合は、"以下の手順を実行します" ONTAPクラスタをセットアップします。ASA r2システムは、SANのみのお客様向けのシンプルなONTAPエクスペリエンスを備えています。

1 "情報の収集"

クラスタのセットアップを開始する前に、セットアッププロセスを完了するために必要な情報を収集します。

2 **"ONTAPクラスタを作成してノードを追加"**

NetAppでは、System Managerを使用して新しいクラスタをセットアップすることを推奨しています。System Managerでは、ノード管理IPアドレスの割り当てやクラスタの初期化など、クラスタセットアップのワークフローをシンプルかつ簡単に実行できます。

3 **"管理LIFをIPv4からIPv6に変換する"**

ONTAP 9.13.1以降では、ONTAPコマンドラインインターフェイス（CLI）を使用して、クラスタの初期セットアップ時にAFF A800およびFAS 8700プラットフォームの管理LIFにIPv6アドレスを割り当てることができます。9.13.1より前のONTAPリリースまたは他のプラットフォームの9.13.1以降では、最初にIPv4アドレスを管理LIFに割り当ててから、クラスタのセットアップの完了後にIPv6アドレスに変換する必要があります。

4 **"Active IQ Config Advisorでクラスタを確認する"**

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

5 "クラスタ全体のシステム時間を同期する"

クラスタ全体でシステム時間を同期して、クラスタ内のすべてのノードの時刻を同じにし、CIFSやKerberosのエラーを回避します。

ONTAPクラスタをセットアップするための情報を収集します。

クラスタのセットアップを開始する前に、クラスタ管理インターフェイスのポートやIPアドレスなど、クラスタのセットアップを完了するために必要な情報を収集しておく必要があります。まずは、クラスタセットアップワークシートに関連するすべての情報を収集してください。クラスタセットアップワークシートを使用すると、クラスタセットアッププロセスで必要となる値を記録できます。デフォルト値が指定されている場合は、その値を使用するか、独自の値を入力できます。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します" ONTAP クラスタをセットアップします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

システムテフオルト

システムのデフォルトは、プライベートクラスタネットワークのデフォルト値です。これらのデフォルト値を使用することを推奨します。ただし、これらの値が要件を満たしていない場合は、テーブルを使用して独自の値を記録できます。

ネットワークスイッチを使用するように構成されたクラスタでは、各クラスタスイッチで9000 MTUサイズを使用する必要があります。

情報の種類	自分の価値観
プライベートクラスタネットワークのポート	
クラスタネットワークのネットマスク	
クラスタインターフェイスの IP アドレス（各ノードの各クラスタネットワークポート用）：各ノードの IP アドレスは同じサブネット上にある必要があります。	

クラスタ情報

情報の種類	自分の価値観
クラスタ名の 1 文字目はアルファベットにする必要があります。最大文字数は 44 文字です。名前には次の特殊文字を使用できます。 . - _	

機能のライセンスキー

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

情報の種類	自分の価値観
機能のライセンスキー	

管理**Storage Virtual Machine（SVM）**

情報の種類	自分の価値観
クラスタ管理者のパスワード クラスタ管理者がコンソールにアクセスするとき、またはセキュアなプロトコルを介してアクセスするときにクラスタから入力を求められる、管理者アカウントのパスワードです。 セキュリティ上の理由から、このワークシートにパスワードを記入することは推奨されません。 パスワードのデフォルトのルールは次のとおりです。 • 8文字以上である必要があります。 • 英文字と数字がそれぞれ1文字以上含まれている必要があります。	
クラスタ管理インターフェイスポート データネットワークに接続されている物理ポート。クラスタ管理者はこのポートを使用してクラスタを管理できます。	
クラスタ管理インターフェイスのIPアドレス クラスタ管理インターフェイスの一意のIPv4アドレスまたはIPv6アドレス。クラスタ管理者は、このアドレスを使用して管理SVMにアクセスし、クラスタを管理します。通常、このアドレスはデータネットワーク上にある必要があります。 このIPアドレスは、組織でIPアドレスを割り当てる管理者から取得できます。 例：192.0.2.66	
クラスタ管理インターフェイスのネットマスク（IPv4） クラスタ管理ネットワークの有効なIPv4アドレスの範囲を定義するサブネットマスク。 例：255.255.255.0	

情報の種類	自分の価値観
クラスタ管理インターフェイスのネットマスクの長さ（IPv6） クラスタ管理インターフェイスでIPv6アドレスを使用する場合のプレフィックス長。クラスタ管理ネットワークの有効なIPv6アドレスの範囲を定義します。 例：64	
クラスタ管理インターフェイスのデフォルトゲートウェイ クラスタ管理ネットワーク上のルータのIPアドレス。	
DNSトメインメイ ネットワークのDNSドメインの名前。 ドメイン名には英数字を使用する必要があります。複数のDNSドメイン名を入力するには、カンマまたはスペースでそれぞれの名前を区切ります。	
ネーム サーバのIPアドレス DNSネーム サーバのIPアドレスです。各アドレスをカンマまたはスペースで区切ります。	

ノード情報（クラスタ内の各ノード用）

情報の種類	自分の価値観
コントローラの物理的な場所（オプション） コントローラの物理的な場所の説明です。このノードをクラスタ内のどこに配置するかを示す概要を使用します（例： Lab 5 、 Row 7 、 Rack B` ）。	
ノード管理インターフェイスポート ノード管理ネットワークに接続されている物理ポートで、クラスタ管理者はこのポートを使用してノードを管理できます。	

情報の種類	自分の価値観
ノード管理インターフェイスのIPアドレス 管理ネットワーク上のノード管理インターフェイスに対する一意のIPv4アドレスまたはIPv6アドレスです。ノード管理インターフェイス ポートをデータ ポートとして定義している場合、このIPアドレスはデータ ネットワーク上で一意のIPアドレスである必要があります。 このIPアドレスは、組織でIPアドレスを割り当てる管理者から取得できます。 例：192.0.2.66	
ノード管理インターフェイスのネットマスク（IPv4） ノード管理ネットワークの有効なIPアドレスの範囲を定義するサブネットマスク。 ノード管理インターフェイスポートをデータポートとして定義している場合は、ネットマスクをデータネットワークのサブネットマスクにする必要があります。 例：255.255.255.0	
ノード管理インターフェイスのネットマスクの長さ（IPv6） ノード管理インターフェイスでIPv6アドレスを使用する場合のプレフィックス長です。ノード管理ネットワークの有効なIPv6アドレスの範囲を定義するプレフィックス長です。 例：64	
ノード管理インターフェイスのデフォルトゲートウェイ ノード管理ネットワーク上のルータのIPアドレス。	

NTPサーバの情報

情報の種類	自分の価値観
NTPサーバのアドレス サイトのNetwork Time Protocol（NTP；ネットワークタイムプロトコル）サーバのIPアドレス。これらのサーバは、クラスタ全体で時間を同期するために使用されます。	

ONTAPクラスタを作成してノードを追加

NetAppでは、System Managerを使用して新しいクラスタを作成することを推奨しています。System Managerでは、クラスタセットアップのワークフローをシンプルかつ簡単に実行できます。ONTAPコマンドラインインターフェイス（CLI）を使用する必要があるのは、MetroCluster構成でONTAP 9.7以前を実行している場合、または特定のプラットフォームでIPv6のみのクラスタを設定する必要がある場合のみです。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します" System Manger を使用して ONTAP クラスタをセットアップします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ONTAP 9.13.1以降では、ONTAP CLIを使用したクラスタの初期セットアップ時に、AFF A800およびFAS8700プラットフォームの管理LIFにIPv6アドレスを割り当てることができます。ONTAP 9.13.1より前のONTAPリリース、または他のプラットフォームのONTAP 9.13.1以降の場合は、System Managerを使用してIPv4アドレスを使用してクラスタを作成し、クラスタのセットアップ完了後にアドレスを使用してクラスタを作成する必要があります"IPv6に変換します"。

System Manager 9.6以前のONTAPでは、IPv6ネットワークを必要とする環境はサポートされません。

開始する前に

- プラットフォームモデルの設置とセットアップの手順に従って、新しいストレージシステムを設置し、ケーブル接続して電源をオンにしておく必要があります。

  を参照してください"AFFおよびFASのドキュメント"。

- "必要な情報の収集"をクリックしてクラスタセットアップを完了します。
- クラスタ内通信用に、クラスタの各ノードにクラスタネットワークインターフェイスが設定されている必要があります。
- CLIを使用してIPv6を設定する場合は、ベース管理コントローラ（BMC）でIPv6を設定して、SSHを使用してシステムにアクセスできるようにする必要があります。

例 **1.** 手順

System Manager

1. ノード管理IPアドレスを割り当てる
   - Windowsコンピュータ
     i. Windowsコンピュータをコントローラと同じサブネットに接続します。

        これにより、システムにノード管理IPアドレスが自動的に割り当てられます。

     ii. [ネットワーク]*ドライブを開き、ノードを検出します。
     iii. クラスタセットアップウィザードを起動するノードを選択します。
   - Windows以外のコンピュータ
     i. クラスタに追加するすべてのノードの電源をオンにします。

        これは、クラスタセットアップの検出を有効にするために必要です。

     ii. 最初のノードのコンソールに接続します。

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

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

     i. AutoSupportステートメントを確認します。

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

        AutoSupportはデフォルトで有効になっています。

     ii. 画面の指示に従って、ノードに管理IPアドレスを割り当てます。
     iii. Webブラウザで、設定したノード管理IPアドレスを入力します"https://node-management-IP"。

        クラスタの残りのノードはSystem Managerで自動的に検出されます。

2. [ストレージシステムの初期化]*で、クラスタ名と管理パスワードを入力します。
3. [ネットワーク]*で、クラスタ管理IPアドレス、サブネットマスク、およびゲートウェイを入力します。
4. ドメインネームサービスを使用してホスト名を解決する場合は、*[ドメインネームサービス（DNS）を使用]*を選択し、DNSサーバ情報を入力します。
5. ネットワークタイムプロトコル（NTP）を使用してクラスタ全体の時間の同期を維持する場合は、**[**その他**]***で[タイムサービス（NTP）を使用する]*を選択し、NTPサーバの情報を入力します。
6. [送信] を選択します。

ONTAP CLI

1. クラスタに追加するすべてのノードの電源をオンにします。

   これは、クラスタセットアップの検出を有効にするために必要です。

2. 最初のノードのコンソールに接続します。

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

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

3. AutoSupportステートメントを確認します。

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

   AutoSupportはデフォルトで有効になっています。

4. 画面の指示に従って、ノードに管理IPアドレスを割り当てます。

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

5. Enter * を押して続行します。

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

6. 新しいクラスタを作成します。

   a. 入力 `create`

   b. システムのデフォルトを受け入れるか、独自の値を入力します。

   c. セットアップが完了したら、クラスタにログインし、クラスタがアクティブで、第1ノードが正常であることを確認します。 `cluster show`

      次の例は、最初のノード（cluster1-01）が正常に機能しており、参加条件を満たしているクラスタを示しています。

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

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

7. クラスタにノードを追加します。

   一度に1つのノードをクラスタに追加できます。次のノードの追加を開始するには、各ノードの追加処理を完了し、そのノードがクラスタに属している必要があります。

   NL-SASドライブを最大24本搭載したFAS2720では、パフォーマンスを最適化するために、ストレージのデフォルト構成がアクティブ / パッシブに設定されていることを確認する必要があります。詳細については、のドキュメントを参照してください "ルート/データパーティショニングを使用するノードでのアクティブ/パッシブ構成の設定"。

   a. クラスタに追加するノードにログインします。

      コンソールでクラスタセットアップウィザードが起動します。

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

   b. AutoSupportステートメントを確認します。

      AutoSupportはデフォルトで有効になっています。

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

   c. 画面の指示に従って、ノードにIPアドレスを割り当てます。

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

   d. Enter * を押して続行します。

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

   e. 入力 `join`

   f. 画面の指示に従ってノードをセットアップし、クラスタに追加します。

   g. セットアップが完了したら、ノードが正常に機能しており、クラスタへの参加条件を満たしていることを確認します。 `cluster show`

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

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

8. 手順7を繰り返して、残りの各ノードを追加します。

次のステップ

- 必要に応じて、"IPv4からIPv6に変換します"
- "Active IQ Config Advisorを実行して構成を検証し、一般的な構成エラーがないかどうかを確認"です。

必要に応じて、ONTAP管理LIFをIPv4からIPv6に変換する

ONTAP 9.13.1以降では、ONTAPコマンドラインインターフェイス（CLI）を使用して、クラスタの初期セットアップ時にAFF A800およびFAS 8700プラットフォームの管理LIFにIPv6アドレスを割り当てることができます。9.13.1より前のONTAPリリースまたは他のプラットフォームの9.13.1以降では、最初にIPv4アドレスを管理LIFに割り当ててから、クラスタのセットアップの完了後にIPv6アドレスに変換する必要があります。

DHCPを使用した自動割り当てIPアドレスとWindows検出機能を使用したハードウェアのセットアップが完了したあとにSystem Managerを起動すると、System ManagerでIPv6管理アドレスを設定できます。

手順

1. クラスタに対してIPv6を有効にします。

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

2. 権限をadvancedに設定します。

```
set priv advanced
```

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

```
network ndp prefix show
```

4. IPv6管理LIFを作成します。

   addressパラメータのformatを使用し`prefix::id`て、IPv6アドレスを手動で作成します。

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

5. LIFが作成されたことを確認します。

```
network interface show
```

6. 設定したIPアドレスに到達できることを確認します。

```
network ping6
```

7. IPv4 LIFを「意図的に停止」とマークします。

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

8. IPv4管理LIFを削除します。

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

9. IPv4管理LIFが削除されたことを確認します。

```
network interface show
```

関連情報

- "ネットワークインターフェイス"
- "network ndp prefix show"
- "ネットワークオプションipv6 modify"

Digital Advisor Config AdvisorでONTAPクラスタを確認する

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

Config Advisorは、ラップトップ、仮想マシン、またはサーバにインストールするWebベースのアプリケーションで、Windows、Linux、Macの各プラットフォームで動作します。

Config Advisorでは、一連のコマンドを実行してインストールを検証し、クラスタスイッチやストレージスイッチなどの構成全体の健全性をチェックします。

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

   "Active IQ Config Advisor"

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

   ガイドモードを選択すると、接続されているスイッチが自動的に検出されます。

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

ONTAPクラスタ全体のシステム時間を同期する

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

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

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

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

   ```
   cluster date show
   ```

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

   次の例は、クラスタ内の各ノードの日付とタイムゾーンを示しています。

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

2. すべてのノードの日付またはタイムゾーンを変更します。

```
cluster date modify
```

次に、クラスタのタイムゾーンをGMTに変更する例を示します。

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

3. クラスタをNTPサーバに関連付けます。

対称認証を使用せずにNTPサーバを設定するには、次のコマンドを入力します。

```
cluster time-service ntp server create -server <server_name>
```

対称認証を使用するNTPサーバを設定するには、次のコマンドを入力します。

```
cluster time-service ntp server create -server <server_ip_address> -key
-id <key_id>
```

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

この例では、クラスタにDNSが設定されていることを前提としています。DNSを設定していない場合は、NTPサーバのIPアドレスを指定する必要があります。

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

4. クラスタがNTPサーバに関連付けられていることを確認します。

```
cluster time-service ntp server show
```

次の例は、クラスタがNTPサーバntp1.example.comに関連付けられていることを示しています。

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

NTPサーバの対称認証の管理用コマンド

ONTAP 9 .5以降では、ネットワークタイムプロトコル（NTP）バージョン3がサポートされます。NTPv3にはSHA-1キーを使用した対称認証が含まれているため、ネットワークセキュリティが向上します。

作業	使用するコマンド
対称認証を使用せずにNTPサーバを設定する	`cluster time-service ntp server create -server server_name`
対称認証を使用してNTPサーバを設定する	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
既存のNTPサーバに対して対称認証を有効にする 必要なキーIDを追加することで、既存のNTPサーバを変更して認証を有効にすることができます。	`cluster time-service ntp server modify -server server_name -key-id key_id`
共有NTPキーを設定する	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` • 注：共有キーは ID で参照されます。ID、そのタイプ、および値がノードとNTPサーバの両方で同じである必要があります。
不明なキーIDでNTPサーバを設定する	`cluster time-service ntp server create -server server_name -key-id key_id`

作業	使用するコマンド
NTPサーバで設定されていないキーIDでサーバを設定します。	`cluster time-service ntp server create -server server_name -key-id key_id` • 注：* キー ID 、タイプ、および値は、 NTP サーバに設定されているキー ID 、タイプ、および値と同じである必要があります。
対称認証を無効にする	`cluster time-service ntp server modify -server server_name -authentication disabled`

関連情報

- "システム管理"
- "クラスタタイムサービスNTP"

ONTAPソフトウェアとファームウェアのアップグレードとリバート

ONTAPのアップグレード

ONTAPアップグレードの詳細

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

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

アップグレードを開始するには、アップグレードの準備を行う必要があります。Active IQデジタルアドバイザ(デジタルアドバイザとも呼ばれます)の有効なSupportEdge契約がある場合は、次の"Upgrade Advisorを使用してアップグレードを準備する"手順を実行してください。Upgrade Advisorは、クラスタを評価し、構成に固有のアップグレードプランを作成することで、不確実性とリスクを最小限に抑えるためのインテリジェンスを提供します。Active IQデジタルアドバイザの有効なSupportEdge契約をお持ちでない場合は、次の"Upgrade Advisorを使用せずにアップグレードを準備"手順を実行してください。

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

> ONTAP 9.12.1 以降、System Manager はNetAppコンソールと完全に統合されています。システムにコンソールが設定されている場合は、システム ページからアップグレードできます。

ONTAPソフトウェアのアップグレードについてサポートが必要な場合は、NetAppプロフェッショナルサービスをご利用"マネージドアップグレードサービス"ください。このサービスの利用をご希望の場合は、NetAppの営業担当者またはにお問い合わせください"ネットアップの営業問い合わせフォームを送信する"。マネージドアップグレードサービスおよびその他のタイプのアップグレードサポートは、追加料金なしで利用でき"SupportEdge Expertサービス"ます。

関連情報

- "サポートされるアップグレードパス"

ONTAPはいつアップグレードすればよいですか。

ONTAPソフトウェアは定期的にアップグレードする必要があります。ONTAPをアップグレードすると、新しい機能や拡張された機能を利用して、既知の問題に対する最新の修正を実装できます。

ONTAPのメジャーアップグレード

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

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

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

ONTAPパッチアップグレード

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

ONTAPリリースの詳細については、を参照して"推奨される最小パッチレベル"ください。

ONTAPのリリース日

ONTAP 9 .8リリース以降、NetAppではONTAPリリースを暦年に2回提供しています。計画は変更される可能性がありますが、新しいONTAPリリースは暦年の第2四半期と第4四半期に提供する予定です。この情報は、最新のONTAPリリースを利用するためのアップグレード期間を計画する際に使用します。

バージョン	リリース日
9.17.1	2025年9月
9.16.1	2025年1月
9.15.1	2024年7月
9.14.1	2024年1月
9.13.1	2023年6月
9.12.1	2023年2月
9.11.1	2022年7月
9.10.1	2022年1月
9.9.1	2021年6月

ONTAPのサポートレベル

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

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

関連情報

- 学び"現在サポートされているONTAPリリースの新機能"、
- 詳細については、をご覧ください "推奨される最小ONTAPリリース"。
- 詳細については、をご覧ください "ONTAPソフトウェアバージョンのサポート"。
- の詳細については、を"ONTAPリリースモデル"参照してください。

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

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

ONTAPソフトウェアのアップグレードを開始する準備ができている場合は、この手順を実行する必要はあり

ません。に従う必要があり"自動アップグレードプロセス"ます。この手順には、自動アップグレードの事前チェックが実行されます。

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

開始する前に

そうするべきだ"ターゲットのONTAPソフトウェアイメージのダウンロード"

の自動アップグレードの事前チェックを実行するには"直接マルチホップアップグレード"、目的のONTAPバージョンのソフトウェアパッケージのみをダウンロードします。実際のアップグレードを開始するまで、中間バージョンのONTAPをロードする必要はありません。たとえば、9.7から9.11.1へのアップグレードの自動アップグレード前チェックを実行する場合は、ONTAP 9 .11.1のソフトウェアパッケージをダウンロードする必要があります。ONTAP 9 8.1用のソフトウェアパッケージをダウンロードする必要はありません。

例 **2.** 手順

System Manager

1. ONTAPターゲットイメージを検証します。

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

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

実行中のバージョン	操作
ONTAP 9 .8以降	[クラスタ]>[概要]*をクリックします。
ONTAP 9.5 、 9.6 、および 9.7	[* Configuration * （設定 * ）] > [* Cluster * （クラスタ * ）] > [* Update * （アップデート *
ONTAP 9 .4以前	[* Configuration * （構成 * ）] > [* Cluster Update （クラスタの更新）] を

   b. [Overview]*ペインの右隅で、をクリックします ⋮。

   c. ONTAPアップデート*をクリックします。

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

状況	そしたら…。
ローカル フォルダーから新しいソフトウェアイメージを追加します。 すでにローカルクライアントに接続されている必要があります"イメージをダウンロードしました"。	i. で、[ローカルから追加]*をクリックします。 ii. ソフトウェアイメージを保存した場所を参照し、イメージを選択して、 * 開く * をクリックします。
HTTPサーバまたはFTPサーバから新しいソフトウェアイメージを追加する	i. [サーバーから追加] をクリックします。 ii. [新しいソフトウェアイメージの追加]ダイアログボックスで、NetApp Support SiteからONTAPソフトウェアイメージをダウンロードしたHTTPサーバまたはFTPサーバのURLを入力します。 匿名FTPのURLは、の形式で指定する必要があります ftp://anonymous@ftpserver。 iii. [追加]*をクリックします。
使用可能なイメージを選択	リストされている画像のいずれかを選択します。

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

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

CLI

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

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

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.15.1/image.tgz

Package download completed.
Package processing completed.
```

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

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

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

3. アップグレード前の自動チェックを実行します。

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

```
cluster1::> cluster image validate -version 9.15.1 -show-validation
-details true

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

4. 検証ステータスを確認します。

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

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

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

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

Details:

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

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

出力例

アップグレード前チェックの出力例全体

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to
be performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Use the Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system
supportability configuration information.

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


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

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

Details:

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

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

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

```
Details:

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

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

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

```
Configuration LDAP
Check
Node to SP/BMC       OK                N/A
connectivity check
OKM/KMIP enabled     OK                N/A
systems - Missing
keys check
ONTAP API to REST    Warning           Warning: NetApp ONTAP API has
been
transition warning                     used on this cluster for ONTAP
data
                                       storage management within the
last 30
                                       days. NetApp ONTAP API is
approaching
                                       end of availability.
                                       Action: Transition your
automation
                                       tools from ONTAP API to ONTAP
REST
                                       API. For more details, refer to
                                       CPC-00410 - End of availability:
                                       ONTAPI

https://mysupport.netapp.com/info/
                                       communications/ECMLP2880232.html
ONTAP Image          OK                N/A
Capability Status
OpenSSL 3.0.x        OK                N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                N/A
validation check
Platform Health      OK                N/A
Monitor check
Pre-Update           OK                N/A
Configuration
Verification
RDB Replica Health   OK                N/A
Check
Replicated database  OK                N/A
schema consistency
check
Running Jobs Status  OK                N/A
SAN LIF association  OK                N/A
status check
```

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

```
Overall Status       Warning           Warning
75 entries were displayed.
```

ONTAPのアップグレードの準備

ONTAPのアップグレードにかかる時間の決定

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

> 外部キー管理サーバおよびKey Management Interoperability Protocol（KMIP）でNetApp暗号化を使用している場合は、各HAペアのアップグレードに1時間以上かかることがあります。

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

Upgrade Advisorを使用してONTAPのアップグレードを準備する

の契約が有効な場合は"SupportEdgeサービス""Digital Advisor"、Upgrade Advisorを使用してアップグレードプランを生成することをお勧めします。

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

Digital Advisorは、ONTAPの新しいバージョンにアップグレードすることで解決できる環境内の問題を特定します。Upgrade Advisorサービスは、アップグレードの計画を支援し、アップグレード先のONTAPバージョンで認識しておく必要がある問題のレポートを提供します。

> Upgrade Advisorでレポートを作成するには、AutoSupportログが必要です。AutoSupportを有効にしている場合、Upgrade Advisorはログにアクセスでき、レポートを正常に作成できます。AutoSupportを有効にしていない場合は、有効にできます "AutoSupportファイルの手動アップロード"。

Digital Advisorの有効なSupport Edge Services契約を結んでいない場合は、次の"Upgrade Advisorを使用せずにアップグレードを準備する"手順を実行してください。

手順

1. "Active IQデジタルアドバイザの起動"
2. Digital Advisor"クラスタに関連するリスクを表示して手動で対処"の場合。

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

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

次のステップ

- Upgrade Advisorで、クラスタに推奨されるターゲットONTAPリリースのを確認し"ONTAPリリースノート"、Upgrade Advisorで生成された計画に従ってクラスタをアップグレードする必要があります。
- アップグレードを開始する前に実行する必要があります"SPまたはBMCをリブートする"。

Upgrade Advisorを使用せずにアップグレードを準備

Upgrade Advisorを使用せずにONTAPソフトウェアのアップグレードを準備する

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

の有効なSupportEdge契約がある場合は"Digital Advisor"、"Upgrade Advisorを使用したアップグレード計画"を参照してください。Active IQデジタルアドバイザ（デジタルアドバイザとも呼ばれます）にアクセスできない場合は、次の手順を実行してONTAPアップグレードの準備を行う必要があります。

1. "ターゲットのONTAPリリースを選択"です。
2. ターゲットリリースに対応した『』の「アップグレードに関する注意事項」および「既知の問題」および「制限事項」のセクションを確認してください"ONTAP 9 リリース ノート"。

   _アップグレードに関する注意事項_アップグレード前に把握しておくべき潜在的な問題について説明してください。_既知の問題と制限_アップグレード後に発生する可能性のある予期しないシステム動作について説明します。

   リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

3. "ハードウェア構成に対するONTAPのサポートの確認"です。

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

4. "Active IQ Config Advisorを使用して、一般的な構成エラーがないことを確認します。"
5. サポートされているONTAPを参照して"アップグレードパス"、直接アップグレードが可能か、アップグレードを段階的に完了する必要があるかを確認します。
6. "LIFフェイルオーバーの設定を確認する"です。

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

7. "SVMルーティング設定の確認"です。
8. "特別な考慮事項の確認"をクリックします。

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

実行する必要があります。

9. "SPまたはBMCをリブートする"です。

NetAppで推奨されるアップグレード先の**ONTAP**バージョンを選択

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

アップグレードの計画にUpgrade Advisorを使用しない場合は、NetAppの推奨事項に基づいてアップグレード対象のONTAPリリースを選択するか、またはパフォーマンスのニーズを満たす最小リリースを選択する必要があります。

- 利用可能な最新リリースへのアップグレード（推奨）

  NetAppは、ONTAPソフトウェアを、最新リリース番号のONTAPの最新パッチ バージョンにアップグレードすることを推奨しています。クラスタ内のストレージ システムで最新リリース番号がサポートされていないために当該バージョンへのアップグレードができない場合は、サポートされる最新の番号のリリースにアップグレードするようにしてください。

- 推奨される最小リリース

  クラスタで推奨される最小リリースにアップグレードを制限する場合は、を参照して、"推奨される最小ONTAPリリース"アップグレード先のONTAPのバージョンを確認します。

ハードウェア構成に対する**ONTAP**ターゲットリリースのサポートの確認

ONTAPをアップグレードする前に、使用しているハードウェア構成がターゲットのONTAPリリースでサポートされていることを確認する必要があります。

すべての構成

を使用 "NetApp Hardware Universe"して、ハードウェアプラットフォームおよびクラスタスイッチと管理スイッチがターゲットのONTAPリリースでサポートされていることを確認します。

アップグレード可能なONTAPのバージョンは、ハードウェア構成によっては制限される場合があります。アップグレード後のONTAPソフトウェアのバージョンがハードウェアでサポートされていない場合は、まずクラスタに新しいノードを追加し、データを移行し、古いノードを削除してから、ONTAPソフトウェアをアップグレードする必要があります。手順~を実行します"ONTAPクラスタに新しいノードを追加する"。

クラスタスイッチと管理スイッチには、クラスタネットワークスイッチ（NX-OS）、管理ネットワークスイッチ（IOS）、およびリファレンス構成ファイル（RCF）があります。クラスタスイッチと管理スイッチがサポート対象であるにもかかわらず、ターゲットのONTAPリリースに必要な最小限のソフトウェアバージョンを実行していない場合は、スイッチをサポート対象のソフトウェアバージョンにアップグレードします。

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

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

MetroClusterコウセイ

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

SANコウセイ

クラスタがSAN用に構成されている場合は、ONTAPをアップグレードする前に、を使用して "NetApp Interoperability Matrix Tool"、SAN構成が完全にサポートされていることを確認します。

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

Active IQ Config Advisor を使用して **ONTAP** をアップグレードする前に、一般的な構成エラーを特定します。

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

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

Active IQ Config Advisorのサポートには制限があり、オンラインでのみ利用できます。

手順

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

サポートされる**ONTAP**のアップグレードパス

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

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

現在の**ONTAP**バージョンを確認するには：

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

`show`。

アップグレードパスの種類

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

- 直接

  1つのソフトウェアイメージを使用して、隣接する次のONTAPリリースファミリーにいつでも直接アップグレードできます。多くのリリースでは、ソフトウェアイメージをインストールして、実行中のリリースよりも最大4リリース後のリリースに直接アップグレードすることもできます。

  たとえば、9.11.1から9.12.1への直接アップグレードパスや、9.11.1から9.15.1への直接アップグレードパスを使用できます。

  では、all_direct_upgradeパスがサポートされ"バージョンガコンザイノクラスタ"ます。

- ダイレクトマルチホップ

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

  たとえば、クラスタで9.3が実行されていて9.7にアップグレードする場合は、9.5と9.7の両方のONTAPインストールパッケージをロードしてから、9.7へのANDUを開始します。ONTAPは、最初にクラスタを9.5に、次に9.7に自動的にアップグレードします。このプロセスでは、テイクオーバー/ギブバック処理と関連するリブートが複数回発生することがあります。

- マルチステージ

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

  たとえば、現在9.6を実行している環境で9.11.1にアップグレードする場合は、まず9.6から9.8へ、次に9.8から9.11.1へのマルチステージアップグレードを完了する必要があります。以前のリリースからのアップグレードでは、3つ以上のステージといくつかの中間アップグレードが必要になる場合があります。

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

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

たとえば、ONTAP 9 .3P9を実行しているシステムで9.11.1にアップグレードする場合は、最初に最新の9.3パッチリリースにアップグレードしてから、9.3から9.11.1へのアップグレードパスに従ってください。

詳細はこちらをご覧ください "NetApp Support Siteで推奨されるONTAP の最小リリース数"。

サポートされるアップグレードパス

ここでは、ONTAPソフトウェアの自動アップグレードと手動アップグレードでサポートされるアップグレード パスをまとめています。これらのアップグレード パスは、オンプレミスのONTAPとONTAP Selectに適用されます。さまざまな "サポートされるCloud Volumes ONTAPのアップグレードパス"。

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

ONTAP 9 .10.1以降から

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスまたは手動アップグレードパス
9.16.1	9.17.1	直販
9.15.1	9.17.1	直販
	9.16.1	直販
9.14.1	9.17.1	直販
	9.16.1	直販
	9.15.1	直販
9.13.1	9.17.1	直販
	9.16.1	直販
	9.15.1	直販
	9.14.1	直販
9.12.1	9.17.1	マルチステージ • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	直販
	9.15.1	直販
	9.14.1	直販
	9.13.1	直販

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスまたは手動アップグレードパス
9.11.1	9.17.1	マルチステージ • 9.11.1 → 9.15.1 • 9.15.1 → 9.17.1
	9.16.1	マルチステージ • 9.11.1 → 9.15.1 • 9.15.1 → 9.16.1
	9.15.1	直販
	9.14.1	直販
	9.13.1	直販
	9.12.1	直販
9.10.1	9.17.1	マルチステージ • 9.10.1 → 9.14.1 • 9.14.1 → 9.17.1
	9.16.1	マルチステージ • 9.10.1 → 9.14.1 • 9.14.1 → 9.16.1
	9.15.1	マルチステージ • 9.10.1 → 9.14.1 • 9.14.1 → 9.15.1
	9.14.1	直販
	9.13.1	直販
	9.12.1	直販
	9.11.1	直販

ONTAP 9 .9.1から

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスまたは手動アップグレードパス
9.9.1	9.17.1	マルチステージ • 9.9.1 → 9.13.1 • 9.13.1 → 9.17.1
	9.16.1	マルチステージ • 9.9.1 → 9.13.1 • 9.13.1 → 9.16.1
	9.15.1	マルチステージ • 9.9.1 → 9.13.1 • 9.13.1 → 9.15.1
	9.14.1	マルチステージ • 9.9.1 → 9.13.1 • 9.13.1 → 9.14.1
	9.13.1	直販
	9.12.1	直販
	9.11.1	直販
	9.10.1	直販

ONTAP 9 .8から

MetroCluster IP構成の次のいずれかのプラットフォームモデルをONTAP 9.8から9.10.1以降にアップグレードする場合は、まずONTAP 9.9.1にアップグレードする必要があります。

- FAS2750
- FAS500f
- AFF A220用
- AFF A250用

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードまたは手動アップグレードパスは次のとおりです。
9.8	9.17.1	マルチステージ • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	マルチステージ • 9.8 → 9.12.1 • 9.12.1 → 9.16.1
	9.15.1	マルチステージ • 9.8 → 9.12.1 • 9.12.1 → 9.15.1
	9.14.1	マルチステージ • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
	9.13.1	マルチステージ • 9.8 → 9.12.1 • 9.12.1 → 9.13.1
	9.12.1	直販
	9.11.1	直販
	9.10.1	直販
	9.9.1	直販

ONTAP 9 .7から

ONTAP 9 .7からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。

自動パス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.7	9.17.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1
	9.15.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.15.1
	9.14.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
	9.13.1	マルチステージ • 9.7 → 9.9.1 • 9.9.1 → 9.13.1
	9.12.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.12.1
	9.11.1	ダイレクトマルチホップ（9.8および9.11.1のイメージが必要）
	9.10.1	ダイレクトマルチホップ（9.8および9.10.1P1以降のPリリースのイメージが必要）
	9.9.1	直販
	9.8	直販

シユトウハス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	手動アップグレードパス
9.7		

	9.11.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.11.1
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	手動アップグレードパス
	9.10.1	マルチステージ • 9.7 → 9.8 • 9.8 → 9.10.1
	9.9.1	直販
	9.8	直販

ONTAP 9 .6から

ONTAP 9 .6からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。

自動パス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.6		

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

シユトウハス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	手動アップグレードパス
9.6		

	9.11.1	マルチステージ • 9.6 → 9.8 • 9.8 → 9.11.1
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	手動アップグレードパス
	9.10.1	マルチステージ • 9.6 → 9.8 • 9.8 → 9.10.1
	9.9.1	マルチステージ • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	直販
	9.7	直販

ONTAP 9 .5から

ONTAP 9 .5からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。

自動パス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.5		

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

シュドウアップグレードパス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	手動アップグレードパス
9.5		

		• 9.5 → 9.7 • 9.7 → 9.9.1
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	手動アップグレードパス
	9.11.1	マルチステージ • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	マルチステージ • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
	9.9.1	マルチステージ • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	マルチステージ • 9.5 → 9.7 • 9.7 → 9.8
	9.7	直販
	9.6	直販

ONTAP 9 .4-9.0から

ONTAP 9 .4、9.3、9.2、9.1、9.0からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。

シトウアツフクレエトハス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.4		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...

	9.6	マルチステージ • 9.4 → 9.5 • 9.5 → 9.6
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
	9.5	直販

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.3		

		び9.7のイメージが必要） • 9.7 → 9.9.1
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
	9.12.1	マルチステージ • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
	9.11.1	マルチステージ • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	マルチステージ • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.10.1（ダイレクト マルチホップ、9.8および9.10.1のイメージが必要）
	9.9.1	マルチステージ • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.9.1
	9.8	マルチステージ • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.8
	9.7	ダイレクトマルチホップ（9.5および9.7のイメージが必要）
	9.6	マルチステージ • 9.3 → 9.5 • 9.5 → 9.6
	9.5	直販
	9.4	使用不可

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.2		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...

		• 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要）
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
	9.8	マルチステージ • 9.2 → 9.3 • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.8
	9.7	マルチステージ • 9.2 → 9.3 • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要）
	9.6	マルチステージ • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	マルチステージ • 9.3 → 9.5 • 9.5 → 9.6
	9.4	使用不可
	9.3	直販

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.1		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...

		• 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要）
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
	9.8	マルチステージ • 9.1 → 9.3 • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要） • 9.7 → 9.8
	9.7	マルチステージ • 9.1 → 9.3 • 9.3 → 9.7（ダイレクト マルチホップ、9.5および9.7のイメージが必要）
	9.6	マルチステージ • 9.1 → 9.3 • 9.3 → 9.6（ダイレクト マルチホップ、9.5および9.6のイメージが必要）
	9.5	マルチステージ • 9.1 → 9.3 • 9.3 → 9.5
	9.4	使用不可
	9.3	直販
	9.2	使用不可

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
9.0		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...

	9.3	マルチステージ • 9.0 → 9.1 • 9.1 → 9.3
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	自動アップグレードパスは...
	9.2	使用不可
	9.1	直販

シュドウアップグレードパス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス
9.4		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス

	9.7	マルチステージ • 9.4 → 9.5
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU** のアップグレードパス
	9.6	マルチステージ • 9.4 → 9.5 • 9.5 → 9.6
	9.5	直販

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス
9.3		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス

	9.7	マルチステージ • 9.3 → 9.5
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**AND** のアップグレードパス
	9.6	マルチステージ • 9.3 → 9.5 • 9.5 → 9.6
	9.5	直販
	9.4	使用不可

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス
9.2		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス

		• 9.3 → 9.5 • 9.5 → 9.7
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**AND** のアップグレードパス
	9.8	マルチステージ • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	マルチステージ • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	マルチステージ • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	マルチステージ • 9.2 → 9.3 • 9.3 → 9.5
	9.4	使用不可
	9.3	直販

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス
9.1		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス

		• 9.3 → 9.5 • 9.5 → 9.7
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**AND** のアップグレードパス
	9.8	マルチステージ • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	マルチステージ • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	マルチステージ • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	マルチステージ • 9.1 → 9.3 • 9.3 → 9.5
	9.4	使用不可
	9.3	直販
	9.2	使用不可

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス
9.0		

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	**ANDU**のアップグレードパス

		• 9.1 → 9.3 • 9.3 → 9.5
現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは ...	**AND** のアップグレードパス
	9.5	マルチステージ • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9.4	使用不可
	9.3	マルチステージ • 9.0 → 9.1 • 9.1 → 9.3
	9.2	使用不可
	9.1	直販

Data ONTAP 8

を使用して、お使いのプラットフォームでターゲットのONTAPリリースを実行できることを確認して "NetApp Hardware Universe"ください。

注： Data ONTAP 8.3アップグレードガイドでは、4ノードクラスタの場合、イプシロンが設定されているノードを最後にアップグレードするように計画してください。誤って記載されています。Data ONTAP 8 .2.3以降のアップグレードでは、この作業は不要になりました。詳細については、を参照してください "NetApp Bugs Online のバグ ID880277"。

Data ONTAP 8 .3.xから

ONTAP 9.1に直接アップグレードしてから、以降のリリースにアップグレードできます。

8.3.xより前の**Data ONTAP**リリース（**8.2.x**を含む）からのアップグレード

最初にData ONTAP 8.3.xにアップグレードし、次にONTAP 9.1にアップグレードしてから、以降のリリースにアップグレードする必要があります。

関連情報

- "ONTAPコマンド リファレンス"
- "cluster image showの実行"
- "system node image show」を参照してください"

アップグレード前の**ONTAP**クラスタ**LIF**のフェイルオーバー設定の確認

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

アップグレードプロセスでは、LIFはアップグレード方式に基づいて移行されます。アップグレード方法に応じて、LIFフェイルオーバーポリシーが使用される場合と使用されない場合があります。

クラスタにノードが8つ以上ある場合は、バッチ方式を使用して自動アップグレードが実行されます。バッチアップグレード方式では、クラスタを複数のバッチに分割し、最初のバッチに含まれるノードセットをアップグレードし、そのノードのハイアベイラビリティ（HA）パートナーをアップグレードしてから、残りのバッチについても同じ処理を繰り返します。ONTAP 9 .7以前でバッチ方式が使用される場合、LIFはアップグレードするノードのHAパートナーに移行されます。ONTAP 9 .8以降でバッチ方式が使用される場合は、LIFが他のバッチグループに移行されます。

クラスタのノードが8つ未満の場合は、ローリング方式を使用して自動アップグレードが実行されます。ローリングアップグレード方式では、HAペアの各ノードでフェイルオーバー処理を開始し、フェイルオーバーしたノードを更新してギブバックを開始します。この処理をクラスタ内のHAペアごとに繰り返します。ローリング方式が使用される場合、LIFはLIFフェイルオーバーポリシーの定義に従ってフェイルオーバーターゲットノードに移行されます。

手順

1. 各データLIFのフェイルオーバーポリシーを表示します。

ONTAPのバージョン	使用するコマンド
9.6以降	`network interface show -service-policy *data* -failover`
9.5以前	`network interface show -role data -failover`

次の例は、2つのデータLIFを含む2ノードクラスタのデフォルトのフェイルオーバー設定を示しています。

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
                                           node1:e0f, node0:e0b,
                                           node0:e0c, node0:e0d,
                                           node0:e0e, node0:e0f
```

「 * Failover Targets * 」フィールドには、各 LIF のフェイルオーバーターゲットが優先順位の高いものから順番に表示されます。たとえば、「lif0」がホームポート（node0のe0b）からフェイルオーバーすると、node0のポートe0cへのフェイルオーバーが最初に試行されます。lif0がe0cにフェイルオーバーできない場合は、node0のポートe0dなどへのフェイルオーバーが試行されます。

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. SAN LIF以外のLIFでフェイルオーバーポリシーが* disabled *に設定されている場合は、コマンドを使用して `network interface modify`フェイルオーバーを有効にします。

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

3. それぞれの LIF について、 LIF のホームノードのアップグレード時に稼働したままにする別のノードのデータポートが「 * Failover Targets * 」フィールドに含まれていることを確認します。

   フェイルオーバーグループにフェイルオーバーターゲットを追加するには、コマンドを使用し `network interface failover-groups modify`ます。

   例

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

関連情報

- "ネットワークおよびLIFの管理"
- "ネットワークインターフェイス"
- "network interface failover-groups modify"

アップグレード前の**ONTAP**クラスタ**SVM**ルーティング設定の確認

システム停止を回避するには、ONTAPソフトウェアをアップグレードする前に、より具体的なルートでは到達できないネットワークアドレスにデフォルトのSVMルートが到達できることを確認する必要があります。SVMにはデフォルトルートを1つ設定することを推奨します。詳細については、を参照してください "SU134：ONTAPの誤ったルーティング設定によってネットワークアクセスが中断されることがある"。

SVMのルーティングテーブルによって、SVMがデスティネーションとの通信に使用するネットワークパスが決まります。ネットワークの問題が発生する前に防止できるように、ルーティングテーブルの仕組みを理解することが重要です。

ルーティング ルールは次のとおりです。

- ONTAPは、最も限定的かつ使用可能なルートでトラフィックをルーティングします。
- より限定的なルートがない場合、最後の手段としてデフォルト ゲートウェイ ルート（0ビットのネットマスク）でトラフィックがルーティングされます。

デスティネーション、ネットマスク、メトリックが同じルートの場合、リブート後またはアップグレード後に同じルートが使用される保証はありません。これは、複数のデフォルトルートを設定している場合に特に問題になる可能性があります。

特別な考慮事項

アップグレード前に特定の**ONTAP**構成を確認する

特定のクラスタ構成では、ONTAPソフトウェアのアップグレードを開始する前に、固有の操作を実行する必要があります。たとえばSAN構成の場合は、アップグレードを開始する前に、適切な数の直接パスと間接パスを使用して各ホストが設定されていることを確認する必要があります。

次の表を参照して、実行する必要がある追加の手順がないかを確認してください。

ONTAPをアップグレードする前の確認事項	回答が * はい * の場合、次の操作を実行します ...
クラスタに複数のバージョンが混在していますか？	異なるバージョンの混在要件を確認
MetroCluster構成を使用していますか。	MetroCluster 構成の具体的なアップグレード要件を確認します
SAN構成を使用しているか。	SANホスト構成の確認
クラスタにSnapMirror関係が定義されているか。	"SnapMirror関係に対するONTAPのバージョンの互換性を確認する"

ONTAPをアップグレードする前の確認事項	回答が * はい * の場合、次の操作を実行します ...
DPタイプのSnapMirror関係が定義されていますか。ONTAP 9 12.1以降にアップグレードする必要がありますか。	"既存のDPタイプの関係をXDPに変換する"
SnapMirror S3を使用していますか？ONTAP 9 12.1以降にアップグレードしていますか？	"SnapMirror S3構成のライセンスを確認する"
カスケードの中間のボリュームで長期保存スナップショットが有効になっていますか?	"カスケードトポロジの中間ボリュームで長期保持のSnapshotを無効にする"
外部キー管理サーバでNetAppストレージ暗号化を使用できますか。	既存のキー管理サーバ接続を削除する
SVMにネットグループがロードされているか。	ネットグループファイルが各ノードに存在することを確認する
SVMを作成したか、ONTAP 9 12.1以前からそれ以降のバージョンにアップグレードしたか。	v4.2-xattrsオプションに明示的な値を割り当てる
SSLv3を使用するLDAPクライアントがあるか。	TLSを使用するためのLDAPクライアントの設定
セッション指向プロトコルを使用しているか。	セッション指向プロトコルの悪影響を確認する
管理者アカウントがSSH公開鍵を使用して認証するクラスタでSSL FIPSモードが有効になっていますか。	SSHホストキーアルゴリズムのサポートの確認
Autonomous Ransomware Protectionにはアクティブな警告がありますか？	異常なアクティビティに関する自律型ランサムウェア対策の警告に対応

バージョンが混在したクラスタに対する**ONTAP**のバージョンの互換性を確認する

バージョンが混在したONTAPクラスタでは、ノードで2つの異なるメジャーバージョンのONTAPが短時間実行されます。たとえば、ONTAP 9.8と9.12.1を実行しているノード、またはONTAP 9.9.1と9.13.1を実行しているノードを含むクラスタは、バージョンが混在したクラスタです。ONTAP 9.9.1P1と9.9.1P5のように、同じバージョン内で異なるパッチレベルを実行しているノードを含むクラスタは、異なるバージョンが混在したクラスタではありません。

Cloud Volumes ONTAPでは、バージョンの混在クラスタはサポートされません。

NetAppでは、一定期間、特定のシナリオにおいて、バージョンの異なるONTAPクラスタが混在してサポートされます。

ONTAPクラスタに複数のバージョンが混在する一般的なシナリオを次に示します。

- 大規模クラスタでのONTAPソフトウェアのアップグレード

  大規模なクラスタ内のすべてのノードのアップグレードには、数日から数週間かかることがあります。クラスタは、すべてのノードがアップグレードされるまでバージョンが混在した状態になります。

- クラスタに新しいノードを追加する場合はONTAPソフトウェアのアップグレードが必要

  クラスタに新しいノードを追加して容量を拡張したり、コントローラを完全に交換するプロセスで新しい

ノードを追加したりできます。いずれの場合も、既存のコントローラから新しいシステムの新しいノードにデータを移行するために、バージョンが混在した状態にしなければならない場合があります。

クラスタが最適に動作するためには、クラスタに複数のバージョンが混在した状態になるまでの時間をできるだけ短くする必要があります。クラスタに複数のバージョンが混在した状態でサポートされる最大期間は、クラスタ内の最も低いONTAPバージョンによって異なります。

混在バージョンのクラスタで実行されている**ONTAP**の最下位バージョン	バージョンが混在した状態を維持できる最大期間
ONTAP 9 .8以降	90日間
ONTAP 9.7以前	7日間

クラスタに複数のバージョンが混在している間は、アップグレードプロセスやデータ移行プロセスに必要なコマンドを除き、クラスタの処理や構成を変更するコマンドは実行しないでください。たとえば、LIFの移行、ストレージの計画的フェイルオーバー処理、大規模なオブジェクトの作成や削除などのアクティビティは、アップグレードとデータ移行が完了するまで実行しないでください。

ONTAPソフトウェアのアップグレードでサポートされるバージョンの混在クラスタ

現在の最小リリースからの直接アップグレードでサポートされている任意のONTAPバージョンとバージョンが混在した状態にすることができます。たとえば、ONTAP 9.11.1を実行している場合は、ONTAP 9.15.1を実行しているノードとバージョンが混在した状態になることがあります。ONTAP 9.11.1とONTAP 9.16.1を実行しているノードとバージョンが混在する状態にすることはできません。ONTAP 9.16.1は、ONTAP 9.11.1からの直接アップグレードではサポートされません。

ONTAPパッチ（P）リリースバージョンは、混合バージョンクラスタの互換性に影響を与えません。例えば、 ONTAP 9.11.1P6を実行している場合、混合バージョンクラスタの互換性のための現在のONTAPリリースはONTAP 9.11.1です。また、 ONTAP 9.12.1を実行していて、ONTAP 9.15.1P2にアップグレードする場合、混合バージョンクラスタの互換性のためのターゲットONTAPリリースはONTAP 9.15.1です。

現在のリリースからの直接アップグレードではサポートされていないバージョンのONTAPにアップグレードするには、複数段階のアップグレードを実行する必要があります。マルチステージアップグレードでは、最初に現在のリリースからの直接アップグレードでサポートされている最も高いリリースでバージョンが混在した状態になります。アップグレードが完了したら、ターゲットリリースに個別にアップグレードを実行します。たとえば、現在の最小リリースがONTAP 9.10.1で、ONTAP 9.16.1にアップグレードする場合は、まずすべてのノードをONTAP 9.14.1にアップグレードするためにバージョンが混在した状態にしてから、ONTAP 9.14.1からONTAP 9.16.1に個別にアップグレードします。との詳細については、こちらをご覧ください"複数の段階でのアップグレード""サポートされるアップグレードパス"。

バージョンが混在したクラスタに含めることができるONTAPのメジャーリリースは2つだけです。たとえば、ONTAP 9.13.1と9.151を実行しているノードやONTAP 9.13.1と9.16.1を実行しているノードで、バージョンが混在したクラスタを作成できます。ONTAP 9.13.1、9.151、および9.16.1を実行しているノードでバージョンを混在させることはできません。

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	アップグレードのバージョンが混在しています...
9.16.1	9.17.1	サポート対象

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	アップグレードのバージョンが混在しています...
9.15.1	9.17.1	サポート対象
	9.16.1	サポート対象
9.14.1	9.17.1	サポート対象
	9.16.1	サポート対象
	9.15.1	サポート対象
9.13.1	9.17.1	サポート対象
	9.16.1	サポート対象
	9.15.1	サポート対象
	9.14.1	サポート対象
9.12.1	9.17.1	サポート対象外
	9.16.1	サポート対象
	9.15.1	サポート対象
	9.14.1	サポート対象
	9.13.1	サポート対象
9.11.1	9.17.1	サポート対象外
	9.16.1	サポート対象外
	9.15.1	サポート対象
	9.14.1	サポート対象
	9.13.1	サポート対象
	9.12.1	サポート対象
9.10.1	9.17.1	サポート対象外
	9.16.1	サポート対象外
	9.15.1	サポート対象外
	9.14.1	サポート対象
	9.13.1	サポート対象
	9.12.1	サポート対象
	9.11.1	サポート対象

現在の **ONTAP** リリース	ターゲットとなる **ONTAP** リリースは **...**	アップグレードのバージョンが混在しています...
9.9.1	9.17.1	サポート対象外
	9.16.1	サポート対象外
	9.15.1	サポート対象外
	9.14.1	サポート対象外
	9.13.1	サポート対象
	9.12.1	サポート対象
	9.11.1	サポート対象
	9.10.1	サポート対象
9.8	9.17.1	サポート対象外
	9.16.1	サポート対象外
	9.15.1	サポート対象外
	9.14.1	サポート対象外
	9.13.1	サポート対象外
	9.12.1	サポート対象
	9.11.1	サポート対象
	9.10.1	サポート対象
	9.9.1	サポート対象

ONTAPクラスタへの新しいノードの追加

クラスタに新しいノードを追加する予定があり、それらのノードで最低限必要なONTAPバージョンが、現在クラスタで実行されているバージョンよりも新しい場合は、サポート範囲内でクラスタ内の既存のノードのソフトウェアをアップグレードしてから、新しいノードを追加する必要があります。既存のすべてのノードを、クラスタに追加するノードで最低限必要なONTAPバージョンにアップグレードするのが理想的です。ただし、既存のノードの一部で新しいバージョンのONTAPがサポートされていないためにそれができない場合は、アップグレード プロセスの一環として、限られた一定の期間、バージョンが混在する状態にならざるを得ません。

手順

1. "アップグレード"新しいコントローラで必要な最小ONTAPバージョンをサポートしていないノードが、新しいコントローラでサポートされる最大ONTAPバージョンまで。

   たとえば、FAS8080でONTAP 9.5が実行されていて、ONTAP 9.12.1が実行される新しいCシリーズ プラットフォームを追加する場合は、FAS8080をONTAP 9.8（サポートされる最上位のONTAPバージョン）

にアップグレードする必要があります。

2. "クラスタへの新しいノードの追加"です。
3. "データの移行"クラスタから削除するノードから新しく追加したノードに移動します。
4. "サポート対象外のノードをクラスタから削除します"です。
5. "アップグレード"クラスタ内の残りのノードを新しいノードと同じバージョンに変更します。

   必要に応じて、クラスタ全体（新しいノードを含む）を、新しいノードで実行されているONTAPのバージョンにアップグレードし"推奨される最新のパッチリリース"ます。

データ移行の詳細については、以下を参照してください。

- "アグリゲートを作成してボリュームを新しいノードに移動"
- "SANボリュームの移動用に新しいiSCSI接続をセットアップします"
- "暗号化を使用してボリュームを移動する"

MetroCluster構成の**ONTAP**のアップグレード要件を確認

MetroCluster構成のONTAPソフトウェアをアップグレードする前に、クラスタが一定の要件を満たしている必要があります。

- 両方のクラスタで同じバージョンのONTAPが実行されている必要があります。

  versionコマンドを使用すると、ONTAPのバージョンを確認できます。

- ONTAPのメジャーアップグレードを実行する場合は、MetroCluster設定を通常モードにする必要があります。
- パッチONTAPアップグレードを実行する場合は、MetroCluster設定を通常モードまたはスイッチオーバーモードのいずれかにすることができます。
- 2ノードクラスタを除くすべての構成で、両方のクラスタを同時に無停止アップグレードできます。

  2ノードクラスタの無停止アップグレードでは、クラスタのノードを一度に1つずつアップグレードする必要があります。

- 両方のクラスタ内のアグリゲートのRAIDステータスがresyncingでないことを確認してください。

  MetroClusterの修復中に、ミラーされたアグリゲートが再同期されます。MetroCluster構成がこの状態にあるかどうかを確認するには、 `storage aggregate plex show -in-progress true`指示。同期しているアグリゲートがある場合は、再同期が完了するまでアップグレードを実行しないでください。

  詳細はこちら `storage aggregate plex show`の中で"ONTAPコマンド リファレンス" 。

- アップグレードの実行中はネゴシエート スイッチオーバー処理が失敗します。

  アップグレード処理またはリバート処理時の問題を回避するために、両方のクラスタで同じバージョンのONTAPを実行しているとき以外は、アップグレードまたはリバート処理中に計画外のスイッチオーバーを実行しないでください。

MetroCluster通常運用時の構成要件

- ソースSVM LIFが稼働し、ホーム ノードに配置されている必要があります。

  デスティネーションSVMのデータLIFについては、稼働し、ホーム ノードに配置されている必要はありません。

- ローカル サイトにあるすべてのアグリゲートがオンラインになっている必要があります。
- ローカル クラスタのSVMが所有するルート ボリュームとデータ ボリュームがすべてオンラインになっている必要があります。

MetroClusterスイッチオーバー時の構成要件

- すべてのLIFが稼働し、ホーム ノードに配置されている必要があります。
- DRサイトにあるルート アグリゲートを除く、すべてのアグリゲートがオンラインになっている必要があります。

  DRサイトにあるルート アグリゲートは、スイッチオーバーの特定のフェーズ中はオフラインになります。

- すべてのボリュームがオンラインである必要があります。

関連情報

"MetroCluster構成のネットワークとストレージのステータスの確認"

ONTAPアップグレード前の**SAN**ホスト構成の確認

SAN環境でONTAPをアップグレードすると、直接パスが変更されます。SANクラスタをアップグレードする前に、各ホストに正しい数の直接パスと間接パスが設定されていること、および各ホストが正しいLIFに接続されていることを確認する必要があります。

手順

1. 各ホストで、十分な数の直接パスと間接パスが設定されていること、および各パスがアクティブであることを確認します。

   各ホストには、クラスタ内の各ノードへのパスが必要です。

2. 各ホストが各ノードのLIFに接続されていることを確認します。

   アップグレード後の比較のために、イニシエータのリストを記録しておく必要があります。ONTAP 9.11.1以降を実行している場合は、System Managerを使用して接続ステータスを確認すると、CLIよりもはるかにわかりやすくなります。

System Manager

a. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストがページに表示されます。リストが大きい場合は、ページの右下隅にあるページ番号をクリックして、リストの追加ページを表示できます。

   igroupに関するさまざまな情報が列に表示されます。9.11.1以降では、igroupの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると、詳細が表示されます。

CLI

- iSCSIイニシエータをリストします

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- FCイニシエータをリスト表示：

```
fcp initiator show -fields igroup,wwpn,lif
```

SnapMirror

SnapMirror関係に互換性があるONTAPのバージョン

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

ユニファイドレプリケーション関係

「 xdmp` 」タイプの SnapMirror 関係では、オンプレミスまたは Cloud Volumes ONTAP リリースを使用します。

ONTAP 9 .9.0以降：

- ONTAP 9 .x.0リリースはクラウドのみのリリースであり、Cloud Volumes ONTAPシステムをサポートします。リリースバージョンのあとにアスタリスク（*）が表示されている場合、クラウドのみのリリースです。

> ONTAP 9.16.0は、をサポートするため、クラウドのみのルールの例外です。"ASA r2システム"リリースバージョンのあとのプラス記号（+）は、ASA R2でサポートされているリリースを示します。ASA R2システムでは、他のASA R2システムとのSnapMirror関係のみがサポートされます。

- ONTAP 9 .x.1リリースは一般リリースであり、オンプレミスシステムとCloud Volumes ONTAPシステム

の両方をサポートします。

いる場合、"高度な容量分散"ONTAP 9.16.1以降を実行しているクラスタのボリュームでが有効になってONTAP 9.16.1より前のバージョンのONTAPを実行しているクラスタへのSnapMirror転送はサポートされません。

双方向の互換性があります。

- ONTAPバージョン 9.4 以降の相互運用性*

ONTAPバージョン…	ONTAP の以前のバージョンとの相互運用性…																				
	9.17.1	9.16.1	9.16.0以上	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4
9.17.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.0以上	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.0*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.14.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ

9.14.0*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.13.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.13.0*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ
9.12.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.12.0*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	いいえ	いいえ
9.11.1	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.11.0*	いいえ	いいえ	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	いいえ	いいえ
9.10.1	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.10.0*	いいえ	いいえ	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ
9.9.1	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.9.0*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	いいえ

9.8	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.7	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*

SnapMirror同期関係

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

ONTAPバージョン…	ONTAP の以前のバージョンとの相互運用性…												
	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.17.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.14.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.13.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.12.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.11.1	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ

9.10.1	いいえ	いいえ	* はい *	* はい *	* はい *	* はい *	* はい *	* はい *	* はい *	* はい *	いいえ	いいえ	いいえ
9.9.1	いいえ	いいえ	いいえ	* はい *	* はい *	* はい *	* はい *	* はい *	* はい *	* はい *	* はい *	いいえ	いいえ
9.8	いいえ	いいえ	いいえ	* はい *	* はい *	* はい *	いいえ	* はい *	* はい *	* はい *	* はい *	* はい *	いいえ
9.7	いいえ	いいえ	いいえ	いいえ	* はい *	* はい *	いいえ	いいえ	* はい *	* はい *	* はい *	* はい *	* はい *
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	* はい *	* はい *	* はい *	* はい *
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	* はい *	* はい *	* はい *

SnapMirror SVMディザスタリカバリ関係

SVMディザスタリカバリのデータと**SVM**保護の場合：

SVMディザスタリカバリは、同じバージョンのONTAPを実行するクラスタ間でのみサポートされます。バージョンに依存しないレプリケーションは**SVM**レプリケーションではサポートされません。

SVM移行のための**SVM**ディザスタリカバリの場合：

- ソース上のONTAPの以前のバージョンから、デスティネーション上のONTAPの同じバージョンまたはそれ以降のバージョンへのレプリケーションが単一方向でサポートされます。
- 次の表に示すように、ターゲットクラスタのONTAPのオンプレミスバージョンが2つ以上ないか、クラウドのメジャーバージョンが2つ以上ないようにする必要があります（ONTAP 9.9.0以降）。
  - 長期的なデータ保護のユースケースでは、レプリケーションはサポートされません。

リリースバージョンのあとにアスタリスク（*）が表示されている場合、クラウドのみのリリースです。

サポートを確認するには、左側の表の列でソースバージョンを確認し、一番上の行でデスティネーションバージョンを確認します（類似バージョンの場合はDR/Migration、新しいバージョンの場合はMigrationのみ）。

ソース	デスティネーション																				
	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1
9.4	DR/移行	移行	移行																			
9.5		DR/移行	移行	移行																		
9.6			DR/移行	移行	移行																	

9.7				DR/移行	移行	移行															
9.8					DR/移行	移行	移行														
9.9.0*						DR/移行	移行	移行	移行	移行	移行										
9.9.1							DR/移行	移行	移行	移行	移行										
9.10.0*								DR/移行	移行	移行	移行	移行	移行								
9.10.1									DR/移行	移行	移行	移行	移行								
9.11.0*										DR/移行	移行	移行	移行	移行	移行						
9.11.1											DR/移行	移行	移行	移行	移行						
9.12.0*												DR/移行	移行	移行	移行	移行	移行				
9.12.1													DR/移行	移行	移行	移行	移行				
9.13.0*														DR/移行	移行	移行	移行	移行			
9.13.1															DR/移行	移行	移行	移行	移行		
9.14.0*																DR/移行	移行	移行	移行	移行	
9.14.1																	DR/移行	移行	移行	移行	移行	
9.15.0*																		DR/移行	移行	移行	移行	移行
9.15.1																			DR/移行	移行	移行	移行

9.16.0																				DR/移行	移行	移行
9.16.1																					DR/移行	移行
9.17.1																						DR/移行

SnapMirrorテイサスタリカハリカンケイ

タイプが「 `D」 でポリシータイプが「 async 」の SnapMirror 関係の場合：

DPタイプのミラーは、ONTAP 9 .11.1以降では初期化できません。ONTAP 9 12.1では完全に廃止されています。詳細については、を参照してください "データ保護SnapMirror関係の廃止"。

次の表で、左側の列はソースボリュームのONTAPバージョン、上部の列はデスティネーションボリュームで使用できるONTAPバージョンを示しています。

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

双方向の互換性はありません。

既存の**ONTAP SnapMirror DP**タイプの関係を**XDP**に変換する

XDP 12.1以降にアップグレードする場合ONTAP 9は、アップグレード前にDPタイプの関係をXDPに変換する必要があります。ONTAP 9.12.1以降では、DPタイプの関係はサポートされません。既存のDPタイプの関係を簡単にXDPに変換して、バージョンに依存しないSnapMirrorを活用できます。

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

タスクの内容

- SnapMirrorは、既存のDPタイプの関係をXDPに自動的に変換しません。関係を変換するには、既存の関係を解除して削除し、新しいXDP関係を作成して関係を再同期する必要があります。
- 変換を計画するときは、XDP SnapMirror関係のバックグラウンド準備とデータウェアハウジングフェーズに時間がかかることに注意してください。ステータスが「準備中」と長時間報告されるSnapMirror関係が表示されることも珍しくありません。

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

手順

1. デスティネーションクラスタから、SnapMirror関係のタイプがDP、ミラーの状態がSnapMirrored、関係のステータスがIdle、関係が正常であることを確認します。

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

次の例は、コマンドの出力を示してい `snapmirror show`ます。

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

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

関係設定の既存の情報を追跡するために、コマンド出力のコピーを保持しておくと便利 `snapmirror show`です。の詳細については `snapmirror show`、を"ONTAPコマンドリファレンス"参照してください。

2. ソースボリュームとデスティネーションボリュームで、両方のボリュームに共通のSnapshotがあることを確認します。

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

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

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


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

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

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

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

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を休止し `volA`ます。

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

の詳細については `snapmirror quiesce`、を"ONTAPコマンド リファレンス"参照してください。

4. 既存のDPタイプの関係を解除します。

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

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

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を解除し `volA`ます。

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

の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

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

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

次の例は、デスティネーションボリュームでSnapshotの自動削除を無効にし `volA_dst`ます。

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

6. 既存のDPタイプの関係を削除します。

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

の詳細については `snapmirror-delete`、を"ONTAPコマンド リファレンス"参照してください。

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

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を削除し `volA`ます。

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

7. ソースで元のSVMディザスタリカバリ関係を解放します。

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

次の例は、SVMディザスタリカバリ関係をリリースします。

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

の詳細については `snapmirror release`、を"ONTAPコマンド リファレンス"参照してください。

8. コマンドで保持した出力を使用して、新しいXDPタイプの関係を作成でき `snapmirror show`ます。

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

新しい関係では、同じソースボリュームとデスティネーションボリュームを使用する必要があります。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

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

次の例は、 `svm1`デフォルトのポリシーを使用して `MirrorAllSnapshots`、の `svm_backup`ソースボリュームとデスティネーションボリューム `volA_dst`の間にSnapMirrorディザスタリカバリ関係を作成します `volA`。

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

9. ソースボリュームとデスティネーションボリュームを再同期します。

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

再同期時間を改善するには、 `-quick-resync`オプションですが、ストレージ効率の節約が失われる可能性があることに注意してください。

このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を再同期し `volA`ます。

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

詳細はこちら `snapmirror resync`の中で"ONTAPコマンド リファレンス" 。

10. Snapshotの自動削除を無効にした場合は、再度有効にします。

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

終了後

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

   の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

2. SnapMirror XDPデスティネーションボリュームでSnapMirrorポリシーの定義に従ってSnapshotの更新が開始されたら、ソースクラスタからコマンドの出力を使用し `snapmirror list-destinations`て新しいSnapMirror XDP関係を表示します。

DPタイフノカンケイニカンスルシヨウサイシヨウホウ

ONTAP 9.3以降では、XDPモードがデフォルトであり、コマンドラインまたは新規または既存のスクリプトでのDPモードの呼び出しは自動的にXDPモードに変換されます。

既存の関係には影響しません。すでにDPタイプの関係は、引き続きDPタイプになります。ONTAP 9.5以降では、データ保護モードを指定しない場合、またはXDPモードを関係タイプとして指定した場合にデフォルトポ

リシーがMirrorAndVaultになります。次の表は、想定される動作を示しています。

指定するモード	タイプ	デフォルトポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAndVault（ユニファイドレプリケーション）
XDP	XDP	MirrorAndVault（ユニファイドレプリケーション）

次の表に示すように、さまざまな状況でXDPに割り当てられたデフォルトポリシーによって、変換時に以前のタイプと同等の機能が維持されます。もちろん、ユニファイドレプリケーションのポリシーなど、必要に応じてさまざまなポリシーを使用できます。

指定するモード	ポリシー	結果
DP	MirrorAllSnapshots	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault
ユニファイドレプリケーション	XDP	MirrorAllSnapshots
SnapMirror DR	XDPDefault	SnapVault

変換の例外は次のとおりです。

- ONTAP 9 .3以前のSVMデータ保護関係のデフォルトは引き続きDPモードです。

  ONTAP 9 .4以降では、SVMデータ保護関係のデフォルトがXDPモードに変更されました。

- ルートボリュームの負荷共有データ保護関係のデフォルトは引き続きDPモードです。
- ONTAP 9 .4以前のSnapLockデータ保護関係のデフォルトは引き続きDPモードです。

  XDP 5以降ONTAP 9では、SnapLockデータ保護関係のデフォルトがXDPモードに変更されました。

- 次のクラスタ全体のオプションを設定した場合、DPの明示的な呼び出しは引き続きデフォルトでDPモードになります。

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

  DPを明示的に呼び出さない場合、このオプションは無視されます。

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"

ONTAPのアップグレード前に長期保持の**Snapshot**を無効にする

カスケード ボリュームの関係では、 ONTAP 9 のすべてのバージョンにおいて、長期保存 (LTR) スナップショットはカスケードの最後のSnapMirror宛先ボリュームでのみサポートされます。カスケード内の中間のボリュームで LTR スナップショットを有効にすると、バックアップとスナップショットが失われます。

詳細はこちら"長期保存スナップショット"。

カスケードの中間ボリュームでLTRスナップショットが有効になっているサポートされていない構成の場合は、テクニカルサポートに連絡して、"NetAppナレッジベース: 長期保存 (LTR) スナップショットが有効になっているボリュームのカスケード接続はサポートされていません"援助をお願いします。

次のONTAPバージョンでは、最終的なSnapMirror宛先ボリュームを除くカスケード内のどのボリュームでもLTR スナップショットを有効にできません。

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

カスケードの中間ボリュームで LTR スナップショットを有効にできるONTAPバージョンから、それをブロックするONTAPバージョンにアップグレードする前に、バックアップとスナップショットの欠落を回避するために LTR スナップショットを無効にする必要があります。

次のような場合に対処する必要があります。

- 長期保持（LTR）Snapshotは、SnapMirrorカスケードの「B」ボリューム、または大きなカスケードの別の中間SnapMirrorデスティネーションボリュームで構成されます。
- LTR Snapshotは、SnapMirrorポリシールールに適用されるスケジュールによって定義されます。このルールでは、Snapshotはソースボリュームからはレプリケートされませんが、デスティネーションボリュームに直接作成されます。

スケジュールとSnapMirrorポリシーの詳細については、"NetAppナレッジベース: ONTAP 9 SnapMirrorポリシー ルールの「スケジュール」パラメータはどのように機能しますか?" 。

手順

1. カスケードの中間ボリュームのSnapMirrorポリシーからLTRルールを削除します。

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
-snapmirror-label <>
```

詳細はこちら `snapmirror policy remove-rule`の中で"ONTAPコマンド リファレンス" 。

2. LTRスケジュールを指定せずに、SnapMirrorラベルのルールを再度追加します。

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>
-snapmirror-label <> -keep <>
```

SnapMirrorポリシールールからLTR Snapshotを削除すると、SnapMirrorは指定されたラベルのSnapshotをソースボリュームからプルします。適切なラベルが設定されたSnapshotを作成するために、ソースボリュームのSnapshotポリシーでスケジュールの追加や変更が必要になる場合もあります。

の詳細については `snapmirror policy add-rule`、を"ONTAPコマンド リファレンス"参照してください。

3. 必要に応じて、ソースボリュームのSnapshotポリシーでスケジュールを変更（または作成）して、SnapMirrorラベルのSnapshotを作成できるようにします。

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

LTRスナップショットは、SnapMirrorカスケード構成内の最終的なSnapMirrorデスティネーションボリュームで引き続き有効にすることができます。

SnapMirror S3構成のONTAPライセンスの確認

SnapMirror S3を使用していて、ONTAP 9 12.1以降にアップグレードする場合は、ONTAPをアップグレードする前に、適切なSnapMirrorライセンスがあることを確認する必要があります。

ONTAPのアップグレード後に、ONTAP 9 .11.1以前とONTAP 9 .12.1以降の間でライセンスを変更すると、SnapMirror S3関係が失敗することがあります。

ONTAP 9.11.1以前

- NetAppでホストされるデスティネーションバケット（ONTAP S3またはStorageGRID）にレプリケートする場合、"ONTAP One"ソフトウェアスイートが導入される前に、SnapMirror S3はデータ保護バンドルに含まれているSnapMirror同期ライセンスを確認します。
- NetApp以外のデスティネーションバケットにレプリケートする場合、SnapMirror S3は、"ONTAP One"ソフトウェアスイートの導入前に提供されていたHybrid Cloud Bundleに含まれているSnapMirrorクラウドライセンスを確認します。

ONTAP 9.12.1以降

- NetAppでホストされるデスティネーションバケット（ONTAP S3またはStorageGRID）にレプリケートする場合、SnapMirror S3は、"ONTAP One"ソフトウェアスイートの導入前に提供されていたデータ保護バンドルに含まれているSnapMirror S3ライセンスを確認します。
- NetApp以外のデスティネーションバケットにレプリケートする場合、SnapMirror S3はSnapMirror S3 Externalライセンスを確認します。このライセンスは、"ONTAP One"ソフトウェアスイートとの導入前に提供されていたHybrid Cloud Bundleに含まれて"ONTAP One互換バンドル"います。

既存の**SnapMirror S3**関係

クラスタに新しいライセンスがなくても、ONTAP 9 .11.1以前からONTAP 9 .12.1以降にアップグレードしたあとも、既存のSnapMirror S3関係は引き続き機能します。

クラスタに適切なライセンスがインストールされていないと、新しいSnapMirror S3関係の作成が失敗します。

ONTAPのアップグレード前に既存の外部キー管理サーバの接続を削除する

ONTAPをアップグレードする前に、NetAppストレージ暗号化（NSE）でONTAP 9 .2以前を実行していて、ONTAP 9 .3以降にアップグレードする場合は、コマンドラインインターフェイス（CLI）を使用して既存の外部キー管理（KMIP）サーバの接続を削除する必要があります。

手順

1. NSEドライブのロックが解除されて開いていること、デフォルトのメーカーセキュアIDである0x0に設定されていることを確認します。

   ```
   storage encryption disk show -disk *
   ```

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

2. advanced権限モードに切り替えます。

   ```
   set -privilege advanced
   ```

   の詳細については `set`、を"ONTAPコマンド リファレンス"参照してください。

3. デフォルトのメーカーセキュアIDである0x0を使用して、FIPSキーを自己暗号化ディスク（SED）に割り当てます。

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

の詳細については `storage encryption disk modify`、を"ONTAPコマンド リファレンス"参照してください。

4. すべてのディスクへのFIPSキーの割り当てが完了したことを確認します。

```
storage encryption disk show-status
```

の詳細については `storage encryption disk show-status`、を"ONTAPコマンド リファレンス"参照してください。

5. すべてのディスクの* mode *がdataに設定されていることを確認します。

```
storage encryption disk show
```

の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

6. 設定されているKMIPサーバを表示します。

```
security key-manager keystore show
```

詳細はこちら `security key-manager keystore show`の中で"ONTAPコマンド リファレンス"。

7. 設定されているKMIPサーバを削除します。

```
security key-manager delete -address <kmip_ip_address>
```

の詳細については `security key-manager delete`、を"ONTAPコマンド リファレンス"参照してください。

8. 外部キー管理ツールの設定を削除します。

```
security key-manager external disable
```

詳細はこちら `security key-manager external disable`の中で"ONTAPコマンド リファレンス"。

この手順でNSE証明書が削除されることはありません。

次のステップ

アップグレードが完了したら、を実行する必要がありますKMIPサーバ接続を再設定する。

ONTAPのアップグレード前にネットグループファイルがすべてのノードに存在することを確認する

ONTAPをアップグレードする前に、ネットグループをStorage Virtual Machine（SVM）にロードした場合は、ネットグループファイルが各ノードに存在することを確認する必要があります。ノード上にネットグループファイルが見つからないと、アップグレードが失敗する可能性があります。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 各SVMのネットグループのステータスを表示します。

```
vserver services netgroup status
```

3. SVMごとに、各ノードに表示されているネットグループ ファイルのハッシュ値が同じであることを確認します。

```
vserver services name-service netgroup status
```

ハッシュ値が同じであれば、次の手順をスキップしてアップグレードまたはリバートを開始できます。それ以外の場合は、次の手順に進みます。

4. クラスタのいずれかのノードで、ネットグループ ファイルを手動でロードします。

```
vserver services netgroup load -vserver vserver_name -source uri
```

このコマンドは、すべてのノードにネットグループ ファイルをダウンロードします。ノード上に既存のネットグループ ファイルがある場合は、そのファイルが上書きされます。

関連情報

"ネットグループの使用"

ONTAPをアップグレードする前に、v4.2-xattrsオプションに明示的な値を割り当てる

NFSv4.2クライアントを使用している場合は、ONTAP 9の特定のリリースおよびパッチからアップグレードする前に、NFSv4.2拡張属性オプションに明示的な値を指定して、アップグレード後のNFS応答エラーを回避する必要があります。

影響を受けるバージョンにONTAPをアップグレードする前にオプションに値が明示的に割り当てられていない場合、 `v4.2-xattrs`NFSv4.2クライアントにはサーバのextended attributesオプションが変更されたことが通知されません。これにより、クライアントとサーバの不一致が原因で、特定のコールに対するNFS応答エラーが発生し `xattrs`ます。

開始する前に

次の条件に該当する場合は、NFSv4.2拡張属性オプションに明示的な値を割り当てる必要があります。

- NFSv4.2を使用して、ONTAP 9 .11.1以前を使用して作成したSVMを使用している。
- 次の影響を受けるリリースおよびパッチからONTAPをアップグレードします。
  - 9.12.1RC1～9.12.1P11
  - 9.13.1RC1～9.13.1P8
  - 9.14.1RC1～9.14.1P1

タスクの内容

この手順で説明するコマンドを使用して値を設定するには、ONTAP 9 12.1以降を実行している必要があります。

がすでにに設定されて `enabled`いる場合は `v4.2-xattrs`、今後の中断を回避するために明示的にに設定する必要があります `enabled`。disabledに設定する `v4.2-xattrs`と、`NFSv4.2`クライアントは、再マウントされるか、オプションがに設定される `enabled`まで、「`invalid argument`」応答を受信できます `v4.2-xattrs`。

手順

- オプションに明示的な値を割り当て `v4.2-xattrs`ます。

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

関連情報

"nfs v4.2-xattrsフィールドがアップグレード後に反転する"

ONTAPのアップグレード前に**TLS**を使用するように**LDAP**クライアントを設定する

ONTAPをアップグレードする前に、TLSを使用するLDAPサーバとのセキュアな通信を実現するために、SSLv3を使用するLDAPクライアントを設定する必要があります。アップグレード後はSSLを使用できなくなります。

デフォルトでは、クライアントアプリケーションとサーバアプリケーション間のLDAP通信は暗号化されません。SSLの使用を禁止し、強制的にTLSを使用する必要があります。

手順

1. 環境内のLDAPサーバがTLSをサポートしていることを確認します。

   サポートされていない場合は、次の手順に進まないでください。TLSをサポートするバージョンにLDAPサーバをアップグレードする必要があります。

2. どのONTAP LDAPクライアント設定でSSL / TLS経由のLDAPが有効になっているかを確認します。

```
vserver services name-service ldap client show
```

SSL / TLS経由のLDAPが有効になっているLDAPクライアント設定がない場合は、残りの手順をスキップできます。ただし、セキュリティを強化するには、TLS経由のLDAPの使用を検討してください。

3. LDAPクライアントごとに、SSLの使用を禁止し、強制的にTLSを使用するように設定します。

```
vserver services name-service ldap client modify -vserver <vserver_name>
-client-config <ldap_client_config_name> -allow-ssl false
```

4. すべてのLDAPクライアントでSSLの使用が許可されていないことを確認します。

```
vserver services name-service ldap client show
```

関連情報

"NFSの管理"

ONTAP アップグレード時のセッション指向プロトコルの悪影響について学習します

クラスタおよびセッション指向プロトコルは、アップグレード中のI/Oサービスなど、特定の領域のクライアントとアプリケーションに悪影響を及ぼす可能性があります。

セッション指向プロトコルを使用する場合は、次の点を考慮してください。

- SMB

  SMBv3 で継続的可用性（ CA ）共有を提供する場合は、自動無停止アップグレード方式（ System Manager または CLI を使用）を使用できます。クライアントによる中断は発生しません。

  SMBv1またはSMBv2を使用した共有、またはSMBv3を使用したCA以外の共有を提供する場合は、アップグレードのテイクオーバー処理やリブート処理の実行中にクライアントセッションが中断されます。アップグレードの開始前に、ユーザにセッションを終了するように通知してください。

  Hyper-VおよびSQL Server over SMBはノンストップ オペレーション（NDO）をサポートします。Hyper-VまたはSQL Server over SMBソリューションを設定した場合は、ONTAPのアップグレード中にもアプリケーション サーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持し、継続的可用性を実現します。

- NFSv4.x

  NFSv4.xクライアントは、NFSv4.xの通常のリカバリ手順を使用してアップグレード中に発生する接続の切断から自動的にリカバリします。このプロセスの実行中、アプリケーションで一時的なI/O遅延が発生することがあります。

- NDMP

  状態が失われるため、クライアントユーザは処理を再試行する必要があります。

- バックアップとリストア

  状態が失われるため、クライアントユーザは処理を再試行する必要があります。

  > アップグレード中またはアップグレード直前にバックアップまたはリストアを開始しないでください。データが失われる可能性があります。

- アプリケーション（OracleやExchangeなど）

  影響はアプリケーションによって異なります。タイムアウト ベースのアプリケーションでは、タイムアウトの値を変更し、ONTAPのリブート時間よりも長く設定することで、悪影響を最小限に抑えることができます。

ONTAPのアップグレード前に**SSH**ホストキーアルゴリズムのサポートを確認する

ONTAPをアップグレードする前に、SSH公開鍵を使用して管理者アカウントを認証するクラスタでSSL FIPSモードが有効になっている場合は、ターゲットのONTAPリリースでホストキーのアルゴリズムがサポートされていることを確認する必要があります。

次の表に、ONTAP SSH接続でサポートされるホストキータイプアルゴリズムを示します。これらのキータイプは、SSH公開認証の設定には適用されません。

ONTAP リリース	FIPSモードでサポートされるキータイプ	FIPS以外のモードでサポートされるキータイプ
9.11.1以降	ECDSA - sha2 - nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss+ ssh-rsa
9.10.1以前	ECDSA - sha2 -nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss+ ssh-rsa

> ssh-ed25519ホスト・キー・アルゴリズムのサポートは、ONTAP 9 .11.1以降で削除されました。

詳細については、を参照してください "FIPS を使用してネットワークセキュリティを設定する"。

サポートされているキーアルゴリズムがない既存のSSH公開鍵アカウントは、アップグレード前にサポートされているキータイプで再設定する必要があります。そうしないと、管理者認証が失敗します。

"SSH公開鍵アカウントの有効化の詳細については、こちらを参照してください。"

ONTAPのアップグレード前にAutonomous Ransomware Protection（ARP；自律ランサムウェア対策）のアクティビティに関する警告を解決する

ONTAP 9 .16.1以降にアップグレードする前に、Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）によって報告された異常なアクティビティの警告に対応する必要があります。ONTAP 9 .16.1では、ARPは機械学習/人工知能（AI）ベースのモデルに変更された。この変更により、ONTAP 9内の既存のARPからの未解決のアクティブな警告がアップグレード後に失われます。

手順

1. で報告された異常なアクティビティに関する警告に対応し"ARP"、潜在的な問題を解決します。
2. アップグレード前に* Update and Clear Suspect File Types *を選択して決定内容を記録し、通常のARPモニタリングを再開して、これらの問題の解決を確認します。

SPまたはBMCをリブートしてONTAPアップグレード時のファームウェア更新を準備する

ONTAPのアップグレード前にファームウェアを手動で更新する必要はありません。クラスタのファームウェアはONTAPアップグレードパッケージに含まれており、各ノードのブートデバイスにコピーされます。新しいファームウェアは、アップグレードプロセスの一環としてインストールされます。

クラスタ内の次のコンポーネントのファームウェアのバージョンがONTAPアップグレードパッケージにバンドルされているファームウェアより古い場合は、自動的に更新されます。

- BIOS / Loader
- サービスプロセッサ（SP）またはベースボード管理コントローラ（BMC）
- ストレージシェルフ
- ディスク
- Flash Cache

スムーズに更新できるよう準備するには、アップグレードを開始する前にSPまたはBMCをリブートする必要があります。

ステップ

1. アップグレードの前にSPまたはBMCをリブートします。

```
system service-processor reboot-sp -node <node_name>
```

一度に1つのSPまたはBMCだけをリブートします。リブートしたSPまたはBMCが完全にリサイクルされるまで待ってから、次のSPまたはBMCをリブートします。

ONTAPのアップグレード間のアップグレードも可能です"ファームウェアを手動で更新します"。Digital Advisorをお持ちの場合は可能です"ONTAP イメージに現在含まれているファームウェアバージョンのリストを表示します"。

更新されたファームウェアバージョンは次のとおりです。

- "システムファームウェア（BIOS、BMC、SP）"
- "シェルフファームウェア"
- "ディスクおよびFlash Cacheファームウェア"

アップグレード前に**ONTAP**ソフトウェアイメージをダウンロードする

ONTAPをアップグレードする前に、まずNetAppサポートサイトからターゲットのONTAPソフトウェアイメージをダウンロードする必要があります。ONTAPのリリースに応じて、ONTAPソフトウェアをネットワーク上のHTTPS、HTTP、FTPサーバ、またはローカルフォルダにダウンロードできます。

実行中のバージョン	イメージをダウンロードできる場所
ONTAP 9.6以降	• HTTPS サーバ + サーバの CA 証明書がローカルシステムにインストールされている必要があります。 • ローカルフォルダ • HTTPサーバまたはFTPサーバ
ONTAP 9.4以降	• ローカルフォルダ • HTTPサーバまたはFTPサーバ
ONTAP 9.0以降	HTTPサーバまたはFTPサーバ

タスクの内容

- を使用して自動無停止アップグレード（ANDU）を実行する場合"マルチホップの直接アップグレードパス"は、アップグレードに必要な中間ONTAPバージョンとターゲットONTAPバージョンの両方に対応するソフトウェアパッケージが必要"ダウンロード"です。たとえば、ONTAP 9 .8からONTAP 9 .13.1にアップグレードする場合は、ONTAP 9 .12.1とONTAP 9 .13.1の両方のソフトウェアパッケージをダウンロードする必要があります。アップグレードパスで中間ソフトウェアパッケージのダウンロードが必要かどうかを確認するには、を参照してください"サポートされるアップグレードパス"。
- NetAppボリューム暗号化を搭載したシステムをONTAP 9 .5以降にアップグレードする場合は、規制対象外の国のONTAPソフトウェアイメージ（NetAppボリューム暗号化を含む）をダウンロードする必要があります。

  制限された国のONTAPソフトウェアイメージを使用してNetAppボリューム暗号化を有効にしたシステムをアップグレードすると、システムがパニック状態になり、ボリュームにアクセスできなくなります。

- ファームウェア用のソフトウェアパッケージを別途ダウンロードする必要はありません。クラスタのファームウェアの更新は、ONTAPソフトウェアのアップグレードパッケージに含まれており、各ノードのブートデバイスにコピーされます。新しいファームウェアは、アップグレードプロセスの一環としてインストールされます。

手順

1. "ソフトウェアのダウンロード"NetAppサポートサイトの領域で、対象のONTAPソフトウェアを探します。

ONTAP Select のアップグレードの場合は、* ONTAP Select Node Upgrade*を選択します。

2. ソフトウェアイメージ（97_q_image.tgzなど）を適切な場所にコピーします。

   ONTAPのリリースによっては、イメージがローカルシステムに提供されるディレクトリ、またはストレージシステム上のローカルフォルダに格納されるディレクトリ、HTTP'HTTPS'FTPサーバのいずれかになります。

ONTAPのアップグレード方法

ONTAPソフトウェアのアップグレード方法

System Managerを使用して、 ONTAPソフトウェアの自動アップグレードを実行できます。また、 ONTAPコマンドラインインターフェイス（CLI）を使用して、自動または手動のアップグレードを実行することもできます。ONTAPのONTAP方法は、構成、現在のONTAPのバージョン、およびクラスタ内のノード数によって異なります。NetApp は、別のアプローチが求められる構成でないかぎり、System Managerを使用して自動アップグレードを実行することを推奨しています。たとえば、 ONTAP 9.3以降を実行している4ノードのMetroCluster構成の場合は、System Managerを使用して自動アップグレード（自動無停止アップグレード、またはANDUと呼ばれることもあります）を実行する必要があります。

NetAppコンソールからONTAP 9.15.1以降にアップグレードする場合は、"NetAppコンソールのドキュメントのアップグレード手順" 。

アップグレードは、ローリング アップグレード プロセスかバッチ アップグレード プロセスを使用して実行できます。どちらも無停止で実行できます。

自動アップグレードでは、ONTAPによってターゲットのONTAPイメージが各ノードに自動的にインストールされ、クラスタのコンポーネントが検証されてクラスタを無停止でアップグレードできることが確認されてから、ノードの数に基づいて、バッチ アップグレードかローリング アップグレードがバックグラウンドで実行されます。手動アップグレードでは、管理者がクラスタ内の各ノードをアップグレードする準備ができていることを手動で確認してから、ローリング アップグレードの手順を実行します。

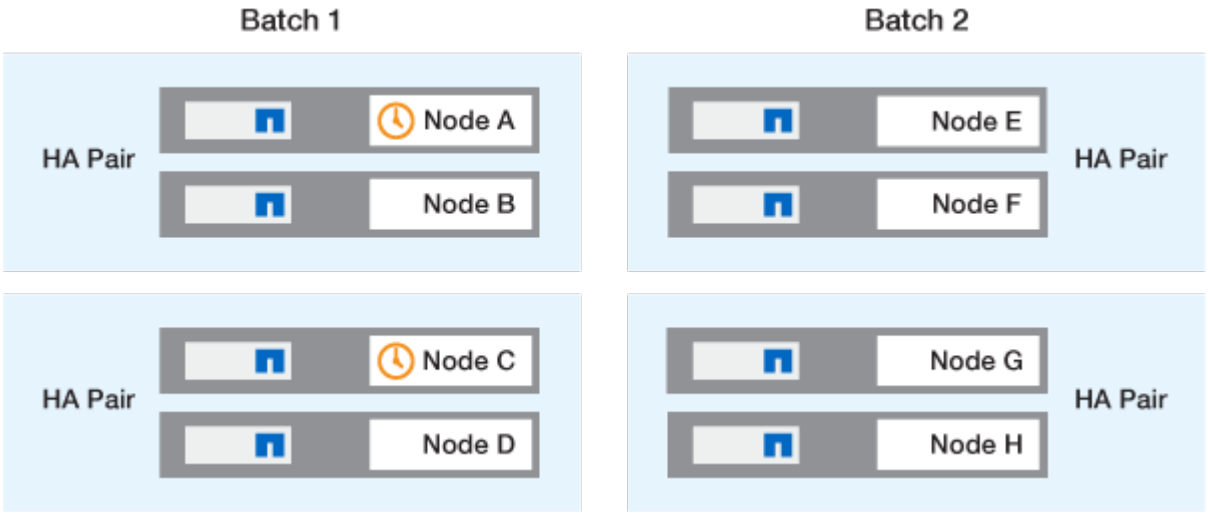
ONTAPのローリング アップグレード

8ノード未満のクラスタでは、ローリング アップグレード プロセスがデフォルトです。ローリング アップグレード プロセスでは、ノードを1つずつオフラインにしてノードのストレージをパートナーにフェイルオーバーし、その間にアップグレードを実行します。一方のノードのアップグレードが完了したら、パートナー ノードから元の所有者ノードに制御を戻し、パートナー ノードで同じ処理を行います。HAペアのそれぞれについて、すべてのHAペアがターゲット リリースに切り替わるまで順番にアップグレードを行います。

ONTAPのバッチ アップグレード

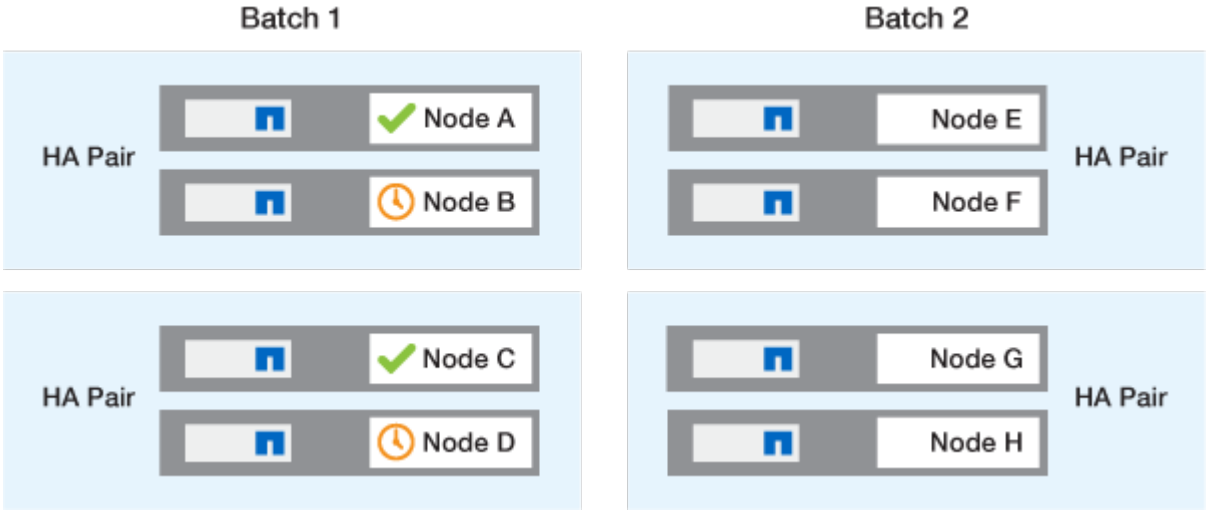
8ノード以上のクラスタでは、バッチ アップグレード プロセスがデフォルトです。バッチ アップグレード プロセスでは、クラスタを2つのバッチに分割します。各バッチには複数のHAペアが含まれます。最初のバッチでは、各HAペアの最初のノードを、そのバッチに含まれる他のすべてのHAペアの最初のノードと同時にアップグレードします。

次の例では、各バッチにHAペアが2つあります。バッチ アップグレードを開始すると、ノードAとノードCが同時にアップグレードされます。



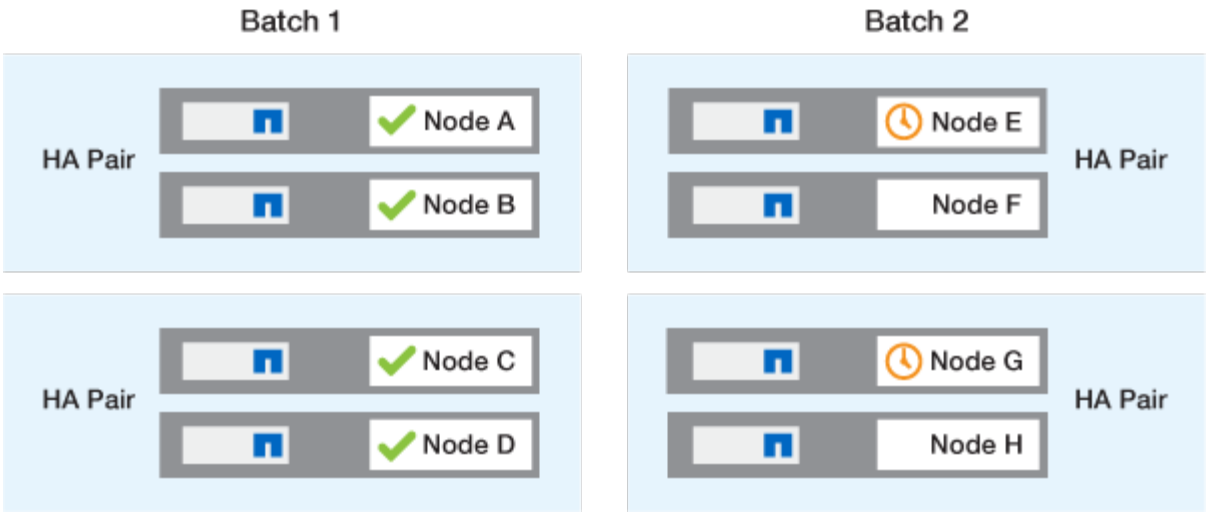
各HAペアの最初のノードのアップグレードが完了したら、バッチ1のパートナーノードが同時にアップグレードされます。

次の例では、ノードAとノードCをアップグレードしたあとに、ノードBとノードDを同時にアップグレードします。



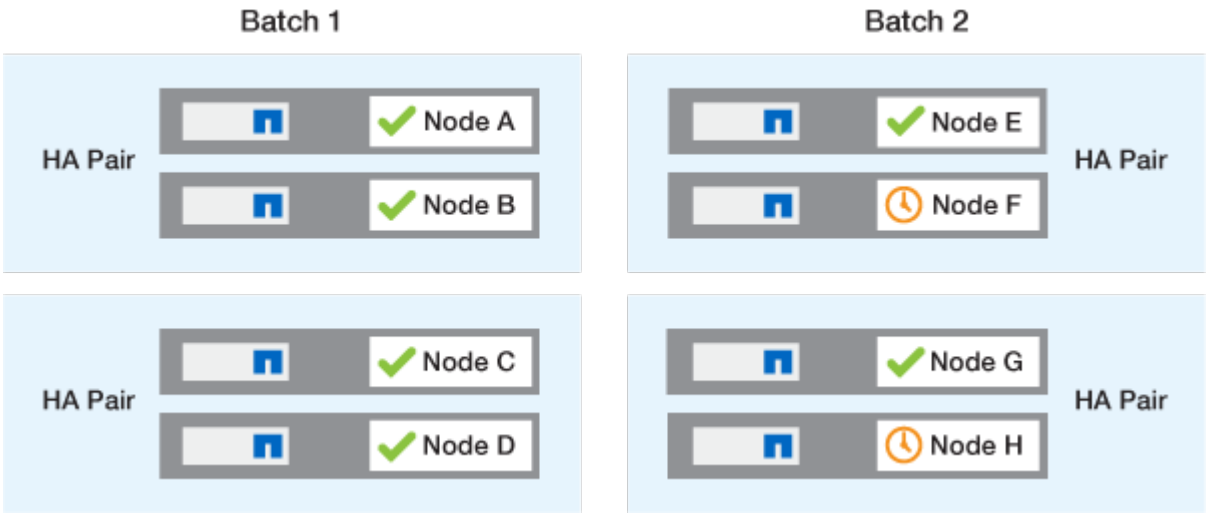
次に、バッチ2に含まれるノードに対して同じ処理を繰り返します。各HAペアの最初のノードは、バッチに含まれる他のすべてのHAペアの最初のノードと同時にアップグレードされます。

次の例では、ノードEとノードGが同時にアップグレードされます。



各HAペアの最初のノードのアップグレードが完了したら、バッチ2のパートナーノードが同時にアップグレードされます。

次の例では、ノードFとノードHを同時にアップグレードしてバッチアップグレードプロセスを完了します。



設定に基づく推奨される**ONTAP**アップグレード方式

お使いの構成でサポートされているアップグレード方法は、推奨される使用方法の順に記載されています。

構成	**ONTAP**のバージョン	ノード数	推奨されるアップグレード方式
標準	9.0以降	2つ以上	• System Managerヲシヨウシタムテイシ • CLIを使用した自動無停止アップグレード
標準	9.0以降	シングル	"自動停止機能"

構成	**ONTAP**のバージョン	ノード数	推奨されるアップグレード方式
MetroCluster	9.3以降	8	• CLIを使用した自動無停止アップグレード • CLIを使用した4ノードまたは8ノードMetroClusterの手動による無停止化
MetroCluster	9.3以降	2、4	• System Managerヲシヨウシタムテイシ • CLIを使用した自動無停止アップグレード
MetroCluster	9.2以前	4つまたは8つ	CLIを使用した4ノードまたは8ノードMetroClusterの手動による無停止化
MetroCluster	9.2以前	2	CLIを使用した2ノードMetroClusterの手動無停止アップグレード

設定に関係なく、すべてのパッチアップグレードではSystem Managerを使用したANDUのアップグレードが推奨されます。

は手動による停止を伴うアップグレード、任意の構成に対して実行できます。ただし、停止を伴うアップグレードを実行するには、アップグレード中にクラスタをオフラインにする必要があります。SAN環境を使用している場合は、停止を伴うアップグレードを実行する前に、すべてのSANクライアントをシャットダウンまたは一時停止できるよう準備してください。停止を伴うアップグレードはONTAP CLIを使用して実行します。

自動無停止**ONTAP**アップグレードによる**ONTAP**イメージのインストール

自動アップグレードを実行すると、ONTAPによってターゲットONTAPイメージが各ノードに自動的にインストールされ、クラスタが正常にアップグレード可能かどうかが検証されてから、クラスタ内のノードの数に基づいてがバックグラウンドで実行されバッチアップグレードまたはローリングアップグレードます。

お使いの構成でサポートされている場合は、System Managerを使用して自動アップグレードを実行する必要があります。ご使用の構成でSystem Managerによる自動アップグレードがサポートされない場合は、ONTAPコマンドラインインターフェイス（CLI）を使用して自動アップグレードを実行できます。

NetApp経由でONTAP 9.15.1以降にアップグレードする場合は、"NetAppコンソールのドキュメントのアップグレード手順" 。

自動無停止アップグレード（ANDU）の開始前にコマンドオプションの設定を変更し `storage failover modify-auto-giveback`ても、アップグレードプロセスには影響しません。ANDUプロセスでは、更新に必要なテイクオーバー/ギブバックの実行時に、このオプションにあらかじめ設定されている値は無視されます。たとえば、ANDUを開始する前にfalseに設定して `-autogiveback`も、ギブバックの前に自動アップグレードは中断されません。の詳細については `storage failover modify-auto-giveback`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

- そうするべきだ"アップグレードを準備"
- ターゲットのONTAPリリースに対応している必要があります"ONTAPソフトウェアイメージのダウンロード"。

  を実行する場合"直接マルチホップアップグレード"は、特定のに必要な両方のONTAPイメージをダウンロードする必要があり"アップグレードパス"ます。

- HAペアごとに、各ノードの同じブロードキャストドメインに1つ以上のポートが必要です。

  ONTAPクラスタのノード数が8つ以上の場合は、自動無停止アップグレードでバッチアップグレード方式が使用され、SFOのテイクオーバー前にデータLIFの移行を優先的に実行します。バッチアップグレード時にLIFを移行する方法は、ONTAPのバージョンによって異なります。

実行しているONTAP	LIFを移行する
• 9.15.1以降 • 9.14.1P5 • 9.13.1P10 • 9.12.1P13 • 9.11.1P16、P17 • 9.10.1P19	他のバッチ グループ内のノード。他のバッチ グループへの移行に失敗した場合、LIFは同じバッチ グループ内のノードのHAパートナーに移行されます。
9.8～9.14.1	他のバッチ グループ内のノード。ネットワーク ブロードキャスト ドメインで他のバッチ グループへのLIFの移行が許可されていない場合は、LIFの移行に失敗し、ANDUが一時停止します。
9.7以前	アップグレードするノードのHAパートナーに接続します。パートナーの同じブロードキャストドメインにポートがない場合、LIFの移行は失敗し、ANDUが一時停止します。

- MetroCluster FC構成でONTAPをアップグレードする場合は、クラスタで自動計画外スイッチオーバーを有効にする必要があります。
- アップグレードプロセスの進行状況を監視する予定がない場合は、を実行してください"手動操作が必要なエラーに関する EMS 通知を要求します"。
- シングルノードクラスタの場合は、このプロセスに従って"自動停止を伴うアップグレード"ください。

  シングルノードクラスタのアップグレードはシステムの停止を伴います。

例 **3.** 手順

System Manager

1. ONTAPターゲットイメージを検証します。

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

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

実行中のバージョン	操作
ONTAP 9 .8以降	[クラスタ]>[概要]*をクリックします。
ONTAP 9.5 、 9.6 、および 9.7	[* Configuration * （設定 * ）] > [* Cluster * （クラスタ * ）] > [* Update * （アップデート *
ONTAP 9 .4以前	[* Configuration * （構成 * ）] > [* Cluster Update （クラスタの更新）] を

   b. [Overview]*ペインの右隅で、をクリックします。

   c. ONTAPアップデート*をクリックします。

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

状況	そしたら…。
ローカルフォルダからの新しいソフトウェアイメージの追加 すでにローカルクライアントに接続されている必要があります"イメージをダウンロードしました"。	i. で、[ローカルから追加]*をクリックします。 ii. ソフトウェアイメージを保存した場所を参照し、イメージを選択して、 * 開く * をクリックします。
HTTPサーバまたはFTPサーバから新しいソフトウェアイメージを追加する	i. [サーバーから追加] をクリックします。 ii. [新しいソフトウェアイメージの追加]ダイアログボックスで、NetApp Support SiteからONTAPソフトウェアイメージをダウンロードしたHTTPサーバまたはFTPサーバのURLを入力します。 匿名FTPのURLは、の形式で指定する必要があります ftp://anonymous@ftpserver。 iii. [追加]*をクリックします。
使用可能なイメージを選択	リストされている画像のいずれかを選択します。

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

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

2. 「 * 次へ * 」をクリックします。
3. [更新（ Update ）] をクリックします。

検証が再度実行されます。残りのエラーまたは警告は、対処方法のリストとともに表示されます。アップグレードを続行する前に、エラーを修正する必要があります。検証が完了して警告が生成された場合は、警告を修正するか、*[警告で更新]*を選択します。

ONTAPでは、デフォルトでを使用して、"バッチアップグレードプロセス"8ノード以上のクラスタをアップグレードします。ONTAP 9.10.1以降では、必要に応じて[一度に1つのHAペアを更新]*を選択してデフォルトの設定を上書きし、クラスタのHAペアをローリングアップグレードプロセスを使用して一度に1つずつアップグレードすることができます。

ノードが3つ以上のMetroCluster構成の場合は、両方のサイトのHAペアでONTAPのアップグレードプロセスが同時に開始されます。2ノードMetroCluster構成の場合は、アップグレードが開始されないサイトで最初にアップグレードが開始されます。最初のアップグレードが完了すると、残りのサイトでアップグレードが開始されます。

4. エラーが原因でアップグレードが一時停止した場合は、エラーメッセージをクリックして詳細を表示し、エラーを修正します"アップグレードを再開する"。

終了後

アップグレードが完了すると、ノードがリブートし、System Managerのログインページが表示されます。ノードのリブートに時間がかかる場合は、ブラウザをリフレッシュしてください。

CLI

1. ONTAPターゲットソフトウェアイメージの検証

MetroCluster構成をアップグレードする場合は、まずクラスタAで次の手順を実行してから、クラスタBで同じ手順を実行する必要があります。

a. 以前のONTAPソフトウェアパッケージを削除します。

```
cluster image package delete -version <previous_ONTAP_Version>
```

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

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

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

Package download completed.
Package processing completed.
```

を実行する場合"直接マルチホップアップグレード"は、アップグレードに必要な中間バージョンのONTAPのソフトウェアパッケージもロードする必要があります。たとえば、9.8から9.13.1にアップグレードする場合は、ONTAP 9 .12.1のソフトウェアパッケージをロードしてから、同じコマンドを使用して9.13.1のソフトウェアパッケージをロードする必要があります。

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

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

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

d. アップグレード前の自動チェックを実行します。

```
cluster image validate -version <package_version_number>
```

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

```
cluster1::> cluster image validate -version 9.13.1

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

a. 検証の進捗を監視します。

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

b. 検証で特定された必要なアクションをすべて完了します。

c. MetroCluster構成をアップグレードする場合は、クラスタBで上記の手順を繰り返します。

2. ソフトウェア アップグレードの見積もりを生成します。

```
cluster image update -version <package_version_number> -estimate
-only
```

MetroCluster構成をアップグレードする場合は、このコマンドをクラスタAとクラスタBのどちらでも実行できます。両方のクラスタで実行する必要はありません。

ソフトウェアアップグレードの見積もりには、更新対象の各コンポーネントの詳細とアップグレードの推定期間が表示されます。

3. ソフトウェアのアップグレードを実行します。

```
cluster image update -version <package_version_number>
```

- を実行する"直接マルチホップアップグレード"場合は、package_version_numberにターゲットONTAPバージョンを使用します。たとえば、ONTAP 9 .8から9.13.1にアップグレードする場合は、package_version_numberとして9.13.1を使用します。
- ONTAPでは、デフォルトでを使用して、"バッチアップグレードプロセス"8ノード以上のクラスタをアップグレードします。必要に応じて、パラメータを使用してデフォルトのプロセスを上書きし、ローリングアップグレードプロセスを使用して一度に1ノードずつクラスタをアップグレードできます `-force-rolling`。
- テイクオーバーとギブバックが完了するたびに、テイクオーバーとギブバックの際に発生するI/Oの中断からクライアントアプリケーションが回復できるように8分間待機します。クライアントが安定するために必要な時間を増減する場合は、パラメータを使用して待機時間を変更できます `-stabilize-minutes`。
- 4ノード以上のMetroCluster構成の場合は、両方のサイトのHAペアで同時に自動アップグレードが開始されます。2ノードMetroCluster構成の場合は、アップグレードが開始されないサイトでアップグレードが開始されます。最初のアップグレードが完了すると、残りのサイトでアップグレードが開始されます。

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
--------------------- ----------
-----------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. クラスタの更新の進捗を表示します。

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

4ノードまたは8ノードのMetroCluster構成をアップグレードする場合、`cluster image show-update-progress`コマンドを実行するノードの進捗状況のみが表示されます。個 々 のノードの進捗状況を確認するには、各ノードでコマンドを実行する必要があります。

5. 各ノードでアップグレードが正常に完了したことを確認します。

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

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

                                                 Estimated
Elapsed
Update Phase          Status                      Duration
Duration
--------------------- ----------------- ---------------
---------------
Pre-update checks     completed                   00:10:00
00:02:07
Data ONTAP updates    completed                   01:31:00
01:39:00
Post-update checks    completed                   00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. AutoSupport通知を送信します。

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

AutoSupportメッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

7. 2ノードのMetroCluster FC構成をアップグレードする場合は、クラスタで自動計画外スイッチオーバーが有効になっていることを確認します。

標準構成、MetroCluster IP構成、またはノードが2つ以上のMetroCluster FC構成の場合は、この手順を実行する必要はありません。

a. 自動計画外スイッチオーバーが有効かどうかを確認します。

```
metrocluster show
```

自動計画外スイッチオーバーが有効な場合、コマンド出力に次のステートメントが表示されます。

```
AUSO Failure Domain    auso-on-cluster-disaster
```

a. このステートメントが表示されない場合は、自動計画外スイッチオーバーを有効にします。

```
metrocluster modify -auto-switchover-failure-domain auso-on-
cluster-disaster
```

b. 自動計画外スイッチオーバーが有効になっていることを確認します。

```
metrocluster show
```

自動アップグレード プロセスでのエラー後の**ONTAP**ソフトウェア アップグレード再開

エラーが原因でONTAPソフトウェアの自動アップグレードが一時停止した場合は、エラーを解決してからアップグレードを続行する必要があります。エラーを解決したら、自動アップグレード プロセスを続行するか、手動でアップグレード プロセスを完了するかを選択できます。自動アップグレードを続行する場合は、アップグレード手順を手動では一切実行しないでください。

例 **4.** 手順

System Manager

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

実行中のバージョン	そしたら…。
ONTAP 9 .8以降	**>**[概要]*をクリックします。
ONTAP 9.7、9.6、または9.5	[* Configuration * （設定 * ）] > [* Cluster * （クラスタ * ）] > [* Update * （アップデート *
ONTAP 9 .4以前	• [* Configuration * （構成 * ）] > [* Cluster Update （クラスタの更新）] を • ペインの右隅にある青い縦の**3**つのドットをクリックし、 ONTAP Update*を選択します。

2. 自動アップグレードを続行するか、キャンセルして手動で続行します。

状況	そしたら…。
自動アップグレードを再開する	[* 再開 *] をクリックします。
自動アップグレードをキャンセルして手動で続行する	[キャンセル（ Cancel ）] をクリックします。

CLI

1. アップグレードエラーを表示します。

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

2. エラーを解決します。
3. アップグレードを再開します。

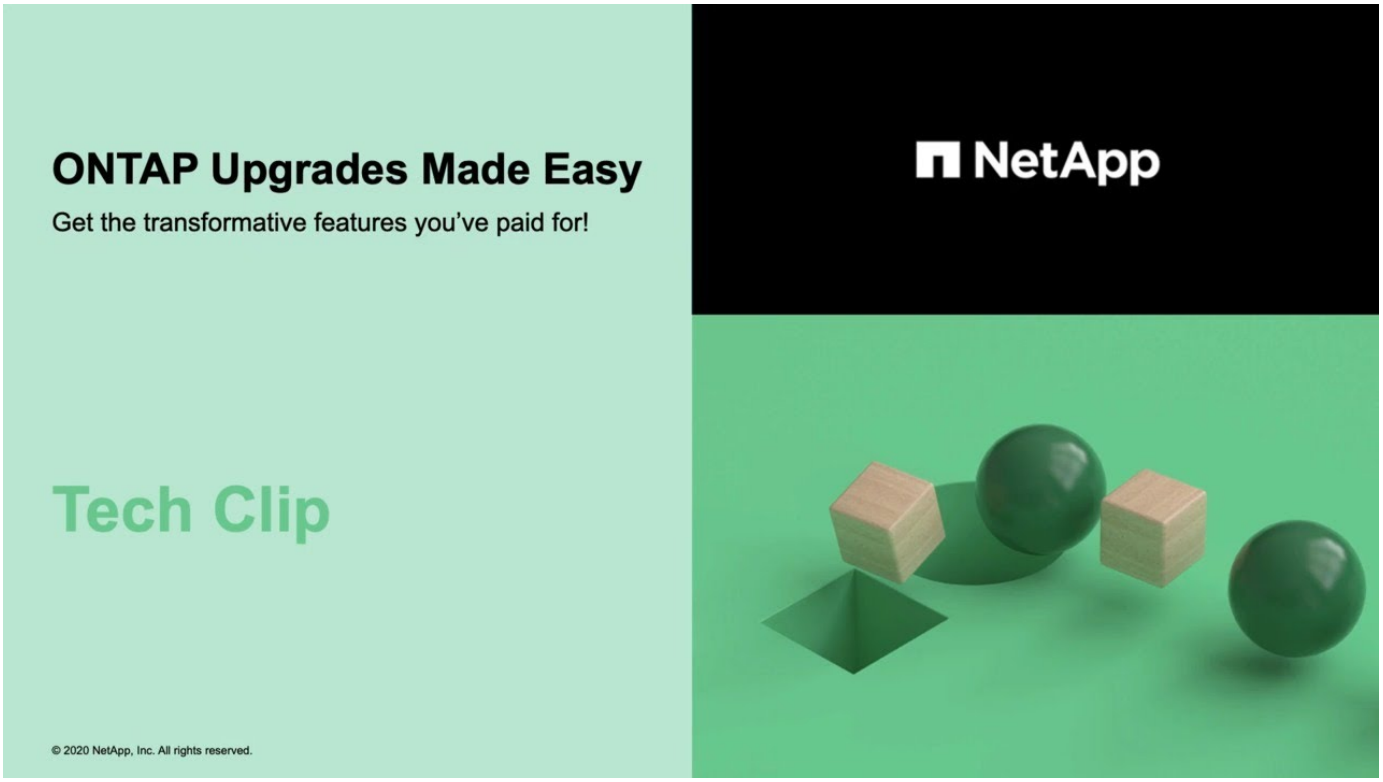
状況	入力するコマンド
自動アップグレードを再開する	`cluster image resume-update`
自動アップグレードをキャンセルして手動で続行する	`cluster image cancel-update`

終了後

"アップグレード後チェックの実行"です。

ビデオ：簡単にアップグレード

ONTAP 9のONTAPアップグレード機能が簡易化されたことを確認してください。8.



関連情報

- "Active IQデジタルアドバイザの起動"
- "Active IQデジタルアドバイザのドキュメント"
- "クラスタイメージ"
- "AutoSupport呼び出し"
- "MetroCluster"

シュドウアップグレード

手動アップグレードのための**ONTAP**ソフトウェアパッケージのインストール

手動アップグレード用のONTAPソフトウェアパッケージをダウンロードしたら、アップグレードを開始する前にローカルにインストールする必要があります。

手順

1. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。 `set -privilege advanced`

   advancedプロンプト(`*>`が表示されます）。

2. イメージをインストールします。

構成	使用するコマンド
• MetroCluster以外 • 2ノード MetroCluster	`system node image update -node * -package <location> -replace -package true -setdefault true -background true` <location> ONTAPのバージョンに応じて、Webサーバまたはローカルフォルダを指定できます。の詳細については system node image update、を"ONTAPコマンド リファレンス"参照してください。 このコマンドを実行すると、ソフトウェアイメージがすべてのノードに同時にインストールされます。一度に1つずつ各ノードにイメージをインストールする場合は、パラメータを指定しない `-background`でください。
• 4ノードMetroCluster • 8ノードMetroCluster構成	`system node image update -node * -package <location> -replace -package true -background true -setdefault false` このコマンドは両方のクラスタで発行する必要があります。 このコマンドは、拡張クエリを使用して、代替イメージとして各ノードにインストールされるターゲットのソフトウェアイメージを変更します。

3. プロンプトが表示されたらと入力し `y`て続行します
4. 各ノードにソフトウェアイメージがインストールされていることを確認します。

```
system node image show-update-progress -node *
```

このコマンドは、ソフトウェアイメージのインストールの現在のステータスを表示します。すべてのノードの Run Status * が Exited * になり、 * Exit Status * が * Success * になるまで、このコマンドを繰り返し実行します。

system node image updateコマンドが失敗し、エラーまたは警告メッセージが表示されることがあります。エラーや警告を解決したら、コマンドを再度実行できます。

次の例では、2ノードクラスタの両方のノードにソフトウェアイメージが正常にインストールされています。

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

CLIを使用した手動による無停止**ONTAP**アップグレード（標準構成）

System Managerを使用した自動アップグレードが推奨されるアップグレード方法です。System Mangerでサポートされない構成の場合は、ONTAPコマンドライン インターフェイス（CLI）を使用して手動無停止アップグレードを実行できます。手動の無停止方式を使用して 2 つ以上のノードのクラスタをアップグレードするには、 HA ペアの各ノードでフェイルオーバー処理を開始し、「 failed 」ノードを更新してギブバックを開始してから、クラスタ内の各 HA ペアについてこの処理を繰り返す必要があります。

開始する前に

アップグレード要件を満たしておく必要があり"準備"ます。

HAペアの最初のノードの更新

ノードのパートナーによるテイクオーバーを開始することで、HAペアの最初のノードを更新できます。最初のノードをアップグレードしている間、ノードのデータはパートナーから提供されます。

メジャー アップグレードを実行する場合は、外部接続用にデータLIFを設定し、最初のONTAPイメージをインストールしたノードをアップグレード対象の最初のノードにする必要があります。

最初のノードをアップグレードしたら、できるだけ早くパートナーノードをアップグレードする必要があります。2つのノードを必要以上に長い間状態のままにしないで"バージョンノコンザイ"ください。

手順

1. AutoSupportメッセージを呼び出して、クラスタ内の最初のノードを更新します。

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

このAutoSupport通知には、更新直前のシステムステータスの記録が含まれます。これにより、更新処理で問題が発生した場合に役立つトラブルシューティング情報が保存されます。

AutoSupportメッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

2. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

3. 新しいONTAPソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

system image modifyコマンドでは、拡張クエリを使用して、（代替イメージとしてインストールされる）新しいONTAPソフトウェアイメージをノードのデフォルトイメージに変更します。

4. 更新の進捗状況を監視します。

```
system node upgrade-revert show
```

5. 新しいONTAPソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、image2が新しいONTAPバージョンで、node0でデフォルトのイメージとして設定されています。

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------- ------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

6. 自動ギブバックが有効になっている場合は、パートナーノードで無効にします。

```
storage failover modify -node nodenameB -auto-giveback false
```

2ノードクラスタの場合は、自動ギブバックを無効にすると、交互に障害が発生した場合に管理クラスタのサービスがオンラインにならないことを示す警告メッセージが表示されます。と入力し `y`て続行します。

7. ノードのパートナーの自動ギブバックが無効になっていることを確認します。

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. 次のコマンドを2回実行して、更新対象のノードが現在クライアントに対して処理を行っているかどうかを確認します。

```
system node run -node nodenameA -command uptime
```

uptimeコマンドでは、ノードの前回のブート以降にNFS、SMB、FC、iSCSIの各クライアントに対してノードが実行した処理の総数が表示されます。プロトコルごとにコマンドを2回実行して、処理数が増加しているかどうかを確認する必要があります。増加している場合は、そのプロトコルのクライアントに対してノードが現在処理を行っています。増加していない場合は、そのプロトコルのクライアントに対してノードは現在処理を行っていません。

ノードの更新後にクライアント トラフィックが再開したことを確認できるように、クライアントの処理数が増加しているプロトコルをすべて書き留めてください。

次の例は、NFS、SMB、FC、およびiSCSIの処理が検出されたノードを示しています。ただし、ノードは現在NFSクライアントとiSCSIクライアントに対してのみ処理を行っています。

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. ノードからすべてのデータLIFを移行します。

```
network interface migrate-all -node nodenameA
```

10. 移行したLIFを確認します。

```
network interface show
```

でLIFのステータスの確認に使用できる、およびパラメータの詳細については"ONTAPコマンド リファレンス"、を参照してください `network interface show`。

次の例は、node0のデータLIFが正常に移行されたことを示しています。それぞれのLIFについて、この例に含まれるフィールドを使用して、LIFのホーム ノードとポート、LIFの移行先である現在のノードとポート、およびLIFの動作ステータスと管理ステータスを確認できます。

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. テイクオーバーを開始します。

```
storage failover takeover -ofnode nodenameA
```

テイクオーバーするノードを新しいソフトウェア イメージでブートするには通常のテイクオーバーが必要なため、-option immediateパラメータは指定しないでください。ノードからLIFを手動で移行しなかった場合は、LIFがノードのHAパートナーに自動的に移行されるので、サービスが停止することはありません。

最初のノードがブートし、Waiting for giveback状態になります。

AutoSupportが有効な場合は、ノードがクラスタ クォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、更新を続行してかまいません。

12. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

バージョンの不一致およびメールボックス形式の問題を示すエラーメッセージが表示される場合があります。これは想定される動作であり、無停止メジャーアップグレードにおける一時的な状態を表しており、悪影響はありません。

次の例は、テイクオーバーが正常に完了したことを示しています。ノードnode0の状態はWaiting for giveback、パートナーの状態はIn takeoverになっています。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. 次の状態になるまで最低8分待ちます。
    - クライアントのマルチパス（導入している場合）が安定している。
    - クライアントがテイクオーバー中に発生した I/O 処理の中断から回復している。

      リカバリ時間はクライアントによって異なり、クライアントアプリケーションの特性によっては8分以上かかることがあります。

14. アグリゲートを最初のノードに戻します。

```
storage failover giveback -ofnode nodenameA
```

ギブバックでは、最初にルート アグリゲートをパートナー ノードに戻し、そのノードのブートが完了すると、ルート以外のアグリゲートと自動的にリバートするように設定されたすべてのLIFを戻します。新しくブートしたノードで、戻されたアグリゲートから順番にクライアントへのデータ提供が開始されます。

15. すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Statusフィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、拒否したサブシステムも表示されます。

16. いずれかのアグリゲートが戻されていない場合は、次の手順を実行します。
    a. 拒否された回避策を確認して、「 ve to 」状態に対処するか、拒否を無視するかを決定します。
    b. 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。
    c. 再実行 `storage failover giveback`指示。

       「 "" ～ "" 」条件をオーバーライドする場合は、 -override-vetoes パラメータを true に設定します。

17. 次の状態になるまで最低8分待ちます。
    - クライアントのマルチパス（導入している場合）が安定している。
    - クライアントがギブバック中に発生したI/O処理の中断から回復している。

      リカバリ時間はクライアントによって異なり、クライアントアプリケーションの特性によっては8分以上かかることがあります。

18. ノードの更新が正常に完了したことを確認します。
    a. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

    b. ノードの更新ステータスが完了になっていることを確認します。

```
system node upgrade-revert show -node nodenameA
```

       ステータスがcompleteと表示されます。

ステータスがcompleteでない場合は、テクニカルサポートにお問い合わせください。

    a. admin権限レベルに戻ります。

```
set -privilege admin
```

19. ノードのポートが動作していることを確認します。

```
network port show -node nodenameA
```

このコマンドは、ONTAP 9の上位バージョンにアップグレードされたノードで実行する必要があります。

次の例は、ノードのすべてのポートが動作していることを示しています。

```
cluster1::> network port show -node node0
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node0
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

20. LIFをノードにリバートします。

```
network interface revert *
```

このコマンドを実行すると、移行したLIFが元のノードに戻されます。

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. ノードのデータLIFが正常にノードにリバートされ、動作していることを確認します。

```
network interface show
```

次の例は、ノードがホストするすべてのデータLIFが正常にノードにリバートされ、動作ステータスが「up」になっていることを示しています。

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0          e0a
true
            data002      up/up    192.0.2.121/24     node0          e0b
true
            data003      up/up    192.0.2.122/24     node0          e0b
true
            data004      up/up    192.0.2.123/24     node0          e0a
true
4 entries were displayed.
```

22. 前の手順でこのノードがクライアントに対して処理を行っていることを確認した場合は、その時点で処理を行っていたプロトコルごとに、ノードがサービスを提供していることを確認します。

```
system node run -node nodenameA -command uptime
```

更新中に、処理数はゼロにリセットされます。

次の例は、更新したノードがNFSクライアントとiSCSIクライアントに対する処理を再開していることを示しています。

```
cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. 前の手順でパートナー ノードの自動ギブバックを無効にした場合は、再度有効にします。

```
storage failover modify -node nodenameB -auto-giveback true
```

できるだけ早くノードのHAパートナーの更新に進んでください。何らかの理由で更新プロセスを中断する必要がある場合は、HAペアの両方のノードで同じバージョンのONTAPを実行する必要があります。

HAペアのパートナー ノードの更新

HAペアの最初のノードを更新したあとは、そのノードでテイクオーバーを開始してパートナーを更新します。パートナーをアップグレードしている間、パートナーのデータは最初のノードから提供されます。

1. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

2. 新しいONTAPソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

system image modifyコマンドでは、拡張クエリを使用して、（代替イメージとしてインストールされる）新しいONTAPソフトウェアイメージがノードのデフォルトイメージになるように変更します。

3. 更新の進捗状況を監視します。

```
system node upgrade-revert show
```

4. 新しいONTAPソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例で `image2`は、がONTAPの新しいバージョンであり、ノードでデフォルトのイメージとして設定されています。

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

5. 自動ギブバックが有効になっている場合は、パートナーノードで無効にします。

```
storage failover modify -node nodenameA -auto-giveback false
```

2ノードクラスタの場合は、自動ギブバックを無効にすると、交互に障害が発生した場合に管理クラスタ

のサービスがオンラインにならないことを示す警告メッセージが表示されます。と入力し `y`て続行します。

6. パートナーノードの自動ギブバックが無効になっていることを確認します。

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- -------------
node0    false
1 entry was displayed.
```

7. 次のコマンドを2回実行して、更新対象のノードが現在クライアントに対して処理を行っているかどうかを確認します。

```
system node run -node nodenameB -command uptime
```

uptimeコマンドでは、ノードの前回のブート以降にNFS、SMB、FC、iSCSIの各クライアントに対してノードが実行した処理の総数が表示されます。プロトコルごとにコマンドを2回実行して、処理数が増加しているかどうかを確認する必要があります。増加している場合は、そのプロトコルのクライアントに対してノードが現在処理を行っています。増加していない場合は、そのプロトコルのクライアントに対してノードは現在処理を行っていません。

ⓘ ノードの更新後にクライアント トラフィックが再開したことを確認できるように、クライアントの処理数が増加しているプロトコルをすべて書き留めてください。

次の例は、NFS、SMB、FC、およびiSCSIの処理が検出されたノードを示しています。ただし、ノードは現在NFSクライアントとiSCSIクライアントに対してのみ処理を行っています。

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. ノードからすべてのデータLIFを移行します。

```
network interface migrate-all -node nodenameB
```

9. 移行したLIFのステータスを確認します。

```
network interface show
```

でLIFのステータスの確認に使用できる、およびパラメータの詳細については"ONTAPコマンド リファレンス"、を参照してください `network interface show`。

次の例は、node1のデータLIFが正常に移行されたことを示しています。それぞれのLIFについて、この例に含まれるフィールドを使用して、LIFのホーム ノードとポート、LIFの移行先である現在のノードとポート、およびLIFの動作ステータスと管理ステータスを確認できます。

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up          up
vs0     data002 node1     e0b       node0     e0b       up          up
vs0     data003 node1     e0b       node0     e0b       up          up
vs0     data004 node1     e0a       node0     e0a       up          up
4 entries were displayed.
```

10. テイクオーバーを開始します。

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediateパラメータは指定しないでください。ノードからLIFを手動で移行しなかった場合は、LIFがノードのHAパートナーに自動的に移行されるため、サービスが停止することはありません。

警告が表示されます。続行するには、と入力する必要があります `y`。

テイクオーバーされたノードがブートし、Waiting for giveback状態になります。

> AutoSupportが有効な場合は、ノードがクラスタ クォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、更新を続行してかまいません。

11. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。ノードnode1の状態はWaiting for giveback、パートナーの状態はIn takeoverになっています。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. 次の条件が有効になるまで、8分以上待ちます。+
    - クライアントのマルチパス（導入している場合）が安定している。
    - クライアントがテイクオーバー中に発生したI/Oの中断から回復している。

      回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては8分以上かかることがあります。

13. アグリゲートをパートナーノードに戻します。

```
storage failover giveback -ofnode nodenameB
```

ギブバック処理では、最初にルートアグリゲートがパートナーノードに戻され、そのノードのブートが完了すると、ルート以外のアグリゲートと自動的にリバートするように設定されたLIFが戻されます。新しくブートしたノードで、戻されたアグリゲートから順番にクライアントへのデータ提供が開始されます。

14. すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Statusフィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、ギブバック処理を拒否したサブシステムも表示されます。

15. いずれかのアグリゲートが戻されていない場合は、次の手順を実行します。
    a. 拒否された回避策を確認して、「 ve to 」状態に対処するか、拒否を無視するかを決定します。
    b. 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。
    c. 再実行 `storage failover giveback`指示。

       「 "" ～ "" 」条件をオーバーライドする場合は、 -override-vetoes パラメータを true に設定します。

16. 次の状態になるまで最低8分待ちます。
    - クライアントのマルチパス（導入している場合）が安定している。
    - クライアントがギブバック中に発生したI/O処理の中断から回復している。

      リカバリ時間はクライアントによって異なり、クライアントアプリケーションの特性によっては8分以上かかることがあります。

17. ノードの更新が正常に完了したことを確認します。

    a. advanced権限レベルに切り替えます。

    ```
    set -privilege advanced
    ```

    b. ノードの更新ステータスが完了になっていることを確認します。

    ```
    system node upgrade-revert show -node nodenameB
    ```

    ステータスがcompleteと表示されます。

    ステータスがcompleteでない場合は、ノードからコマンドを実行し `system node upgrade-revert upgrade`ます。コマンドを実行しても更新が完了しない場合は、テクニカルサポートにお問い合わせください。

    a. admin権限レベルに戻ります。

    ```
    set -privilege admin
    ```

18. ノードのポートが動作していることを確認します。

    ```
    network port show -node nodenameB
    ```

    このコマンドはONTAP 9にアップグレードされたノードで実行する必要があります。4.

    次の例は、ノードのすべてのデータポートが動作していることを示しています。

```
cluster1::> network port show -node node1
                                                                        Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

19. LIFをノードにリバートします。

```
network interface revert *
```

このコマンドを実行すると、移行したLIFが元のノードに戻されます。

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. ノードのデータLIFが正常にノードにリバートされ、動作していることを確認します。

```
network interface show
```

次の例は、ノードでホストされるすべてのデータLIFが正常にノードにリバートされ、動作ステータスが「up」になっていることを示しています。

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1          e0a
true
            data002      up/up    192.0.2.121/24     node1          e0b
true
            data003      up/up    192.0.2.122/24     node1          e0b
true
            data004      up/up    192.0.2.123/24     node1          e0a
true
4 entries were displayed.
```

21. 前の手順でこのノードがクライアントに対して処理を行っていることを確認した場合は、その時点で処理を行っていたプロトコルごとに、ノードがサービスを提供していることを確認します。

```
system node run -node nodenameB -command uptime
```

更新中に、処理数はゼロにリセットされます。

次の例は、更新したノードがNFSクライアントとiSCSIクライアントに対する処理を再開していることを示しています。

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. これがクラスタ内で更新される最後のノードであった場合は、AutoSupport通知をトリガーします。

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

このAutoSupport通知には、更新直前のシステムステータスの記録が含まれます。これにより、更新処理で問題が発生した場合に役立つトラブルシューティング情報が保存されます。

AutoSupportメッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

23. HAペアの両方のノードで新しいONTAPソフトウェアが実行されていることを確認します。

```
set -privilege advanced
```

```
system node image show
```

次の例では、image2がONTAPの更新後のバージョンで、両方のノードのデフォルトのバージョンです。

```
cluster1::*> system node image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. 前の手順でパートナー ノードの自動ギブバックを無効にした場合は、再度有効にします。

```
storage failover modify -node nodenameA -auto-giveback true
```

25. コマンドと `cluster ring show`（advanced権限レベル）コマンドを使用して、クラスタがクォーラムにあること、およびサービスが実行されていることを確認します `cluster show`。

    この手順は、追加のHAペアをアップグレードする前に実行する必要があります。

    および `cluster ring show`の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。

26. admin権限レベルに戻ります。

```
set -privilege admin
```

27. 追加のHAペアがある場合はアップグレードします。

関連情報

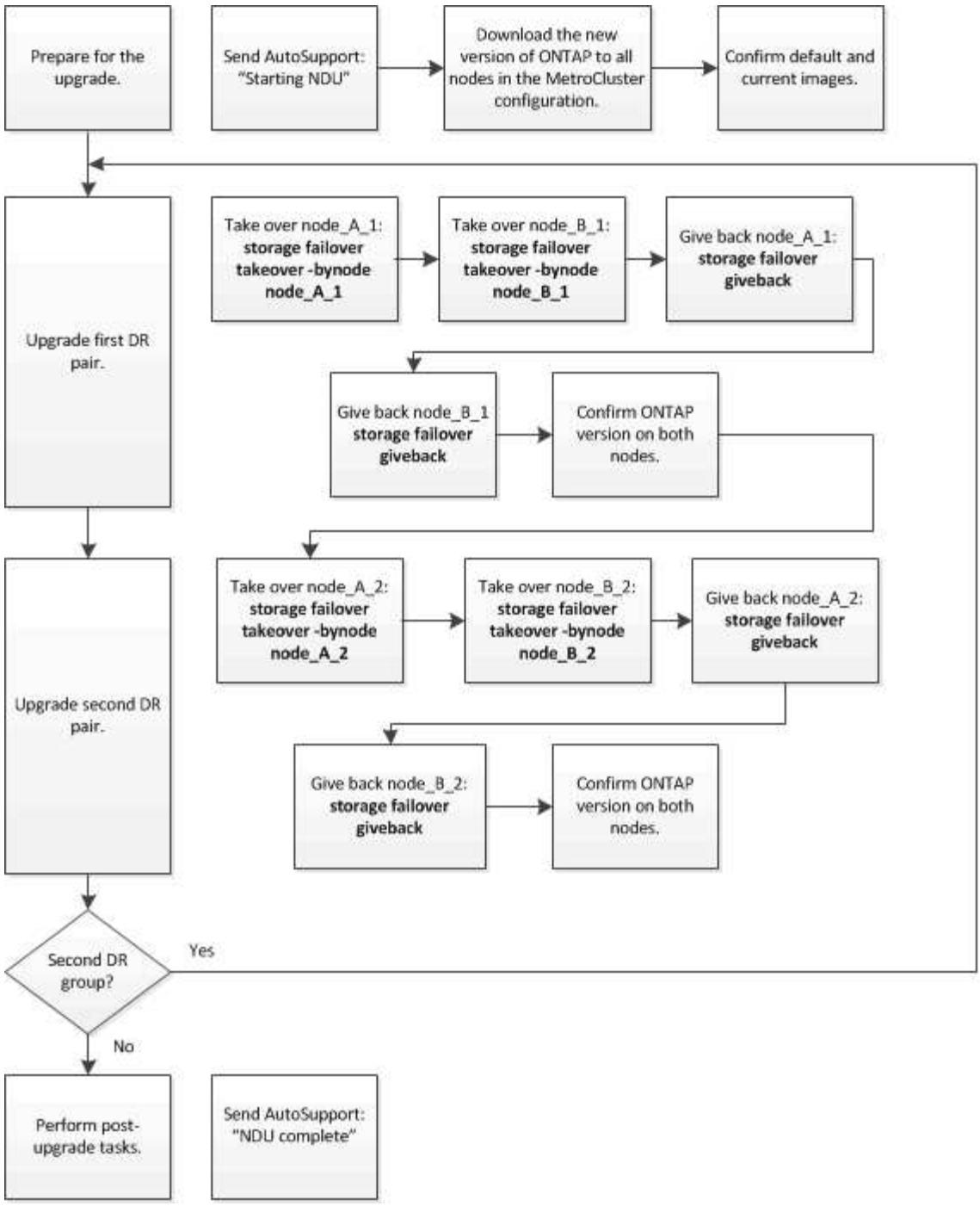
- "AutoSupport呼び出し"
- "システムイメージ"
- "システムノード"
- "ストレージフェイルオーバー"

- "ネットワークインターフェイス"
- "network port show"
- "set -privilege advanced"

CLIを使用した**4**ノードまたは**8**ノード**MetroCluster**構成の手動による無停止**ONTAP**アップグレード

4ノードまたは8ノードMetroCluster構成の手動アップグレードでは、更新の準備を行い、1つまたは2つのDRグループのそれぞれのDRペアを同時に更新し、アップグレード後の手順を実行します。

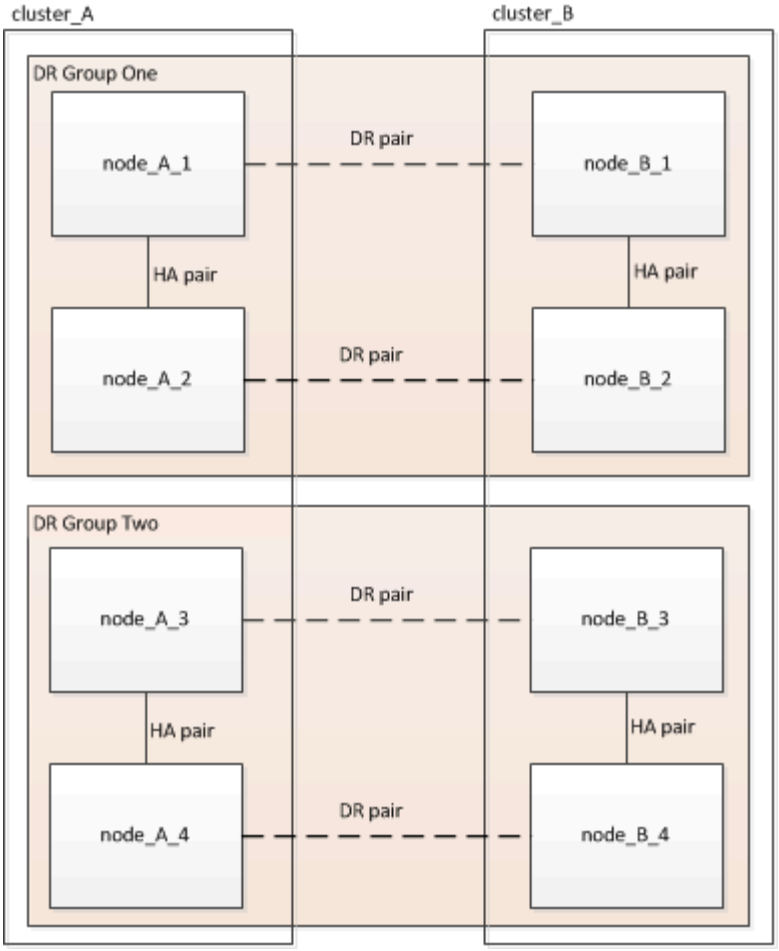
- この作業は、次の構成に適用されます。
  - ONTAP 9.2 以前を実行している 4 ノード MetroCluster FC 構成または IP 構成
  - ONTAP のバージョンに関係なく、 8 ノードの MetroCluster FC 構成
- 2ノードMetroCluster構成の場合は、この手順を使用しないでください。
- 次のタスクでは、ONTAPの古いバージョンと新しいバージョンを参照しています。
  - アップグレードの場合、古いバージョンは ONTAP の以前のバージョンで、 ONTAP の新しいバージョンよりも下位のバージョン番号が割り当てられます。
  - ダウングレード手順での古いバージョンとは、 ONTAP の新しいバージョン、つまり ONTAP の新しいバージョンのバージョン番号よりも上位の番号を持つバージョンを指します。
- このタスクのワークフローの概要は次のとおりです。



8ノードまたは**4**ノードの**MetroCluster**構成で**ONTAP**ソフトウェアを更新する場合の相違点

MetroClusterソフトウェアのアップグレードプロセスは、MetroCluster構成に8ノードと4ノードのどちらが含まれているかによって異なります。

MetroCluster構成は、1つまたは2つのDRグループで構成されます。各DRグループは、2つのHAペアで構成されます（各MetroClusterクラスタに1つのHAペア）。8ノードMetroClusterには、次の2つのDRグループが含まれます。



DRグループは一度に1つずつアップグレードします。

4ノード**MetroCluster**構成の場合：

1. DRグループ1をアップグレードします。
   a. node_A_1とnode_B_1をアップグレードします。
   b. node_A_2とnode_B_2をアップグレードします。

8ノード**MetroCluster**構成の場合は、**DR**グループのアップグレード手順を**2**回行います。

1. DRグループ1をアップグレードします。
   a. node_A_1とnode_B_1をアップグレードします。
   b. node_A_2とnode_B_2をアップグレードします。
2. DRグループ2をアップグレードします。
   a. node_A_3とnode_B_3をアップグレードします。
   b. node_A_4とnode_B_4をアップグレードします。

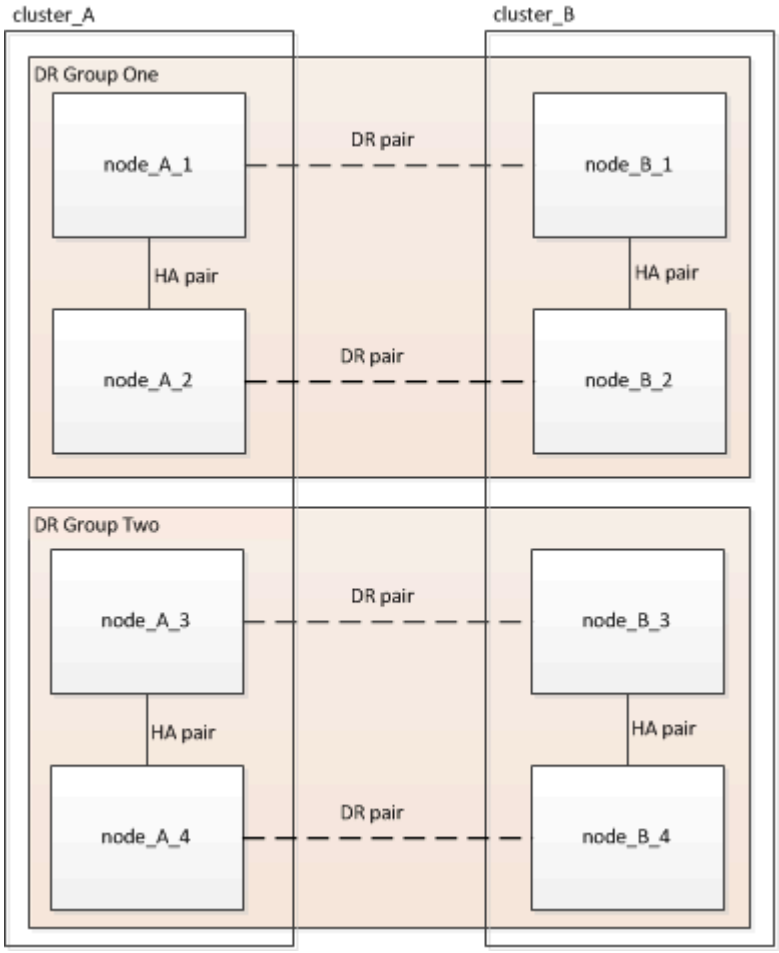
MetroCluster DRグループのアップグレード準備

ノード上のONTAPソフトウェアをアップグレードする前に、ノード間のDR関係を特定して、アップグレードを開始することを知らせるAutoSupportメッセージを送信します。また、各ノードで実行中のONTAPのバージョンを確認します。

ソフトウェアイメージと"インストール済み"ソフトウェアイメージが必要"ダウンロードしました"です。

このタスクは、DRグループごとに実行する必要があります。MetroCluster構成が8つのノードで構成されている場合は、DRグループが2つあります。そのため、このタスクをDRグループごとに繰り返す必要があります。

このタスクの例では、次の図に示す名前を使用してクラスタとノードを識別しています。



1. 構成内のDRペアを特定します。

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
4 entries were displayed.

cluster_A::>
```

2. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

3. cluster_AのONTAPバージョンを確認します。

```
system image show
```

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- -------   -------------------
node_A_1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. cluster_Bのバージョンを確認します。

```
system image show
```

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- -------     -------------------
node_B_1
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node_B_2
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. AutoSupport通知を送信します。

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

このAutoSupport通知には、アップグレード前のシステムステータスの記録が含まれます。アップグレードプロセスで問題が発生した場合に役立つトラブルシューティング情報が保存されます。

AutoSupportメッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

6. 最初のセットに含まれる各ノードについて、ターゲットのONTAPソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

このコマンドは、拡張クエリを使用して、代替イメージとしてインストールされるターゲットのソフトウェアイメージがノードのデフォルトのイメージになるように変更します。

7. ターゲットのONTAPソフトウェアイメージがcluster_Aでデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、image2が新しいONTAPバージョンで、最初のセットに含まれる各ノードでデフォルトのイメージとして設定されています。

```
cluster_A::*> system image show
                  Is      Is               Install
Node     Image    Default Current Version  Date
-------- -------  ------- ------- -------  ------------------
node_A_1
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true   false   Y.Y.Y    MM/DD/YYYY TIME

2 entries were displayed.
```

a. ターゲットのONTAPソフトウェアイメージがcluster_Bでデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、最初のセットに含まれる各ノードで、ターゲットのバージョンがデフォルトのイメージとして設定されています。

```
cluster_B::*> system image show
                  Is      Is               Install
Node     Image    Default Current Version  Date
-------- -------  ------- ------- -------  -------------------
node_A_1
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/YY/YYYY TIME
node_A_2
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/DD/YYYY TIME

2 entries were displayed.
```

8. 各ノードに対して次のコマンドを2回実行して、アップグレード対象のノードが現在クライアントに対して処理を行っているかどうかを確認します。

```
system node run -node target-node -command uptime
```

uptimeコマンドでは、ノードの前回のブート以降にNFS、CIFS、FC、iSCSIの各クライアントに対してノードが実行した処理の総数が表示されます。各プロトコルについてコマンドを2回実行して、処理数が増加しているかどうかを確認する必要があります。増加している場合は、そのプロトコルのクライアントに対してノードが現在処理を行っています。増加していない場合は、そのプロトコルのクライアントに対し

てノードは現在処理を行っていません。

ノードのアップグレード後にクライアント トラフィックが再開したことを確認できるように、クライアントの処理数が増加している各プロトコルを書き留めておいてください。

次の例は、NFS、CIFS、FC、およびiSCSIの処理が含まれるノードを示しています。ただし、ノードは現在NFSクライアントとiSCSIクライアントに対してのみ処理を行っています。

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

MetroCluster DRグループ内の最初の**DR**ペアの更新

ONTAPの新しいバージョンをノードの現在のバージョンにするには、ノードのテイクオーバーとギブバックを適切な順序で行う必要があります。

すべてのノードで古いバージョンのONTAPを実行する必要があります。

この手順では、node_A_1とnode_B_1をアップグレードします。

最初のDRグループのONTAPソフトウェアをアップグレード済みで、8ノードMetroCluster構成内の2つ目のDRグループをアップグレードする場合は、この手順でnode_A_3とnode_B_3を更新します。

1. MetroCluster Tiebreakerソフトウェアが有効になっている場合は、無効にします。
2. HAペアの各ノードで自動ギブバックを無効にします。

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   このコマンドはHAペアのノードごとに実行する必要があります。

3. 自動ギブバックが無効になっていることを確認します。

   ```
   storage failover show -fields auto-giveback
   ```

   次の例は、両方のノードで自動ギブバックが無効になっていることを示しています。

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 false
node_x_2 false
2 entries were displayed.
```

4. 各コントローラのI/Oが50%を超えていないこと、およびCPU利用率がコントローラあたり50%を超えていないことを確認してください。
5. cluster_Aのターゲットノードのテイクオーバーを開始します。

   テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediateパラメータは指定しないでください。

   a. cluster_A（node_A_1）のDRパートナーをテイクオーバーします。

      ```
      storage failover takeover -ofnode node_A_1
      ```

      ノードがブートし、「Waiting for giveback」状態になります。

      AutoSupportが有効な場合は、ノードがクラスタ クォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

   b. テイクオーバーが正常に完了したことを確認します。

      ```
      storage failover show
      ```

      次の例は、テイクオーバーが正常に完了したことを示しています。node_A_1の状態は「Waiting for giveback」、node_A_2の状態は「In takeover」になっています。

```
cluster1::> storage failover show
                                Takeover
Node           Partner          Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       -        Waiting for giveback (HA
mailboxes)
node_A_2       node_A_1       false    In takeover
2 entries were displayed.
```

6. cluster_B（node_B_1）のDRパートナーをテイクオーバーします。

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediateパラメータは指定しないでください。

a. node_B_1をテイクオーバーします。

```
storage failover takeover -ofnode node_B_1
```

ノードがブートし、「Waiting for giveback」状態になります。

AutoSupportが有効な場合は、ノードがクラスタ クォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。node_B_1の状態は「Waiting for giveback」、node_B_2の状態は「In takeover」になっています。

```
 cluster1::> storage failover show
                                Takeover
 Node           Partner        Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
 node_B_2       node_B_1       false    In takeover
 2 entries were displayed.
```

7. 8分以上待ってから、次の条件を満たしていることを確認します。
   - クライアントのマルチパス（導入している場合）が安定している。
   - クライアントがテイクオーバー中に発生したI/Oの中断から回復している。

   回復までの時間はクライアントによって異なり、クライアント アプリケーションの特性によっては8分以上かかることもあります。

8. アグリゲートをターゲット ノードに戻します。

MetroCluster IP構成をONTAP 9.5以降にアップグレードすると、アグリゲートの状態は短時間degradedになったあとに再同期されてmirroredに戻ります。

a. アグリゲートをcluster_AのDRパートナーにギブバックします。

```
storage failover giveback -ofnode node_A_1
```

b. アグリゲートをcluster_BのDRパートナーにギブバックします。

```
storage failover giveback -ofnode node_B_1
```

ギブバック処理では、最初にルート アグリゲートがノードに戻され、そのノードのブートが完了するとルート以外のアグリゲートが戻されます。

9. 両方のクラスタで次のコマンドを実行して、すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Statusフィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、拒否したサブシステムも表示されます。

10. 戻されていないアグリゲートがある場合は、次の操作を実行します。

a. 拒否された回避策を確認して、「 ve to 」状態に対処するか、拒否を無視するかを決定します。

b. 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。

c. storage failover givebackコマンドを再度入力します。

「 "" ～ "" 」条件をオーバーライドする場合は、 -override-vetoes パラメータを true に設定します。

11. 8分以上待ってから、次の条件を満たしていることを確認します。

◦ クライアントのマルチパス（導入している場合）が安定している。

◦ クライアントがギブバック中に発生したI/Oの中断から回復している。

回復までの時間はクライアントによって異なり、クライアント アプリケーションの特性によっては8分以上かかることもあります。

12. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

13. cluster_Aのバージョンを確認します。

```
system image show
```

次の例は、System image2がnode_A_1のデフォルトおよび現在のバージョンであることを示しています。

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node_A_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

14. cluster_Bのバージョンを確認します。

```
system image show
```

次の例は、System image2（ONTAP 9 .0.0）がnode_A_1のデフォルトおよび現在のバージョンであることを示しています。

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node_B_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_B_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

MetroCluster DRグループ内の2つ目のDRペアの更新

ONTAPの新しいバージョンをノードの現在のバージョンにするには、ノードのテイクオーバーとギブバックを正しい順序で実行する必要があります。

最初のDRペア（node_A_1とnode_B_1）をアップグレードしておく必要があります。

このタスクでは、node_A_2とnode_B_2をアップグレードします。

最初のDRグループのONTAPソフトウェアをアップグレードし、8ノードMetroCluster構成の2つ目のDRグループを更新する場合は、この手順でnode_A_4とnode_B_4を更新します。

1. ノードからすべてのデータLIFを移行します。

```
network interface migrate-all -node nodenameA
```

2. cluster_Aのターゲットノードのテイクオーバーを開始します。

   テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediateパラメータは指定しないでください。

   a. cluster_AのDRパートナーをテイクオーバーします。

```
storage failover takeover -ofnode node_A_2 -option allow-version-
mismatch
```

   この `allow-version-mismatch`オプションは、ONTAP 9 .0からONTAP 9 .1へのアップグレードやパッチのアップグレードには必要ありません。

   ノードがブートし、「Waiting for giveback」状態になります。

   AutoSupportが有効な場合は、ノードがクラスタ クォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

   b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

   次の例は、テイクオーバーが正常に完了したことを示しています。node_A_2の状態は「Waiting for giveback」、node_A_1の状態は「In takeover」になっています。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. cluster_Bのターゲット ノードのテイクオーバーを開始します。

   テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediateパラメータは指定しないでください。

   a. cluster_B（node_B_2）のDRパートナーをテイクオーバーします。

アップグレード前のバージョン	入力するコマンド
ONTAP 9.2またはONTAP 9.1	`storage failover takeover -ofnode node_B_2`
ONTAP 9.0またはData ONTAP 8.3.x	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` この `allow-version-mismatch`オプションは、ONTAP 9 .0からONTAP 9 .1へのアップグレードやパッチのアップグレードには必要ありません。

   ノードがブートし、「Waiting for giveback」状態になります。

   AutoSupportが有効な場合は、ノードがクラスタクォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

   b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

   次の例は、テイクオーバーが正常に完了したことを示しています。node_B_2の状態は「Waiting for giveback」、node_B_1の状態は「In takeover」になっています。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. 8分以上待ってから、次の条件を満たしていることを確認します。
   - クライアントのマルチパス（導入している場合）が安定している。
   - クライアントがテイクオーバー中に発生したI/Oの中断から回復している。

     回復までの時間はクライアントによって異なり、クライアント アプリケーションの特性によっては8分以上かかることもあります。

5. アグリゲートをターゲット ノードに戻します。

   MetroCluster IP構成をONTAP 9 5にアップグレードすると、アグリゲートは短時間degraded状態になり、その後再同期されてmirrored状態に戻ります。

   a. アグリゲートをcluster_AのDRパートナーにギブバックします。

      ```
      storage failover giveback -ofnode node_A_2
      ```

   b. アグリゲートをcluster_BのDRパートナーにギブバックします。

      ```
      storage failover giveback -ofnode node_B_2
      ```

      ギブバック処理では、最初にルート アグリゲートがノードに戻され、そのノードのブートが完了するとルート以外のアグリゲートが戻されます。

6. 両方のクラスタで次のコマンドを実行して、すべてのアグリゲートが戻されたことを確認します。

   ```
   storage failover show-giveback
   ```

   Giveback Statusフィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、拒否したサブシステムも表示されます。

7. 戻されていないアグリゲートがある場合は、次の操作を実行します。

   a. 拒否された回避策を確認して、「 ve to 」状態に対処するか、拒否を無視するかを決定します。

b. 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。

c. storage failover givebackコマンドを再度入力します。

「 "" ～ "" 」条件をオーバーライドする場合は、 -override-vetoes パラメータを true に設定します。

8. 8分以上待ってから、次の条件を満たしていることを確認します。
   - クライアントのマルチパス（導入している場合）が安定している。
   - クライアントがギブバック中に発生したI/Oの中断から回復している。

   回復までの時間はクライアントによって異なり、クライアント アプリケーションの特性によっては8分以上かかることもあります。

9. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

10. cluster_Aのバージョンを確認します。

```
system image show
```

次の例は、System image2（ターゲットのONTAPイメージ）がnode_A_2のデフォルトおよび現在のバージョンであることを示しています。

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------- -------------------
node_A_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_A_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. cluster_Bのバージョンを確認します。

```
system image show
```

次の例は、System image2（ターゲットのONTAPイメージ）がnode_B_2のデフォルトかつ現在のバージョンであることを示しています。

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------- -------------------
node_B_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_B_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

12. HAペアの各ノードで、自動ギブバックを有効にします。

```
storage failover modify -node target-node -auto-giveback true
```

このコマンドはHAペアのノードごとに実行する必要があります。

13. 自動ギブバックが有効になったことを確認します。

```
storage failover show -fields auto-giveback
```

次の例では、両方のノードで自動ギブバックが有効になっています。

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

関連情報

- "storage failover giveback"

- "storage failover modify"
- "storage failover show-giveback"
- "storage failover takeover"

ONTAP 9.2以前での2ノードMetroCluster構成の手動無停止アップグレード

2ノードMetroCluster構成のアップグレード方法は、ONTAPのバージョンによって異なります。ONTAP 9.2以前を実行している場合は、この手順を使用して手動による無停止アップグレードを実行します。具体的には、ネゴシエートスイッチオーバーを開始し、「障害」サイトでクラスタを更新してから、スイッチバックを開始します。この処理をもう一方のサイトのクラスタでも繰り返します。

2ノードMetroCluster構成でONTAP 9 .3以降を実行している場合は、を実行しますSystem Managerを使用した自動アップグレード。

手順

1. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

2. アップグレードするクラスタで、新しいONTAPソフトウェアイメージをデフォルトとしてインストールします。

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. ターゲットのソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system node image show
```

次の例は、がデフォルトのイメージとして設定されていることを示してい `NewImage`ます。

```
cluster_B::*> system node image show
                     Is      Is                            Install
Node     Image       Default Current Version               Date
-------- -------     ------- ------- --------------------
------------------
node_B_1
         OldImage  false   true    X.X.X                 MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                 MM/DD/YYYY TIME
2 entries were displayed.
```

4. ターゲットのソフトウェアイメージがデフォルトのイメージとして設定されていない場合は、変更します。

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vserver show
```

6. 更新対象でないクラスタで、ネゴシエート スイッチオーバーを開始します。

```
metrocluster switchover
```

この処理には数分かかることがあります。metrocluster operation showコマンドを使用して、スイッチオーバーが完了したかどうかを確認できます。

次の例では ' ネゴシエート・スイッチオーバーがリモート・クラスタ（ "cluster_a" ）上で実行されますこれにより ' ローカルクラスタ (“cluster_B”) が停止し ' 更新できるようになります

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vserver show
```

8. 「Surviving」クラスタ上のデータアグリゲートを再同期します。

```
metrocluster heal -phase aggregates
```

MetroCluster IP構成をONTAP 9.5以降にアップグレードすると、アグリゲートの状態は短時間degradedになったあとに再同期されてmirroredに戻ります。

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. 修復処理が正常に完了したことを確認します。

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. 「Surviving」クラスタのルートアグリゲートを再同期します。

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. 修復処理が正常に完了したことを確認します。

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. 停止したクラスタで、LOADERプロンプトからノードをブートします。

```
boot_ontap
```

13. ブート プロセスの終了を待ってから、すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vserver show
```

14. 「Surviving」クラスタからスイッチバックを実行します。

```
metrocluster switchback
```

15. スイッチバックが正常に完了したことを確認します。

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vserver show
```

17. もう一方のクラスタで、ここまでのすべての手順を繰り返します。
18. MetroCluster構成が正常であることを確認します。
    a. 構成を確認します。

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

b. 結果の詳細を表示するには、metrocluster check runコマンドを使用します。

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

d. スイッチオーバー処理をシミュレートします。

```
metrocluster switchover -simulate
```

e. スイッチオーバーのシミュレーション結果を確認します。

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. admin権限レベルに戻ります。

```
set -privilege admin
```

g. もう一方のクラスタで、上記の手順を繰り返します。

終了後

いずれかを実行します"アップグレードゴノテジュン"。

関連情報

"MetroClusterディザスタリカバリ"

CLIを使用した手動による停止を伴う**ONTAP**アップグレード

新しいONTAPリリースにアップグレードする際にクラスタをオフラインにしてもかまわない場合は、停止を伴うアップグレード方式を使用できます。この方式では、各HAペアのストレージフェイルオーバーを無効にし、クラスタ内の各ノードをリブートしてから、ストレージフェイルオーバーを再度有効にします。

- と"インストール"ソフトウェアイメージが必要です"ダウンロード"。
- SAN環境を使用している場合は、すべてのSANクライアントをシャットダウンするか、アップグレードが完了するまで一時停止する必要があります。

  停止を伴うアップグレードの前にSANクライアントをシャットダウンまたは一時停止しないと、クライアントファイルシステムおよびアプリケーションでエラーが発生し、アップグレードの完了後に手動によるリカバリが必要になる可能性があります。

停止を伴うアップグレードでは、各HAペアのストレージフェイルオーバーを無効にして各ノードを更新するため、ダウンタイムが必要です。ストレージフェイルオーバーを無効にすると、各ノードはシングルノードクラスタとして動作します。つまり、ノードに関連するシステムサービスは、システムをリブートするまで中断されます。

手順

1. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「* y *」と入力します。

```
set -privilege advanced
```

advancedプロンプト(`*>`が表示されます）。

2. 新しいONTAPソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node * -iscurrent false} -isdefault true
```

このコマンドでは、拡張クエリを使用して、（代替イメージとしてインストールされる）ターゲットのONTAPソフトウェアイメージが各ノードのデフォルトのイメージになるように変更します。

3. 新しいONTAPソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、image 2が新しいONTAPバージョンで、両方のノードでデフォルトのイメージとして設定されています。

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

4. 次のいずれかの手順を実行します。

クラスタの構成	操作
1ノード	次の手順に進みます。

クラスタの構成	操作

2ノード	a. クラスタ ハイアベイラビリティを無効にします。
	`cluster ha modify -configured false`
	プロンプトが表示されたらと入力し `y`て続行します
	b. HAペアのストレージフェイルオーバーを無効にします。
	`storage failover modify -node * -enabled false`

3ノード以上	クラスタ内の各HAペアのストレージフェイルオーバーを無効にします。 `storage failover modify -node * -enabled false`

5. クラスタ内のノードをリブートします。

```
system node reboot -node nodename -ignore-quorum-warnings
```

複数のノードを一度にリブートしないでください。

ノードが新しいONTAPイメージでブートします。ONTAPログイン プロンプトが表示され、リブート プロセスが完了したことが示されます。

6. ノードまたはノード セットが新しいONTAPイメージでリブートされたら、権限レベルをadvancedに設定します。

```
set -privilege advanced
```

続行するかどうかを尋ねられたら、「* y *」と入力します

7. 新しいソフトウェアが実行されていることを確認します。

```
system node image show
```

次の例では、image1が新しいONTAPバージョンで、node0で現在のバージョンとして設定されています。

```
cluster1::*> system node image show
                  Is      Is                    Install
Node     Image    Default Current Version       Date
-------- -------  ------- ------- --------      -------------------
node0
         image1   true    true    X.X.X          MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y         MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X         MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y         MM/DD/YYYY TIME
4 entries were displayed.
```

8. アップグレードが正常に完了したことを確認します。

   a. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

   b. 各ノードのアップグレードステータスが完了になっていることを確認します。

   ```
   system node upgrade-revert show -node nodename
   ```

   ステータスがcompleteと表示されます。

ステータスがcompleteでない場合は"ネットアップサポートにお問い合わせください"、すぐに実行します。

   a. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

9. 追加するノードごとに、手順5~8を繰り返します。
10. クラスタが複数のノードで構成されている場合は、クラスタ内の各HAペアのストレージフェイルオーバーを有効にします。

```
storage failover modify -node * -enabled true
```

11. クラスタが2つのノードだけで構成されている場合は、クラスタのハイアベイラビリティを有効にします。

```
cluster ha modify -configured true
```

関連情報

- "storage failover modify"

ONTAPアップグレード後の作業

ONTAPアップグレード後の作業

ONTAPをアップグレードしたら、クラスタの準備状況を確認するためにいくつかのタスクを実行する必要があります。

1. "クラスタの確認"です。

   ONTAPをアップグレードしたら、クラスタのバージョン、クラスタの健全性、およびストレージの健全性を確認する必要があります。MetroCluster FC構成を使用している場合は、クラスタで自動計画外スイッチオーバーが有効になっていることも確認する必要があります。

2. "すべてのLIFがホームポートにあることを確認する"です。

   リブート時に、割り当てられているフェイルオーバーポートに一部のLIFが移行されることがあります。クラスタのアップグレード後、ホームポートにないLIFを有効にしてリバートする必要があります。

3. クラスタに固有であることを確認します"特別な考慮事項"。

   クラスタに特定の構成が存在する場合は、アップグレード後に追加の手順を実行する必要があります。

4. "Disk Qualification Package（DQP）を更新する"です。

   ONTAPアップグレードの一環としてDQPが更新されることはありません。

ONTAPのアップグレード後のクラスタの確認

ONTAPをアップグレードしたら、クラスタのバージョン、クラスタの健全性、およびストレージの健全性を確認します。MetroCluster FC構成の場合は、クラスタで自動計画外スイッチオーバーが有効になっていることも確認します。

クラスタ バージョンの確認

すべてのHAペアをアップグレードしたら、versionコマンドを使用して、すべてのノードでターゲット リリースが実行されていることを確認する必要があります。

クラスタ バージョンは、クラスタ内のいずれかのノードで実行されているONTAPの最下位のバージョンです。クラスタ バージョンがターゲットのONTAPリリースになっていない場合は、クラスタをアップグレードできます。

1. クラスタ バージョンがターゲットのONTAPリリースになっていることを確認します。

```
version
```

2. クラスタ バージョンがターゲットのONTAPリリースになっていない場合は、すべてのノードのアップグレード ステータスを確認する必要があります。

```
system node upgrade-revert show
```

クラスタの健全性を確認

クラスタをアップグレードしたら、ノードが正常に機能していてクラスタに追加するための条件を満たしていること、およびクラスタがクォーラムにあることを確認する必要があります。

1. クラスタ内のノードがオンラインであり、クラスタに参加するための条件を満たしていることを確認します。

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

正常でないノードや条件を満たしていないノードがある場合は、EMSログでエラーを確認して対処します。

2. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

3. 各RDBプロセスの設定の詳細を確認します。

   - リレーショナルデータベースのエポックとデータベースのエポックは、各ノードで一致している必要があります。
   - リングごとのクォーラムマスターがすべてのノードで同じである必要があります。

     各リングのクォーラムマスターが異なる場合があることに注意してください。

表示する RDB プロセス	入力するコマンド

管理アプリケーション	`cluster ring show -unitname mgmt`
ボリューム ロケーション データベース	`cluster ring show -unitname vldb`
仮想インターフェイス マネージャ	`cluster ring show -unitname vifmgr`
SAN管理デーモン	`cluster ring show -unitname bcomd`

の詳細については `cluster ring show`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、ボリューム ロケーション データベースのプロセスを示しています。

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. SAN環境を使用している場合は、各ノードがSANクォーラムにあることを確認します。

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

関連情報

"システム管理"

自動計画外スイッチオーバーが有効になっていることを確認する（**MetroCluster FC**構成のみ）

クラスタがMetroCluster FC構成の場合は、ONTAPのアップグレード後に自動計画外スイッチオーバーが有効になっていることを確認する必要があります。

MetroCluster IP構成を使用している場合は、この手順を省略してください。

手順

1. 自動計画外スイッチオーバーが有効かどうかを確認します。

   ```
   metrocluster show
   ```

   自動計画外スイッチオーバーが有効な場合、コマンド出力に次のステートメントが表示されます。

   ```
   AUSO Failure Domain  auso-on-cluster-disaster
   ```

2. 次のステートメントが表示されない場合は、自動計画外スイッチオーバーを有効にします。

   ```
   metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
   disaster
   ```

3. 自動計画外スイッチオーバーが有効になっていることを確認します。

   ```
   metrocluster show
   ```

関連情報

"ディスクおよびアグリゲートの管理"

ONTAPのアップグレード後にすべての**LIF**がホームポートにあることを確認する

ONTAPのアップグレードプロセス中に発生するリブートの際に、一部のLIFがホームポートから割り当てられたフェイルオーバーポートに移行されることがあります。アップグレード後、ホームポートにないLIFを有効にしてリバートする必要があります。

手順

1. すべてのLIFのステータスを表示します。

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

   いずれかのLIFについて、* Status Admin が「**down**」または is home *が「false」の場合は、次の手順に進みます。

2. データLIFを有効にします。

```
network interface modify {-role data} -status-admin up
```

3. LIFをそれぞれのホームポートにリバートします。

```
network interface revert *
```

4. すべてのLIFがそれぞれのホームポートにあることを確認します。

```
network interface show
```

次の例では、SVM vs0のすべてのLIFがそれぞれのホームポートにあります。

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network          Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node     Port    Home
-------- ---------- ---------- ---------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24   node0    e0e     true
         data002    up/up      192.0.2.121/24   node0    e0f     true
         data003    up/up      192.0.2.122/24   node0    e2a     true
         data004    up/up      192.0.2.123/24   node0    e2b     true
         data005    up/up      192.0.2.124/24   node1    e0e     true
         data006    up/up      192.0.2.125/24   node1    e0f     true
         data007    up/up      192.0.2.126/24   node1    e2a     true
         data008    up/up      192.0.2.127/24   node1    e2b     true
8 entries were displayed.
```

関連情報

- "ネットワークインターフェイス"

特別な設定

アップグレード後の特定の**ONTAP**設定の確認

クラスタの構成が次のいずれかに該当する場合は、ONTAPソフトウェアのアップグレード後に追加の手順が必要になることがあります。

確認する項目	回答が * はい * の場合、次の操作を実行します ...
ONTAP 9 .7以前からONTAP 9 .8以降にアップグレードしましたか？	ネットワーク構成の確認 EMS 宛先への到達可能性を提供しないネットワーク サービス ポリシーから EMS LIF サービスを削除します。
クラスタはMetroCluster構成に含まれていますか。	ネットワークとストレージのステータスを確認する
SAN構成を使用しているか。	SAN構成の確認
ONTAP 9 .3以前からアップグレードし、NetAppストレージ暗号化を使用していますか。	KMIPサーバ接続の再設定
負荷共有ミラーがあるか。	移動した負荷共有ミラーのソースボリュームの再配置
ONTAP 9 9.1より前のバージョンで作成されたサービスプロセッサ（SP）アクセスのユーザアカウントはありますか。	サービスプロセッサにアクセスできるアカウントの変更を確認する

アップグレード後の**ONTAP**ネットワーク構成の確認

ONTAP 9 .7x以前のバージョンからONTAP 9 .8以降にアップグレードしたら、ネットワーク設定を確認する必要があります。アップグレード後、ONTAPはレイヤ2の到達可能性を自動的に監視します。

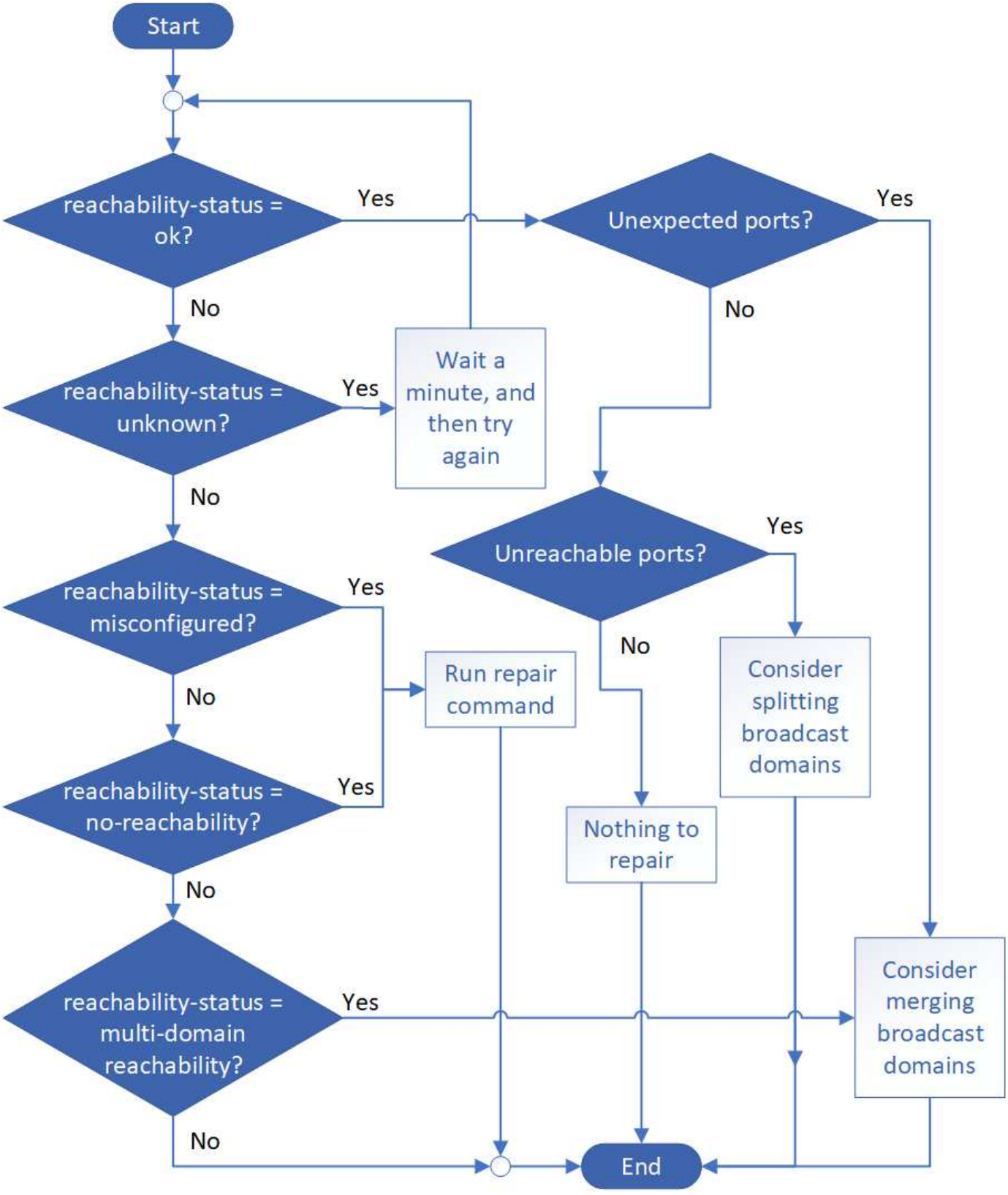
ステップ

1. 各ポートに想定されるブロードキャストドメインへの到達可能性があることを確認します。

   ```
   network port reachability show -detail
   ```

   の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。

このコマンド出力には、到達可能性の結果が表示されます。次のDecision Treeと表を使用して、到達可能性の結果（到達可能性ステータス）を理解し、次に何をすべきかを判断します。



プレゼンスステータス	説明

OK	ポートに割り当てられているブロードキャストドメインにレイヤ 2 の到達可能性があります。 到達可能性ステータスが「ok」で、「予期しないポート」がある場合は、1つ以上のブロードキャストドメインをマージすることを検討してください。詳細については、を参照してください "ブロードキャストドメインのマージ"。 到達可能性ステータスが「ok」で、到達不能なポートがある場合は、1つ以上のブロードキャストドメインをスプリットすることを検討してください。詳細については、を参照してください "ブロードキャストドメインのスプリット"。 到達可能性ステータスが「ok」で、予期しないポートや到達不能なポートがない場合、設定は正しいです。
誤設定 - 到達可能性	ポートに割り当てられているブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、到達可能なブロードキャストドメインにポートが割り当てられます。 `network port reachability repair -node -port` 詳細については、を参照してください "ポートの到達可能性を修復"。 の詳細については `network port reachability repair`、を"ONTAPコマンド リファレンス"参照してください。
到達不能	既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、自動的にデフォルトIPspace内に作成された新しいブロードキャストドメインにポートが割り当てられます。 `network port reachability repair -node -port` 詳細については、を参照してください "ポートの到達可能性を修復"。
multi-domain-reachable	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、ポートに割り当てられているブロードキャストドメインを1つ以上のブロードキャストドメインにマージする必要がないかどうかを確認します。 詳細については、またはを参照してください"ブロードキャストドメインのマージ""ポートの到達可能性を修復"。

不明	reachable-status が「 unknown 」の場合は、数分待ってからもう一度コマンドを実行してください。

ポートを修理したら、削除されたLIFとVLANを確認して解決する必要があります。ポートがインターフェイスグループに属していた場合は、そのインターフェイスグループの状況についても理解しておく必要があります。詳細については、を参照してください "ポートの到達可能性を修復"。

ONTAPのアップグレード後にネットワークサービスポリシーから**EMS LIF**サービスを削除する

ONTAP 9.7 以前から ONTAP 9.8 以降にアップグレードする前にイベント管理システム (EMS) メッセージを設定している場合、アップグレード後に EMS メッセージが配信されない可能性があります。

アップグレード中、 `management-ems` EMS LIF サービスである が、管理 SVM 内のすべての既存のサービス ポリシーに追加されます。これにより、サービスポリシーに関連付けられた任意のLIFからEMSメッセージを送信できるようになります。選択したLIFがイベント通知の送信先に到達できない場合、メッセージは配信されません。

これを防ぐには、アップグレード後に、宛先への到達可能性を提供しないネットワーク サービス ポリシーから EMS LIF サービスを削除する必要があります。

"ONTAP LIFとサービスポリシーの詳細"です。

手順

1. EMS メッセージを送信できる LIF と関連するネットワーク サービス ポリシーを識別します。

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------   ------------------
cluster-1      cluster_mgmt   default-management
cluster-1      node1-mgmt     default-management
cluster-1      node2-mgmt     default-management
cluster-1      inter_cluster  default-intercluster
4 entries were displayed.
```

2. 各LIFがEMSデスティネーションに接続されているかどうかを確認します。

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

各ノードでこの手順を実行します。

例

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. advanced権限レベルに切り替えます。

```
set advanced
```

4. 到達可能性のないLIFの場合は、 `management-ems`対応するサービス ポリシーからの LIF サービス:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

の詳細については `network interface service-policy remove-service`、を"ONTAPコマンドリファレンス"参照してください。

5. management-ems LIFが、EMSデスティネーションに到達できるようにするLIFにのみ関連付けられていることを確認します。

```
network interface show -fields service-policy -services management-ems
```

ONTAPアップグレード後の**MetroCluster**構成のネットワークとストレージのステータスの確認

MetroCluster構成のONTAPクラスタをアップグレードしたら、各クラスタのLIF、アグリゲート、およびボリュームのステータスを確認する必要があります。

1. LIFのステータスを確認します。

```
network interface show
```

通常運用時は、ソースSVMのLIFの管理ステータスが稼働状態で、ホーム ノードに配置されている必要があります。デスティネーションSVMのLIFについては、稼働し、ホーム ノードに配置されている必要はありません。スイッチオーバー時には、すべてのLIFの管理ステータスが稼働状態になっている必要がありますが、ホーム ノードに配置されている必要はありません。

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                   e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                   e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                   e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                   e3c
true
            ...

27 entries were displayed.
```

2. アグリゲートの状態を確認します。

```
storage aggregate show -state !online
```

このコマンドを実行すると、オンラインでないアグリゲートが表示されます。通常運用時は、ローカルサイトにあるすべてのアグリゲートがオンラインになっている必要があります。ただし、MetroCluster構成がスイッチオーバー中の場合は、ディザスタリカバリサイトにあるルートアグリゲートをオフラインにできます。

次の例は、通常運用時のクラスタを示しています。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

次の例は、スイッチオーバー時のクラスタを示しています。ディザスタ リカバリ サイトにあるルートアグリゲートはオフラインです。

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. ボリュームの状態を確認します。

```
volume show -state !online
```

このコマンドを実行すると、オンラインでないボリュームが表示されます。

通常運用時（スイッチオーバー状態ではない）のMetroCluster構成には、クラスタのセカンダリSVM（名前に「-mc」が付いているSVM）が所有するすべてのボリュームが表示されます。

これらのボリュームはスイッチオーバー時にのみオンラインになります。

次の例は、通常運用時のクラスタを示しています。ディザスタ リカバリ サイトにあるボリュームはオフラインです。

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. 整合性のないボリュームがないことを確認します。

```
volume show -is-inconsistent true
```

参照"NetAppナレッジベース: ボリュームにWAFLの不整合が表示される"不一致なボリュームに対処する方法について。

ONTAPアップグレード後のSAN構成の確認

ONTAPのアップグレード後、SAN環境では、アップグレード前にLIFに接続されていた各イニシエータがLIFに正常に再接続されたことを確認する必要があります。

1. 各イニシエータが正しいLIFに接続されていることを確認します。

   イニシエータのリストを、アップグレードの準備時に作成したリストと比較する必要があります。ONTAP 9.11.1以降を実行している場合は、System Managerを使用して接続ステータスを確認すると、CLIよりもはるかにわかりやすくなります。

System Manager

a. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストがページに表示されます。リストが大きい場合は、ページの右下隅にあるページ番号をクリックして、リストの追加ページを表示できます。

   igroupに関するさまざまな情報が列に表示されます。9.11.1以降では、igroupの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると、詳細が表示されます。

CLI

- iSCSIイニシエータをリストします

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- FCイニシエータをリスト表示：

```
fcp initiator show -fields igroup,wwpn,lif
```

ONTAP 9 .2以前からのアップグレード後に**KMIP**サーバ接続を再設定する

ONTAP 9 .2以前のバージョンからONTAP 9 .3以降にアップグレードした場合は、外部キー管理（KMIP）サーバの接続を再設定する必要があります。

手順

1. キー管理ツールの接続を設定します。

```
security key-manager setup
```

2. KMIPサーバを追加します。

```
security key-manager add -address <key_management_server_ip_address>
```

3. KMIPサーバが接続されていることを確認します。

```
security key-manager show -status
```

4. キー サーバを照会します。

```
security key-manager query
```

5. 新しい認証キーとパスフレーズを作成します。

```
security key-manager create-key -prompt-for-key true
```

32 文字以上のパスフレーズを設定してください。

6. 新しい認証キーを照会します。

```
security key-manager query
```

7. 新しい認証キーを自己暗号化ディスク（SED）に割り当てます。

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```

クエリからの新しい認証キーを使用します。

8. 必要に応じて、FIPSキーをSEDに割り当てます。

```
storage encryption disk modify -disk <disk_id> -fips-key-id
<fips_authentication_key_id>
```

セキュリティの設定によりデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。それ以外の場合は、両方に同じ認証キーを使用します。

関連情報

- "security key-manager setupの実行"
- "ストレージ暗号化ディスクの変更"

ONTAPのアップグレード後に移動した負荷共有ミラーのソースボリュームの再配置

ONTAPをアップグレードしたら、負荷共有ミラーのソースボリュームをアップグレード前の場所に戻す必要があります。

手順

1. 負荷共有ミラーのソースボリュームを移動する前に作成したレコードを使用して、負荷共有ミラーのソースボリュームの移動先を特定します。
2. 負荷共有ミラーのソースボリュームを元の場所に戻します。

```
volume move start
```

ONTAPのアップグレード後にサービスプロセッサにアクセスできるユーザアカウントの変更

admin以外のロールでサービスプロセッサ（SP）にアクセスできるユーザアカウントをONTAP 9 .8以前で作成した場合、ONTAP 9 .9.1以降にアップグレードすると、パラメータのadmin以外の値 `-role`がに変更され `admin`ます。

詳細については、を参照してください "SPにアクセスできるアカウント"。

ONTAPのアップグレード後に**Disk Qualification Package**を更新する

ONTAPソフトウェアをアップグレードしたら、ONTAP Disk Qualification Package（DQP）をダウンロードしてインストールする必要があります。ONTAPのアップグレードの一環としてDQPが更新されることはありません。

DQPには、新しく認定されたすべてのドライブとONTAPがやり取りするための正しいパラメータが含まれています。お使いのバージョンのDQPに新しく認定されたドライブの情報が含まれていない場合、ONTAPはドライブを適切に構成するための情報を得られません。

DQPは四半期ごとに更新することを推奨します。また、次のような場合にもDQPを更新する必要があります。

- 新しいタイプやサイズのドライブをクラスタ内のノードに追加したとき

  たとえば、1TBのドライブをすでに使用している場合に2TBのドライブを追加するには、DQPの最新情報を確認する必要があります。

- ディスクファームウェアを更新したとき
- 新しいディスクファームウェアまたはDQPファイルが利用可能になったとき

関連情報

- "NetAppのダウンロード：Disk Qualification Package"
- "NetAppのダウンロード：ディスクドライブファームウェア"

ファームウェア、システム、セキュリティの更新

ONTAPでのファームウェア、システム、セキュリティの更新の概要

ONTAPのバージョンに応じて、自動ファームウェア、システム、およびセキュリティの更新を有効にすることができます。

ONTAPバージョン	ジドウコウシンノナイヨウ
9.16.1以降	• 人工知能（ARP / AI）による自律型ランサムウェア対策 • ONTAPタイムゾーンデータベース • ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア • サービスプロセッサおよびBMCモジュール用のSP / BMCファームウェア
9.13.1以降	• ONTAPタイムゾーンデータベース • ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア • サービスプロセッサおよびBMCモジュール用のSP / BMCファームウェア
9.10.1以降	• ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア • サービスプロセッサおよびBMCモジュール用のSP / BMCファームウェア
9.9.1以前	サポート対象外

お使いのバージョンのONTAPで自動更新が利用できない場合、または自動更新が有効になっていない場合は、ファームウェア、タイムゾーンデータベース、およびセキュリティ更新を手動で実行できます。

関連リンク

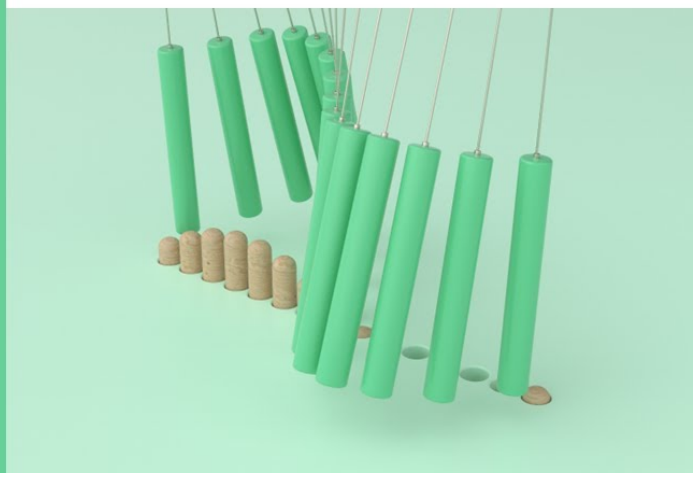
- "ファームウェアを手動で更新する方法"
- "技術情報記事「ONTAP 9でタイムゾーン情報を更新する方法」"
- "セキュリティ更新を手動で行う方法"

ビデオ:自動ファームウェアアップデート機能

ONTAP 9.10.1以降で利用できる自動ファームウェア更新機能を確認してください。

Automatic Firmware Update feature is available starting in ONTAP 9.10.1

By Jim Svesnik,
Quality Assurance Engineer



インストールの自動更新をスケジュールする方法

同じクラスタ内の対象となるすべてのノードが自動更新対象としてグループ化されます。対象となるノードの自動更新がスケジュールされる期間は、更新の優先度レベルと、環境内で更新が必要なシステムの割合によって異なります。

たとえば、システム全体の10%以下が優先度の低いアップデートの対象となる場合、対象となるすべてのシステムに対して1週間以内にアップデートがスケジュールされます。ただし、システム全体の76%以上が優先度の低いアップデートの対象である場合は、対象となるシステム間で8週間にわたって順次アップデートが行われます。この段階的インストールは、修正が必要な更新に関する問題が発生した場合の環境全体のリスクを軽減するのに役立ちます。

週ごとに自動更新がスケジュールされているシステム全体の割合は、次のとおりです。

重要な更新について

更新が必要なシステムの割合	**1**週目に更新される割合	**2**週目に更新される割合
50%以下	100%	
51～100%	30%	70%

優先度の高いアップデート

更新が必要なシステムの割合	週ごとに発生する更新の割合			
	* 1週目*	* 2週目*	* 3週目*	* 4週目*
* 25%以下*	100%			

更新が必要なシステムの割合	週ごとに発生する更新の割合			
* 26-50%*	30%	70%		
* 50-100%*	10%	20%	30%	40%

通常の優先度の更新の場合

更新が必要なシステムの割合	週ごとに発生する更新の割合							
	* 1週目*	* 2週目*	* 3週目*	* 4週目*	* 5週目*	* 6週目*	* 7週目*	* 8週目*
* 10%以下*	100%							
* 11-20%*	30%	70%						
* 21-50%*	10%	20%	30%	40%				
* 51-75%*	5%	10%	15%	20%	20%	30%		
* 76-100%*	5%	5%	10%	10%	15%	15%	20%	20%

自動更新を有効にする

自動更新を有効にすると、ONTAPが手動操作なしでファームウェア、システム、およびセキュリティ更新プログラムをダウンロードしてインストールできるようになります。

自動更新を有効にするには、EULA の条件に同意し、環境に応じて各システム コンポーネントのデフォルトの更新動作を確認または構成する必要があります。

各システム コンポーネントの自動更新の可用性は、 ONTAPのバージョンによって異なります。

ONTAPのバージョン	利用可能な自動更新
9.16.1以降	• 人工知能（ARP / AI）による自律型ランサムウェア対策 • ONTAPタイムゾーンデータベース • ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア • サービスプロセッサおよびBMCモジュール用のSP / BMCファームウェア • Disk Qualification Package（DQP）

ONTAPのバージョン	利用可能な自動更新
9.13.1以降	• ONTAPタイムゾーンデータベース • ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア • サービスプロセッサおよびBMCモジュール用のSP / BMCファームウェア • Disk Qualification Package（DQP）
9.10.1以降	• ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア • サービスプロセッサおよびBMCモジュール用のSP / BMCファームウェア • Disk Qualification Package（DQP）

開始する前に

- 最新のサポート契約が必要です。これは、*[システムの詳細]*ページで確認できます"NetApp Support Site"。
- 自動更新を有効にするには、最初にHTTPSでAutoSupportを有効にする必要があります。クラスタでAutoSupportが有効になっていない場合や、別の転送プロトコルを使用してクラスタでAutoSupportが有効になっている場合は、この手順の実行中にHTTPSで有効にすることができます。

> AutoSupport OnDemandはデフォルトで有効になり、HTTPS転送プロトコルを使用してテクニカルサポートにメッセージを送信するように設定すると機能します。

- ONTAP 9.10.1以降で自動更新を有効にする場合は、次の追加URLへのHTTPS接続が確立されていることを確認してください。
  - https://support-sg-naeast.netapp.com
  - https://support-sg-nawest.netapp.com

タスクの内容

ONTAP 9.16.1 より前に作成され、その後 9.16.1 以降にアップグレードされたクラスタの場合:

- 自動更新機能がすでに有効になっている場合、アップグレード後もシステム コンポーネント更新のデフォルトは変更されません。
- 自動更新がまだ有効になっていない場合は、 ONTAP 9.16.1 以降のシステム コンポーネント更新のデフォルトが適用されます。

自動システム コンポーネント更新のデフォルトは、 ONTAP のバージョンに応じて、自動的に更新するか通知を表示するかのいずれかに設定されています。手順を完了する前に、これらの設定が環境に対して正しいことを確認してください。

ここでは "ビデオ"、自動更新プロセスの使用方法の概要を示します。

例 **5.** 手順

System Manager - ONTAP 9.16.1以降

1. System Managerで、* Cluster > Settings *の順に選択します。
2. HTTPSでAutoSupport OnDemandを有効にしていない場合は、を選択して続行するために必要な設定を有効にします。
3. セクションで、[有効化]*を選択します。
4. 更新タイプごとに実行するアクションを指定します。

   各更新タイプの更新を自動的に更新するか、通知を表示するか、または更新を自動的に却下するかを選択できます。

5. 利用条件に同意し、*[保存]*を選択します。

System Manager - ONTAP 9.15.1以前

1. System Managerで、*[イベント]*を選択します。
2. セクションの[自動更新を有効にする]の横にある[操作]>[有効にする]*を選択します。
3. AutoSupportでHTTPSが有効になっていない場合は、有効にする場合に選択します。
4. 利用条件に同意し、*[保存]*を選択します。

CLI

1. 自動ファームウェア更新を有効にします。

```
system service-processor image modify -node <node_name> -autoupdate
true
```

関連情報

- "AutoSupportを使用する準備"
- "HTTPS経由のAutoSupportメッセージ配信のトラブルシューティング"

自動更新の変更

自動更新機能が有効になっていて、デフォルトのシステム コンポーネントの設定がされている場合、 ONTAP は推奨されるすべての更新を自動的に検出し、ダウンロードしてインストールできます。推奨される更新をインストール前に確認したり、自動的に却下したりする必要がある場合は、デフォルトの動作を希望する設定に変更できます。

例 **6.** 手順

ONTAP 9.16.1以降

1. System Managerで、*[クラスタ]>[設定]*に移動します。
2. [ソフトウェアの更新]*セクションで、を選択します →。
3. [その他のすべてのアップデート]タブを選択し、*[自動アップデート設定の編集]*をクリックします。
4. 更新タイプごとに実行するデフォルトのアクションを指定します。

   各更新タイプの更新を自動的に更新するか、通知を表示するか、または更新を自動的に却下するかを選択できます。

   ⓘ ONTAPタイムゾーンデータベースは、*システムファイル*更新タイプによって制御されます。

5. 利用条件に同意し、*[保存]*を選択します。

ONTAP 9.15.1以前

1. System Manager で、 * Cluster > Settings * の順にクリックします。
2. [自動更新]セクションで、をクリックし ⋮ てアクションのリストを表示します。
3. [自動更新設定の編集] をクリックします。
4. 更新タイプごとに実行するデフォルトのアクションを指定します。

   各タイプの更新を自動的に更新するか、通知を表示するか、または更新を自動的に却下するかを選択できます。

   ⓘ ONTAPタイムゾーンデータベースは、システムファイルの更新タイプによって制御されます。

推奨される自動更新の管理

自動更新ログには、更新に関する推奨事項のリストと、説明、カテゴリ、インストール予定時刻、ステータス、エラーなどの詳細が表示されます。ログを表示して、各推奨事項に対して実行するアクションを決定できます。

手順

1. 推奨事項のリストを表示します。

をクラスタ設定から表示します	更新タブからの表示
a. [クラスタ]>[設定]*をクリックします。 b. ONTAPのバージョンに応じて、次のいずれかを実行します。 ◦ ONTAP 9 .15.1以前の場合は、*自動更新*セクションでをクリックし、オプションをクリックしてすべての更新を表示します。 ◦ ONTAP 9 .16.1以降の場合は、ソフトウェアアップデート*セクションでを選択します。[その他のすべてのアップデート]ペインの右隅にある[その他のアップデート]*をクリックし、オプションをクリックしてすべてのアップデートを表示します。	a. [クラスタ]>[概要]*をクリックします。 b. [概要]セクションで、[その他]*をクリックし、[ONTAPの更新]*をクリックします。 c. ONTAPのバージョンに応じて、次の手順を実行します。 ◦ ONTAP 9 .15.1以前の場合は、*ファームウェア・アップデート*をクリックします。 ◦ ONTAP 9 .16.1以降の場合は、*その他のすべてのアップデート*をクリックします。 d. 更新ページで*詳細*をクリックし、オプションをクリックしてすべての更新を表示します。

2. 説明の横にあるをクリックする と、推奨事項に対して実行できる操作のリストが表示されます。

   推奨構成の状態に応じて、次のいずれかの操作を実行できます。

更新の状態	可能です
はスケジュールされていません	• アップデート * ：アップデート処理を開始します。 • スケジュール *: 更新プロセスを開始する日付を設定できます。 • Dismiss * ：推奨事項をリストから削除します。
がスケジュールされました	• アップデート * ：アップデート処理を開始します。 • スケジュールの編集 *: 更新プロセスを開始するためのスケジュールされた日付を変更できます。 • スケジュールのキャンセル *: スケジュールされた日付をキャンセルします。
が却下されました	• Unun求め * ：推奨事項をリストに返します。
が適用されているか、ダウンロード中です	• キャンセル * ：更新をキャンセルします。

ファームウェアの手動更新

System.9.1以降ONTAP 9では、に登録している場合、"Active IQ Unified Manager"System Managerでアラートを受信し、サポートされているデバイス（ディスク、ディスクシェルフ、サービスプロセッサ（SP）、ベースボード管理コントローラ（BMC）など）のファームウェアの更新がクラスタで保留になっていることを通知できます。

ONTAP 9 .8を実行している場合、またはActive IQ Unified Managerに登録していない場合は、NetAppサポートサイトに移動してファームウェアの更新をダウンロードします。

開始する前に

ファームウェアをスムーズに更新するためには、更新を開始する前にSPまたはBMCをリブートする必要があります。コマンドを使用し `system service-processor reboot-sp -node node_name`てリブートします。の詳細については `system service-processor reboot-sp`、を"ONTAPコマンド リファレンス"参照してください。

手順

使用しているONTAPのバージョンと、Active IQ Unified Managerに登録されている場合は、該当する手順に従ってください。

デジタルアドバイザ搭載の**ONTAP 9 .16.1**以降

手順

1. System Managerで、*[ダッシュボード]*に移動します。

   「 * Health * 」セクションに、クラスタに推奨されるファームウェア・アップデートがあるかどうかを示すメッセージが表示されます。

2. アラートメッセージをクリックします。
3. 推奨される更新プログラムのリストのセキュリティ更新プログラムの横にある*[アクション]*を選択します。
4. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。

   更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。

ONTAP 9 .9.1から**9.15.1**（**Digital Advisor**使用時）

1. System Managerで、*[ダッシュボード]*に移動します。

   「 * Health * 」セクションに、クラスタに推奨されるファームウェア・アップデートがあるかどうかを示すメッセージが表示されます。

2. アラートメッセージをクリックします。

   [* ファームウェア・アップデート *] タブが [* アップデート *] ページに表示されます。

3. 実行するファームウェア更新の*[NetAppサポートサイトからダウンロード]*をクリックします。

   NetAppサポートサイトが表示されます。

4. NetAppサポートサイトにログインし、更新に必要なファームウェアイメージパッケージをダウンロードします。
5. ネットワーク上のHTTPサーバまたはFTPサーバ、またはローカルフォルダにファイルをコピーします。
6. System Manager で、 * Cluster > Overview * をクリックします。
7. ペインの右隅で[その他]をクリックし、[ONTAPの更新]*を選択します。
8. [* ファームウェア・アップデート *] をクリックします。
9. ONTAPのバージョンに応じて、次の手順を実行します。

ONTAP 9.9.1および9.10.0	ONTAP 9.10.1以降
a. サーバーから * を選択するか、 * ローカルクライアント * を選択します b. サーバのURLまたはファイルの場所を指定します。	a. 推奨される更新プログラムのリストで、*[アクション]*を選択します。 b. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。 更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。 c. [ファームウェアの更新]*ボタンを選択します。

ONTAP 9 .8以降（デジタルアドバイザなし）

1. に移動"NetAppサポートサイト"してログインします。
2. クラスタファームウェアの更新に使用するファームウェアパッケージを選択します。
3. ネットワーク上のHTTPサーバまたはFTPサーバ、またはローカルフォルダにファイルをコピーします。
4. System Manager で、 * Cluster > Overview * をクリックします。
5. 概要*ペインの右隅で*詳細*をクリックし、 ONTAPアップデート*または*ソフトウェアアップデート*（バージョンによって異なります）を選択します。
6. ONTAPのバージョンに応じて、次の手順を実行します。
   - ONTAP 9 .15.1以前の場合は、*ファームウェア・アップデート*をクリックします。
   - ONTAP 9 .16.1以降の場合は、*その他のすべてのアップデート*をクリックします。
7. ONTAPのバージョンに応じて、次の手順を実行します。

ONTAP 9 .8、9.9.1、および9.10.0	ONTAP 9.10.1以降
1. サーバーから * を選択するか、 * ローカルクライアント * を選択します 2. サーバのURLまたはファイルの場所を指定します。	1. 推奨される更新プログラムのリストで、*[アクション]*を選択します。 2. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。 更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。 3. [ファームウェアの更新]*ボタンを選択します。

終了後

アップデートは、 * ファームウェア・アップデートの概要 * で監視または確認できます。却下された更新プロ

グラムまたはインストールに失敗した更新プログラムを表示するには、ONTAPのバージョンに応じて次のいずれかを実行します。

- ONTAP 9 .15.1以前の場合は、*[クラスタ]>[設定]>[自動更新]>[すべての自動更新を表示]*をクリックします。
- ONTAP 9 .16.1以降の場合は、**[クラスタ]>[設定]>[**ソフトウェアの更新**]***をクリックします。**[**その他のすべての更新**]**ペインの右隅にある[その他の更新]をクリックし⋮、[すべての自動更新を表示]*を選択します。

ONTAPのリバート

ONTAPクラスタをリバートするにはテクニカルサポートが必要ですか。

次の状況では、ONTAPクラスタをリバートする前にテクニカルサポートにお問い合わせください。

- 本番環境

  テクニカル・サポートの支援なしに本番環境クラスタをリバートしないでください。

- ONTAP 9.5以降でボリュームを作成し、以前のバージョンにリバートする必要がある。

  適応圧縮を使用するボリュームは、リバート前に圧縮を解除する必要があります。

新規クラスタまたはテストクラスタは支援なしでリバートできます。次のいずれかの問題が発生してクラスタをリバートしようとした場合は、テクニカルサポートにお問い合わせください。

- リバートが失敗するか完了できません。
- リバートは終了したが、本番環境でクラスタを使用できない。
- リバートが終了してクラスタが本番環境に移行したが、正しく動作しない。

サポートされるONTAPリバートパス

ONTAPソフトウェアを現在のONTAPバージョンよりも前の1つのリリースに直接リバートすることができます。たとえば、9.15.1を実行している場合、9.13.1に直接リバートすることはできません。9.14.1にリバートしてから、9.14.1から9.13.1への個別のリバートを実行する必要があります。

ONTAP 9.4以前へのリバートはサポートされていません。サポートされていないバージョンのONTAPにリバートしないでください。

コマンドを使用して、各ノードで実行されているONTAPのバージョンを確認できます `system image show`。

サポートされる次のリバートパスは、オンプレミスのONTAPリリースのみを対象としています。クラウドでのONTAPのリバートについては、を参照してください "Cloud Volumes ONTAP をリバートまたはダウングレードする"。

現在実行しているバージョン	目的
ONTAP 9.17.1	ONTAP 9 .16.1
ONTAP 9 .16.1	ONTAP 9 .15.1
ONTAP 9 .15.1	ONTAP 9 .14.1
ONTAP 9 .14.1	ONTAP 9 .13.1
ONTAP 9 .13.1	ONTAP 9 12.1
ONTAP 9 12.1	ONTAP 9 .11.1
ONTAP 9 .11.1	ONTAP 9 10.1
ONTAP 9 10.1	ONTAP 9 .9.1
ONTAP 9 .9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5

ONTAPのリバートに関する問題と制限事項

ONTAPクラスタをリバートする前に、リバートの問題と制限事項を考慮する必要があります。

- リバートではシステムが停止します。

  リバートの実行中はクライアントからアクセスできなくなります。本番環境クラスタをリバートする場合は、この停止時間を考慮して計画してください。

- リバートを実行すると、クラスタ内のすべてのノードが対象になります。

  リバートはクラスタ内のすべてのノードに影響しますが、リバートはHAペアごとに実行して完了してから、他のHAペアをリバートする必要があります。

- リバートは、すべてのノードで新しいターゲットリリースが実行されると完了です。

  クラスタに複数のバージョンが混在している場合は、リバート要件を満たすために必要なコマンドを除き、クラスタの処理や構成を変更するコマンドは実行しないでください（監視処理は可能です）。

一部のノードのみをリバートした状態で、クラスタを元のリリースにアップグレードしないでください。

- ノードをリバートすると、Flash Cacheモジュール内のキャッシュデータがクリアされます。

  Flash Cacheモジュールにはキャッシュデータがないため、ノードは初回の読み取り要求をディスクから処理するため、この期間の読み取りパフォーマンスが低下します。読み取り要求に対応するたびに、再びキャッシュにデータが蓄えられます。

- ONTAP 9 .xで実行されているテープにバックアップしたLUNは、9.x以降のリリースにのみリストアできます。以前のリリースにはリストアできません。
- 現在使用しているバージョンのONTAPがインバンドACP（IBACP）機能をサポートしている場合に、IBACPをサポートしていないバージョンのONTAPにリバートすると、ディスクシェルフへの代替パスは無効になります。
- LDAPを使用しているStorage Virtual Machine（SVM）がある場合は、リバートの前にLDAPリファーラルを無効にする必要があります。
- MetroClusterに準拠しているがMetroCluster検証されていないスイッチを使用するMetroCluster IPシステムでは、ONTAP 9 .6以前を使用するシステムはサポートされないため、ONTAP 9 .7から9.6へのリバートにはシステムが停止します。
- ノードをONTAP 9.13.1以前にリバートする前に、暗号化されたSVMルートボリュームを暗号化されていないボリュームに変換する必要があります。

  SVMルートボリュームの暗号化をサポートしていないバージョンにリバートしようとすると、警告が表示されてリバートがブロックされます。

ONTAPリバートの準備

ONTAPクラスタをリバートする前に確認するリソース

ONTAPクラスタをリバートする前に、ハードウェアのサポートを確認し、発生する可能性がある問題や解決が必要な問題についてリソースを確認する必要があります。

1. ターゲットリリースのを確認します"ONTAP 9 リリース ノート"。

   「重要な注意事項」セクションでは、ダウングレードまたはリバートの前に注意すべき潜在的な問題について説明します。

2. ハードウェアプラットフォームがターゲットリリースでサポートされていることを確認します。

   "NetApp Hardware Universe"

3. クラスタスイッチと管理スイッチがターゲットリリースでサポートされていることを確認します。

   NX-OS（クラスタネットワークスイッチ）、IOS（管理ネットワークスイッチ）、およびRCFソフトウェアのバージョンがリバート先のONTAPのバージョンに対応していることを確認する必要があります。

   "NetAppのダウンロード：Ciscoイーサネットスイッチ"

4. クラスタがSAN用に構成されている場合は、SAN構成が完全にサポートされていることを確認します。

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

"NetApp Interoperability Matrix Tool"

ONTAPクラスタをリバートする前に実行するシステム検証

ONTAPクラスタをリバートする前に、クラスタの健全性、ストレージの健全性、およびシステム時間を確認する必要があります。また、クラスタで実行中のジョブがないことを確認する必要があります。

クラスタの健全性を確認

ONTAPクラスタをリバートする前に、ノードが正常に機能していてクラスタに追加するための条件を満たしていること、およびクラスタがクォーラムにあることを確認する必要があります。

手順

1. クラスタ内のノードがオンラインであり、クラスタに参加するための条件を満たしていることを確認します。

```
cluster show
```

この例では、すべてのノードが正常に機能しており、クラスタに参加するための条件を満たしています。

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

正常でないノードや条件を満たしていないノードがある場合は、EMSログでエラーを確認して対処します。

2. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

と入力し `y`て続行します。

3. 各RDBプロセスの設定の詳細を確認します。

   - リレーショナルデータベースのエポックとデータベースのエポックは、各ノードで一致している必要があります。
   - リングごとのクォーラムマスターがすべてのノードで同じである必要があります。

各リングのクォーラムマスターが異なる場合があることに注意してください。

表示する **RDB** プロセス	入力するコマンド
管理アプリケーション	`cluster ring show -unitname mgmt`
ボリューム ロケーション データベース	`cluster ring show -unitname vldb`
仮想インターフェイス マネージャ	`cluster ring show -unitname vifmgr`
SAN管理デーモン	`cluster ring show -unitname bcomd`

次の例は、ボリューム ロケーション データベースのプロセスを示しています。

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

5. SAN環境を使用している場合は、各ノードがSANクォーラムにあることを確認します。

```
event log show  -severity informational -message-name scsiblade.*
```

各ノードの最新のscsibladeイベントメッセージに、SCSIブレードがクォーラムにあることが示されます。

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node        Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

関連情報

"システム管理"

ストレージの健全性を確認

ONTAPクラスタをリバートする前に、ディスク、アグリゲート、およびボリュームのステータスを確認する必要があります。

手順

1. ディスクのステータスを確認します。

確認する項目	操作
破損ディスク	a. 破損ディスクを表示します。 `storage disk show -state broken` b. 破損ディスクを取り外すか交換します。
メンテナンス中または再構築中のディスク	a. メンテナンス、保留、または再構築中の状態のディスクを表示します。 `storage disk show -state maintenance`
pending	reconstructing ---- .. メンテナンスまたは再構築の処理が完了するまで待ってから次に進みます。

2. 物理ストレージと論理ストレージ（ストレージのアグリゲートも含む）の状態を表示して、すべてのアグリゲートがオンラインであることを確認します。+

```
storage aggregate show -state !online
```

このコマンドを実行すると、オンラインでないアグリゲートが表示されます。メジャーアップグレードまたはリバートの実行前と実行後に、すべてのアグリゲートがオンラインになっている必要があります。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. 次のコマンドを実行して、すべてのボリュームがオンラインであることを確認します。 _not_online

```
volume show -state !online
```

メジャーアップグレードまたはリバートの実行前と実行後に、すべてのボリュームがオンラインになっている必要があります。

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 整合性のないボリュームがないことを確認します。

```
volume show -is-inconsistent true
```

参照"NetAppナレッジベース: ボリュームにWAFLの不整合が表示される"不一致なボリュームに対処する方法について。

関連情報

"ディスクおよびアグリゲートの管理"

システム時間の確認

ONTAPクラスタをリバートする前に、NTPが設定されていること、およびクラスタ全体で時刻が同期されていることを確認する必要があります。

手順

1. クラスタがNTPサーバに関連付けられていることを確認します。

```
cluster time-service ntp server show
```

2. 各ノードの日付と時刻が同じであることを確認します。

```
cluster date show
```

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

実行中のジョブがないことを確認する

ONTAPクラスタをリバートする前に、クラスタジョブのステータスを確認する必要があります。アグリゲート、ボリューム、NDMP（ダンプまたはリストア）、またはSnapshotに関する実行中のジョブ（作成、削除、移動、変更、複製、マウントなど）やキューに格納されているジョブがある場合は、ジョブが完了するまで待つか、キューのエントリを停止します。

手順

1. アグリゲート、ボリューム、またはSnapshotに関する実行中のジョブとキューに登録されているジョブのリストを確認します。

```
job show
```

この例では、2つのジョブがキューに登録されています。

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
8629   Vol Reaper           cluster1   -              Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                            cluster1   -              Queued
       Description: Certificate Expiry Check
```

2. アグリゲート、ボリューム、またはSnapshotに関する実行中のジョブとキューに登録されているジョブを削除します。

```
job delete -id <job_id>
```

3. アグリゲート、ボリューム、またはSnapshotに関する実行中のジョブとキューに登録されているジョブがないことを確認します。

```
job show
```

次の例では、実行中のジョブとキューに登録されているジョブがすべて削除されています。

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

関連情報

- "storage disk show"

ONTAPのバージョン固有のリバート前チェックを実行する

使用しているONTAPのバージョンに応じたリバート前のタスク

ONTAPのバージョンによっては、リバートプロセスを開始する前に追加の準備作業が必要になる場合があります。

リバート元	リバートプロセスを開始する前に実行する処理
ONTAP 9の任意のバージョン	• "継続的可用性を備えていないSMBセッションを終了する"です。 • "SnapMirror関係とSnapVault関係のリバート要件の確認"です。 • "重複排除ボリュームに十分な空きスペースがあることを確認する"です。 • "スナップショットの準備"です。 • "SnapLockボリュームの自動コミット期間を時間に設定する"です。 • MetroCluster構成の場合は、を"自動計画外スイッチオーバーを無効にする"参照してください。

リバート元	リバートプロセスを開始する前に実行する処理
ONTAP 9.17.1	• SANのONTAP ARP機能を有効にしている場合は、 "無効にする" 。
ONTAP 9 .16.1	• NVMe / TCP接続用にTLSが設定されている場合は、を"NVMeホストでTLS設定を無効にする"参照してください。 • qtreeの拡張パフォーマンス監視を有効にしている場合は、を"無効にする"参照してください。 • CORSを使用してONTAP s3バケットにアクセスする場合は、を"CORS設定の削除"参照してください。
ONTAP 9 .14.1	クライアント接続のトランキングを有効にしている場合は、を"NFSv4.1サーバでトランキングを無効にする"参照してください。
ONTAP 9 12.1	• NASデータ用のS3クライアントアクセスを設定済みの場合は、"S3 NASバケット設定を削除します。" • NVMeプロトコルを実行し、インバンド認証を設定している場合は、を"インバンド認証を無効にする"参照してください。 • MetroCluster構成の場合は、を"IPSecを無効にする"参照してください。
ONTAP 9.11.1	Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）を設定している場合は、"ARPライセンスの確認"
ONTAP 9.6	SnapMirror同期関係がある場合は、"リバートのために関係を準備する"。

ONTAP 9の任意のバージョン

ONTAPをリバートする前に特定の**SMB**セッションを終了する

ONTAP 9のいずれかのバージョンからONTAPクラスタをリバートする前に、継続的可用性に対応していないSMBセッションを特定して正常に終了する必要があります。

Hyper-VクライアントまたはMicrosoft SQL Serverクライアントが SMB 3.0プロトコルを使用してアクセスする、継続的可用性を備えたSMB共有は、アップグレードまたはダウングレードの前に終了する必要はありません。

手順

1. 継続的可用性に対応していない、確立済みのSMBセッションを特定します。

```
vserver cifs session show -continuously-available No -instance
```

このコマンドは、継続的可用性が確保されていないSMBセッションに関する詳細情報を表示します。ONTAPのダウングレードを開始する前に終了する必要があります。

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                          Node: node1
                       Vserver: vs1
                    Session ID: 1
                 Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
               Connected Time: 8m 39s
                    Idle Time: 7m 45s
            Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. 必要に応じて、特定した各SMBセッションで開いているファイルを確認します。

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare         No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare         No
Path: \file1.txt
2 entries were displayed.
```

SnapMirror関係と**SnapVault**関係の**ONTAP**リバート要件

コマンドは、 `system node revert-to`リバートプロセスを完了するために削除または再設定が必要なSnapMirror関係およびSnapVault関係について通知します。ただし、リバートを開始する前に以下の要件について理解しておく必要があります。

- すべての SnapVault 関係とデータ保護ミラー関係を休止してから解除する必要があります。

  共通のSnapshotが存在する場合は、リバートの完了後にこれらの関係を再同期して再開できます。

- 次のタイプの SnapMirror ポリシーを SnapVault 関係に含めることはできません。
  - 非同期ミラー

    このポリシータイプを使用する関係をすべて削除する必要があります。

  - MirrorAndVault

    このような関係が存在する場合は、 SnapMirror ポリシーを mirror-vault に変更する必要があります。

- すべての負荷共有ミラー関係とデスティネーションボリュームを削除する必要があります。
- FlexClone デスティネーションボリュームとの SnapMirror 関係を削除する必要があります。
- 各 SnapMirror ポリシーでネットワーク圧縮を無効にする必要があります。
- async-mirror タイプの SnapMirror ポリシーから all_source_snapshot ルールを削除する必要があります。

  ルートボリュームでの Single File Snapshot Restore （ SFSR ）処理と Partial File Snapshot Restore （ PFSR ）処理は廃止されました。

- リバートを実行する前に、実行中の単一ファイルおよびSnapshotのリストア処理を完了しておく必要があ

ります。

リストア処理が完了するまで待つか、リストア処理を中止できます。

- 未完了の単一ファイルおよびSnapshotのリストア処理がある場合は、コマンドを使用して削除する必要があります `snapmirror restore`。

  の詳細については `snapmirror restore`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPをリバートする前に重複排除機能が有効なボリュームの空きスペースを確認する

ONTAP 9のいずれかのバージョンからONTAPクラスタをリバートする前に、リバート処理に使用する十分な空きスペースがボリュームにあることを確認する必要があります。

ゼロのブロックのインライン検出によって実現した削減に対応できる十分なスペースがボリュームに必要です。参照"NetAppナレッジベース: ONTAP 9 で重複排除、圧縮、コンパクションによるスペース節約を確認する方法"。

リバートするボリュームで重複排除とデータ圧縮の両方を有効にした場合は、重複排除をリバートする前にデータ圧縮をリバートする必要があります。

手順

1. ボリュームで実行されている効率化処理の進捗状況を表示します。

   ```
   volume efficiency show -fields vserver,volume,progress
   ```

2. アクティブな重複排除処理とキューに登録されている重複排除処理をすべて停止

   ```
   volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
   ```

3. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

4. ボリュームの効率化メタデータをONTAPの目的のバージョンにダウングレードします。

   ```
   volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
   -version <version>
   ```

   次の例は、ボリュームVolAの効率化メタデータをONTAP 9.xにリバートします。

   ```
   volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
   ```

volume efficiency revert-toコマンドは、このコマンドを実行するノードに存在するボリュームをリバートします。ノード間でのボリュームのリバートは行いません。

5. ダウングレードの進捗を監視します。

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. リバートに失敗した場合は、インスタンスを表示して、リバートに失敗した理由を確認します。

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. リバート処理の完了後、admin権限レベルに戻ります。

```
set -privilege admin
```

詳細については、をご覧ください "論理ストレージ管理"。

ONTAPクラスタをリバートする前に**Snapshot**を準備する

ONTAP 9のいずれかのバージョンからONTAPクラスタをリバートする前に、すべてのSnapshotポリシーを無効にし、現在のリリースへのアップグレード後に作成されたSnapshotを削除する必要があります。

SnapMirror 環境でリバートを実行する場合は、次のミラー関係を事前に削除しておく必要があります。

- すべての負荷共有ミラー関係
- ONTAP 8.3.x で作成したすべてのデータ保護ミラー関係
- ONTAP 8.3.x でクラスタが再作成された場合は、すべてのデータ保護ミラー関係

手順

1. すべてのデータSVMのSnapshotポリシーを無効にします。

```
volume snapshot policy modify -vserver * -enabled false
```

2. 各ノードのアグリゲートのSnapshotポリシーを無効にします。
   a. ノードのアグリゲートを特定します。

```
run -node <nodename> -command aggr status
```

b. 各アグリゲートのSnapshotポリシーを無効にします。

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

c. 残りのノードそれぞれに対して同じ手順を繰り返します。

3. 各ノードのルートボリュームのSnapshotポリシーを無効にします。

a. ノードのルートボリュームを特定します。

```
run -node <node_name> -command vol status
```

ルートボリュームは、コマンド出力の* Options *列にrootとして表記されます `vol status`。

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

a. ルートボリュームのSnapshotポリシーを無効にします。

```
run -node <node_name> vol options root_volume_name nosnap on
```

b. 残りのノードそれぞれに対して同じ手順を繰り返します。

4. 現在のリリースへのアップグレード後に作成されたSnapshotをすべて削除します。

a. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

b. Snapshotを無効にします。

```
snapshot policy modify -vserver * -enabled false
```

c. ノードの新しいバージョンのSnapshotを削除します。

```
volume snapshot prepare-for-revert -node <node_name>
```

このコマンドは、各データボリューム、ルートアグリゲート、およびルートボリューム上の新しいバ

ージョンのSnapshotを削除します。

削除できないSnapshotがあると、コマンドは失敗し、Snapshotを削除する前に実行する必要があるアクションがあれば通知されます。必要な操作を完了してからコマンドを再実行してから、次の手順に進む必要があります `volume snapshot prepare-for-revert`。

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all snapshots that have the format
used by the current version of ONTAP. It will fail if any snapshot
policies are enabled, or
         if any snapshots have an owner. Continue? {y|n}: y
```

a. Snapshotが削除されたことを確認します。

```
volume snapshot show -node nodename
```

b. 新しいバージョンのSnapshotが残っている場合は、強制的に削除します。

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
-constituent true} -ignore-owners -force
```

c. 残りのノードごとに上記の手順を繰り返します。

d. admin権限レベルに戻ります。

```
set -privilege admin
```

これらの手順を MetroCluster 構成内の両方のクラスタで実行する必要があります。

ONTAPをリバートする前の**SnapLock**ボリュームの自動コミット期間の設定

ONTAPクラスタをONTAP 9のいずれかのバージョンからリバートする場合は、事前にSnapLockボリュームの自動コミット期間の値を日数ではなく時間数で設定する必要があります。SnapLockボリュームの自動コミット値を確認し、必要に応じて日数を時間数に変更します。

手順

1. クラスタ内にサポートされない自動コミット期間が設定されているSnapLock があることを確認します。

```
volume snaplock show -autocommit-period *days
```

2. サポートされない自動コミット期間を時間に変更します。

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

MetroCluster構成を元に戻す前に、計画外の自動スイッチオーバーを無効にする

ONTAP 9 のいずれかのバージョンを実行しているMetroCluster構成を元に戻す前に、自動計画外スイッチオーバー (AUSO) を無効にする必要があります。

ステップ

1. MetroCluster の両方のクラスタで、自動計画外スイッチオーバーを無効にします。

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

関連情報

"MetroClusterの管理とディザスタリカバリ"

ONTAP 9.17.1

ONTAP 9.17.1 から戻す前に、**SAN** ボリュームの自律ランサムウェア保護を無効にします。

SANボリュームのONTAP ARP機能は、 ONTAP 9.16.1以前ではサポートされていません。ONTAPONTAP以前にリバートする前に、SANボリュームのARPを無効にすることをお勧めします。そうすることで、リバート後のバージョンで実際の検出処理を行わずに機能がアクティブなままになり、CPUとディスクリソースを消費してしまう事態を防ぐことができます。

例 **7.** 手順

System Manager

1. ストレージ **>** ボリューム を選択し、ボリュームの名前を選択します。
2. ボリューム 概要の セキュリティ タブで、ステータス を選択して、有効から無効に切り替えます。

CLI

1. ボリューム上のランサムウェア保護を無効にします。

```
security anti-ransomware volume disable -volume <vol_name> -vserver
<svm_name>
```

ONTAP 9 .16.1

ONTAP 9.16.1からリバートする前にNVMeホストでTLSを無効にする

NVMeホストでNVMe/TCP接続用のTLSセキュアチャネルが設定されている場合は、ONTAP 9.16.1からクラスタをリバートする前にそのチャネルを無効にする必要があります。

手順

1. ホストからTLSセキュアチャネル設定を削除します。

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

このコマンドはサブシステムからホストを削除し、TLS設定を使用せずにサブシステムにホストを再作成します。

2. TLSセキュアチャネルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

ONTAP 9.16.1からリバートする前に拡張qtreeパフォーマンス監視を無効にする

ONTAP 9 .16.1以降では、ONTAP REST APIを使用して、レイテンシ指標や履歴統計などの拡張されたqtree監視機能にアクセスできます。いずれかのqtreeで拡張qtree監視が有効になっている場合は、9.16.1からリバートする前に、falseに設定する必要があります `ext_performance_monitoring.enabled`。

詳細については、をご覧ください "qtreeのパフォーマンス監視機能が強化されたクラスタのリバート"。

ONTAP 9.16.1からリバートする前にCORS設定を削除する

Cross-Origin Resource Sharing（CORS）を使用してONTAP S3バケットにアクセスしている場合は、ONTAP 9.16.1からリバートする前にバケットを削除する必要があります。

詳細については、をご覧ください "CORSヲシヨウシタONTAPクラスタノリハアト"。

ONTAP 9 .14.1

ONTAP 9.14.1からリバートする前にNFSv4.1セッショントランキングを無効にする

クライアント接続のトランキングを有効にしている場合は、ONTAP 9.14.1からリバートする前に、NFSv4.1サーバでトランキングを無効にする必要があります。

コマンドを入力すると、 `revert-to`続行する前にトランキングを無効にするように求める警告メッセージが表示されます。

ONTAP 9.13.1にリバートすると、トランク接続を使用するクライアントは、単一の接続を使用するようにフォールバックされます。データのスループットには影響しますが、システム停止は発生しません。リバートの動作は、SVMのNFSv4.1トランキングオプションをenabledからdisabledに変更した場合と同じです。

手順

1. NFSv4.1サーバでトランキングを無効にします。

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. NFSが必要に応じて設定されていることを確認します。

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9 12.1

ONTAP 9.12.1からリバートする前にS3 NASバケット設定を削除する

NASデータ用のS3クライアントアクセスを設定している場合は、ONTAP 9.12.1からリバートする前に、ONTAPコマンドラインインターフェイス（CLI）を使用してNASバケット設定を削除し、ネームマッピング（S3ユーザからWindowsユーザまたはUNIXユーザ）を削除する必要があります。

タスクの内容

リバートプロセスでは、次のタスクがバックグラウンドで実行されます。

- 部分的に完了したシングルトンオブジェクトの作成（非表示ディレクトリ内のすべてのエントリ）をすべて削除します。
- 非表示のディレクトリをすべて削除します。S3 NASバケットからマッピングされたエクスポートのルートからアクセス可能なボリュームごとに、1つずつがになっている可能性があります。
- アップロードテーブルを削除します。
- 設定されているすべてのS3サーバのdefault-unix-userとdefault-windows-userの値を削除します。

手順

1. S3 NASバケット設定を削除します。

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket
<s3_nas_bucket_name>
```

の詳細については `vserver object-store-server bucket delete`、を"ONTAPコマンド リファレンス"参照してください。

2. UNIXのネームマッピングを削除します。

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

の詳細については `vserver name-mapping delete`、を"ONTAPコマンド リファレンス"参照してください。

3. Windowsのネームマッピングを削除します。

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. SVMからS3プロトコルを削除します。

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

の詳細については `vserver remove-protocols`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 9.12.1からリバートする前に**NVMe**インバンド認証を無効にする

NVMeプロトコルを実行している場合は、ONTAP 9.12.1からクラスタをリバートする前に、インバンド認証を無効にする必要があります。DH-HMAC-CHAPを使用するインバンド認証が無効になっていない場合、リバートは失敗します。

手順

1. ホストをサブシステムから削除してDH-HMAC-CHAP認証を無効にします。

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. DH-HMAC-CHAP認証プロトコルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

3. 認証を使用せずにホストをサブシステムに再度追加します。

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

ONTAP 9.12.1からリバートする前に**MetroCluster**設定で**IPSec**を無効にする

ONTAP 9.12.1からMetroCluster設定をリバートする前に、IPsecをディセーブルにする必

要があります。

リバート前にチェックが実行され、MetroCluster設定内にIPSec設定がないことが確認されます。リバートを続行する前に、IPsec設定をすべて削除し、IPsecを無効にする必要があります。IPsecが有効になっている場合、ユーザポリシーが設定されていなくても、ONTAPのリバートはブロックされます。

ONTAP 9 .11.1

ONTAP 9.11.1からリバートする前に**Autonomous Ransomware Protection**のライセンスを確認する

Autonomous Ransomware Protection（ARP）を設定している場合に、ONTAP 9.11.1からONTAP 9.10.1にリバートすると、警告メッセージが表示され、ARP機能が制限されることがあります。

ONTAP 9 .11.1では、マルチテナントキー管理（MTKM）ライセンスに代わってAnti-Ransomwareライセンスが使用されました。システムにAnti_ransomwareライセンスがあり、MT_EK_MGMTライセンスがない場合は、リバート中に、リバート時に新しいボリュームでARPを有効にできないという警告が表示されます。

既存の保護を使用するボリュームはリバート後も正常に機能し、ONTAP CLIを使用してARPステータスを表示できます。System Managerでは、MTKMライセンスがないとARPステータスを表示できません。

したがって、ONTAP 9 .10.1にリバートしたあともARPを続行する場合は、リバート前にMTKMライセンスがインストールされていることを確認してください。"ARPライセンスについて説明します。"

ONTAP 9.6

SnapMirror同期関係を使用する**ONTAP 9.6**からシステムをリバートする場合の考慮事項

ONTAP 9 .6からONTAP 9にリバートする前に、SnapMirror同期関係に関する考慮事項を確認しておく必要があります。5。

SnapMirror同期関係がある場合は、リバート前に次の手順を実行する必要があります。

- ソースボリュームがNFSv4またはSMBを使用してデータを提供しているSnapMirror同期関係を削除する必要があります。

  ONTAP 9 .5はNFSv4とSMBをサポートしていません。

- ミラー-ミラーカスケード構成のSnapMirror同期関係を削除する必要があります。

  ミラー-ミラーカスケード構成は、ONTAP 9のSnapMirror同期関係ではサポートされません。5.

- リバート時にONTAP 9.5の共通のSnapshotを使用できない場合は、リバート後にSnapMirror同期関係を初期化する必要があります。

  2時間後にONTAP 9.6にアップグレードすると、ONTAP 9.5の共通のSnapshotがONTAP 9.6の共通のSnapshotに自動的に置き換えられます。そのため、ONTAP 9.5の共通のSnapshotを使用できない場合、リバート後にSnapMirror同期関係を再同期することはできません。

ONTAPソフトウェアイメージのダウンロードとインストール

現在のONTAPソフトウェアをリバートする前に、対象のソフトウェアバージョンをNetAppサポートサイトからダウンロードしてインストールする必要があります。

ONTAPソフトウェアイメージのダウンロード

ソフトウェアイメージはプラットフォームモデルに固有です。ご使用のクラスタに適したイメージを取得する必要があります。ソフトウェアイメージ、ファームウェアのバージョン情報、プラットフォームモデルの最新のファームウェアは、NetAppサポートサイトで入手できます。ソフトウェアイメージには、特定のバージョンのONTAPのリリース時に使用可能だったシステムファームウェアの最新バージョンが含まれています。

NetAppボリューム暗号化を使用するシステムをONTAP 9.5以降からリバートする場合は、規制対象外の国用の（NetAppボリューム暗号化を含む）ONTAPソフトウェアイメージをダウンロードする必要があります。制限された国のONTAPソフトウェアイメージを使用してNetAppボリューム暗号化が有効なシステムをリバートすると、システムがパニック状態になり、ボリュームにアクセスできなくなります。

手順

1. "ソフトウェアのダウンロード"NetAppサポートサイトの領域で、対象のONTAPソフトウェアを探します。
2. ソフトウェアイメージをコピーします（例： `97_q_image.tgz` ） NetAppサポートサイトから

   イメージは、イメージの提供元となるHTTPサーバまたはFTPサーバ上のディレクトリ、またはローカルフォルダにコピーできます。

ONTAPソフトウェアイメージのインストール

NetAppサポートサイトからターゲットのONTAPソフトウェアイメージをダウンロードしたら、クラスタノードにインストールします。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

   advancedプロンプト(`*>`が表示されます）。

2. プロンプトが表示されたらと入力し `y`て続行します
3. ソフトウェアイメージをインストールします。
   - 標準構成または2ノードMetroCluster構成の場合は、次のコマンドを入力します。

     ```
     system node image update -node * -package
     <http://example.com/downloads/image.tgz> -replace-package true
     -replace {image1|image2} -background true -setdefault true
     ```

このコマンドは、ソフトウェアイメージをすべてのノードに同時にダウンロードしてインストールします。一度に1つずつ各ノードにイメージをダウンロードしてインストールする場合は、パラメータを指定しない `-background`でください。また、このコマンドでは、拡張クエリを使用して、代替イメージとしてインストールされるターゲットのソフトウェアイメージがノードのデフォルトのイメージになるように変更します。

- 4ノードまたは8ノードのMetroCluster構成の場合は、両方のクラスタで次のコマンドを入力します。

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault false
```

このコマンドは、ソフトウェアイメージをすべてのノードに同時にダウンロードしてインストールします。一度に1つずつ各ノードにイメージをダウンロードしてインストールする場合は、パラメータを指定しない `-background`でください。また、このコマンドでは、拡張クエリを使用して、代替イメージとして各ノードにインストールされるターゲットのソフトウェアイメージを変更します。

4. プロンプトが表示されたらと入力し `y`て続行します
5. ソフトウェアイメージが各ノードにダウンロードおよびインストールされたことを確認します。

```
system node image show-update-progress -node *
```

このコマンドは、ソフトウェアイメージのダウンロードとインストールの現在のステータスを表示します。すべてのノードの*実行ステータス*が「終了」、*終了ステータス*が「成功」と表示されるまで、このコマンドを実行し続けてください。

system node image updateコマンドが失敗し、エラーまたは警告メッセージが表示されることがあります。エラーや警告を解決したら、コマンドを再度実行できます。

次の例では、2ノードクラスタの両方のノードでソフトウェアイメージのダウンロードとインストールが正常に完了しています。

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

関連情報

- "システムノードイメージの更新"

ONTAPクラスタをリバートします。

ONTAPクラスタをリバートするとシステムが停止します。リバート中はクラスタをオフラインにする必要があります。テクニカルサポートの支援なしで本番環境クラスタをリバートしないでください。

新しいクラスタまたはテストクラスタをリバートするには、ストレージフェイルオーバーとデータLIFを無効にし、リバートの前提条件を指定してから、クラスタ内の各ノードでクラスタとファイルシステムの設定をリバートする必要があります。

始める前に。

- の作業を完了しておく必要があります"リバート前の検証"。
- 必要なの手順を完了しておく必要があります"特定のONTAPバージョンの事前チェック"。
- あなたは持っているべきだった"対象のONTAPソフトウェアイメージをダウンロードしてインストールしました" 。

手順1：クラスタをリバート用に準備する

クラスタノードをリバートする前に、ターゲットのONTAPイメージがインストールされていることを確認し、クラスタ内のすべてのデータLIFを無効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

続行するかどうかを尋ねられたら、「* y *」と入力します。

2. ターゲットのONTAP ソフトウェアがインストールされていることを確認します。

```
system image show
```

次の例では、両方のノードに代替イメージとしてバージョン9.13.1がインストールされています。

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

3. クラスタ内のすべてのデータLIFを無効にします。

```
network interface modify {-role data} -status-admin down
```

4. クラスタ間FlexCache 関係があるかどうかを確認します。

```
flexcache origin show-caches -relationship-type inter-cluster
```

5. クラスタ間フラッシュが存在する場合は、キャッシュクラスタのデータLIFを無効にします。

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

手順**2**：クラスタノードをリバートする

クラスタをリバートするには、HAペアの最初のノードをリバートしてから、パートナーノードをリバートする必要があります。その後、すべてのノードがリバートされるまで、クラスタ内のHAペアごとにこの手順を繰り返します。MetroCluster構成を使用している場合は、構成内の両方のクラスタで上記の手順を繰り返す必

要があります。

4ノード以上

手順

1. リバートするノードにログインします。

   ノードをリバートするには、ノードのノード管理LIFを介してクラスタにログインする必要があります。

2. HAペアのノードのストレージフェイルオーバーを無効にします。

   ```
   storage failover modify -node <nodename> -enabled false
   ```

   ストレージフェイルオーバーを無効にする必要があるのは、HAペアに対して1回だけです。ノードのストレージフェイルオーバーを無効にすると、ノードのパートナーでもストレージフェイルオーバーが無効になります。

3. ノードのターゲットONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。

   ```
   system image modify -node <nodename> -image <target_image>
   -isdefault true
   ```

4. ターゲットのONTAP ソフトウェアイメージが、リバートするノードのデフォルトのイメージとして設定されたことを確認します。

   ```
   system image show
   ```

   次の例では、node0でデフォルトのイメージとしてバージョン9.13.1が設定されています。

   ```
   cluster1::*> system image show
                    Is      Is                  Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- --------    -------------------
   node0
            image1  false   true    9.14.1       MM/DD/YYYY TIME
            image2  true    false   9.13.1       MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1       MM/DD/YYYY TIME
            image2  false   false   9.13.1       MM/DD/YYYY TIME
   4 entries were displayed.
   ```

5. ノードをリバートする準備が完了していることを確認します。

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

パラメータは、 `check-only`Snapshotポリシーの無効化や新しいバージョンのONTAPへのアップグレード後に作成されたSnapshotの削除など、リバート前に対処する必要がある前提条件を示します。

オプションは、 `-version`リバート先のONTAPリリースを指定します。たとえば、9.14.1から9.13.1にリバートする場合、オプションの正しい値 `-version`は9.13.1です。

6. ノードのクラスタ構成をリバートします。

```
system node revert-to -node <nodename> -version 9.x
```

クラスタ設定がリバートされ、クラスタシェルからログアウトされます。

7. ログインプロンプトが表示されたら、システムシェルにログインするかどうかを確認するメッセージが表示されたら、「* No *」と入力します。

ログインプロンプトが表示されるまで、30分以上かかることがあります。

8. adminでクラスタシェルにログインします。
9. ノードシェルに切り替えます。

```
run -node <nodename>
```

クラスタシェルに再度ログインしたあと、ノードシェルコマンドを使用できるようになるまでに数分かかることがあります。そのため、コマンドが失敗した場合は、数分待ってからもう一度実行してください。

10. ノードのファイルシステム設定をリバートします。

```
revert_to 9.x
```

このコマンドは、ノードのファイルシステム設定をリバートする準備が完了していることを確認してから、リバートします。前提条件が特定された場合は、それらに対処してからコマンドを再実行する必要があります `revert_to`。

> システムコンソールを使用してリバートプロセスを監視すると、ノードシェルよりも詳細な情報が表示されます。

autobootがtrueの場合、コマンドの完了時にノードがONTAPでリブートされます。

autobootがfalseに設定されている場合は、コマンドの完了時にLoaderプロンプトが表示されます。と入力し `yes`てリバートし、を使用してノードを手動でリブートします。 `boot_ontap`

11. ノードがリブートしたら、新しいソフトウェアが実行されていることを確認します。

```
system node image show
```

次の例では、image1が新しいONTAPバージョンで、node0で現在のバージョンとして設定されています。

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

12. ノードのリバートステータスがcompleteであることを確認します。

```
system node upgrade-revert show -node <nodename>
```

ステータスが「complete」、「not needed」、または「There are no table entries returned」のいずれかになっている必要があります。

13. HAペアのもう一方のノードで上記の手順を繰り返してから、残りのHAペアについても同じ手順を繰り返します。

MetroCluster構成を使用している場合は、構成内の両方のクラスタで上記の手順を繰り返す必要があります。

14. すべてのノードをリバートしたら、クラスタのハイアベイラビリティを再度有効にします。

```
storage failover modify -node* -enabled true
```

2ノードクラスタ

1. リバートするノードにログインします。

ノードをリバートするには、ノードのノード管理LIFを介してクラスタにログインする必要があります。

2. クラスタのハイアベイラビリティ（HA）を無効にします。

```
cluster ha modify -configured false
```

3. ストレージフェイルオーバーを無効にします。

```
storage failover modify -node <nodename> -enabled false
```

ストレージフェイルオーバーを無効にする必要があるのは、HAペアに対して1回だけです。ノードのストレージフェイルオーバーを無効にすると、ノードのパートナーでもストレージフェイルオーバーが無効になります。

4. ノードのターゲットONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify -node <nodename> -image <target_image>
-isdefault true
```

5. ターゲットのONTAP ソフトウェアイメージが、リバートするノードのデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、node0でデフォルトのイメージとしてバージョン9.13.1が設定されています。

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   false   true    9.14.1       MM/DD/YYYY TIME
         image2   true    false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

6. ノードにイプシロンが現在設定されているかどうかを確認します。

```
cluster show -node <nodename>
```

次の例は、ノードにイプシロンが設定されていることを示しています。

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

a. ノードにイプシロンが設定されている場合は、イプシロンをパートナーに転送できるように、イプシロンをfalseに設定します。

```
cluster modify -node <nodename> -epsilon false
```

b. パートナーノードでイプシロンをtrueに設定して、イプシロンをパートナーに転送します。

```
cluster modify -node <node_partner_name> -epsilon true
```

7. ノードをリバートする準備が完了していることを確認します。

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

パラメータは、 `check-only`Snapshotポリシーの無効化、新しいバージョンのONTAPへのアップグレード後に作成されたSnapshotの削除など、リバート前に対処する必要がある条件を示します。

その `-version`オプションは、戻す先のONTAPリリースを指します。例えば、9.14から9.13に戻す場合、 `-version`オプションは9.13です。

クラスタ設定がリバートされ、クラスタシェルからログアウトされます。

8. ノードのクラスタ構成をリバートします。

```
system node revert-to -node <nodename> -version 9.x
```

9. ログインプロンプトが表示されたら、システムシェルにログインするかどうかを確認するメッセージが表示されたらと入力します `No`。

ログインプロンプトが表示されるまで、30分以上かかることがあります。

10. adminでクラスタシェルにログインします。
11. ノードシェルに切り替えます。

```
run -node <nodename>
```

クラスタシェルに再度ログインしたあと、ノードシェルコマンドを使用できるようになるまでに数分かかることがあります。そのため、コマンドが失敗した場合は、数分待ってからもう一度実行してください。

12. ノードのファイルシステム設定をリバートします。

```
revert_to 9.x
```

このコマンドは、ノードのファイルシステム設定をリバートする準備が完了していることを確認してから、リバートします。前提条件が特定された場合は、それらに対処してからコマンドを再実行する必要があります `revert_to`。

システムコンソールを使用してリバートプロセスを監視すると、ノードシェルよりも詳細な情報が表示されます。

autobootがtrueの場合、コマンドの完了時にノードがONTAPでリブートされます。

autobootがfalseに設定されている場合は、コマンドの完了時にLoaderプロンプトが表示されます。と入力し `yes`てリバートし、を使用してノードを手動でリブートします。 `boot_ontap`

13. ノードがリブートしたら、新しいソフトウェアが実行されていることを確認します。

```
system node image show
```

次の例では、image1が新しいONTAPバージョンで、node0で現在のバージョンとして設定されています。

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

14. ノードのリバートステータスが完了になっていることを確認します。

```
system node upgrade-revert show -node <nodename>
```

ステータスが「complete」、「not needed」、または「There are no table entries returned」のいずれかになっている必要があります。

15. HAペアのもう一方のノードで、上記の手順を繰り返します。
16. 両方のノードをリバートしたら、クラスタのハイアベイラビリティを再度有効にします。

```
cluster ha modify -configured true
```

17. 両方のノードでストレージフェイルオーバーを再度有効にします。

```
storage failover modify -node <nodename> -enabled true
```

関連情報

- "storage failover modify"

ONTAPリバート後の処理

ONTAPリバート後のクラスタとストレージの健全性の確認

ONTAPクラスタをリバートしたら、ノードが正常に機能していてクラスタに追加するための条件を満たしていること、およびクラスタがクォーラムにあることを確認する必要があります。また、ディスク、アグリゲート、およびボリュームのステータスも確認する必要があります。

クラスタの健全性を確認

手順

1. クラスタ内のノードがオンラインであり、クラスタに参加するための条件を満たしていることを確認します。

```
cluster show
```

この例では、クラスタは正常に機能しており、すべてのノードがクラスタに参加する資格を持っています。

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

正常でないノードや条件を満たしていないノードがある場合は、EMSログでエラーを確認して対処します。

2. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

と入力し `y`て続行します。

3. 各RDBプロセスの設定の詳細を確認します。

   - リレーショナルデータベースのエポックとデータベースのエポックは、各ノードで一致している必要があります。
   - リングごとのクォーラムマスターがすべてのノードで同じである必要があります。

     各リングのクォーラムマスターが異なる場合があることに注意してください。

表示する **RDB** プロセス	入力するコマンド
管理アプリケーション	`cluster ring show -unitname mgmt`
ボリューム ロケーション データベース	`cluster ring show -unitname vldb`
仮想インターフェイス マネージャ	`cluster ring show -unitname vifmgr`
SAN管理デーモン	`cluster ring show -unitname bcomd`

次の例は、ボリューム ロケーション データベースのプロセスを示しています。

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

5. SAN環境を使用している場合は、各ノードがSANクォーラムにあることを確認します。

```
event log show  -severity informational -message-name scsiblade.*
```

各ノードの最新のscsibladeイベントメッセージに、SCSIブレードがクォーラムにあることが示されます。

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

関連情報

"システム管理"

ストレージの健全性を確認

クラスタをリバートまたはダウングレードしたら、ディスク、アグリゲート、およびボリュームのステータスを確認する必要があります。

手順

1. ディスクのステータスを確認します。

確認する項目	操作
破損ディスク	a. 破損ディスクを表示します。 `storage disk show -state broken` b. 破損ディスクを取り外すか交換します。
メンテナンス中または再構築中のディスク	a. メンテナンス、保留、または再構築中の状態のディスクを表示します。 `storage disk show -state maintenance`
pending	reconstructing ---- .. メンテナンスまたは再構築の処理が完了するまで待ってから次に進みます。

2. 物理ストレージと論理ストレージ（ストレージのアグリゲートを含む）の状態を表示して、すべてのアグリゲートがオンラインであることを確認します。

```
storage aggregate show -state !online
```

このコマンドを実行すると、オンラインでないアグリゲートが表示されます。メジャーアップグレードまたはリバートの実行前と実行後に、すべてのアグリゲートがオンラインになっている必要があります。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. 次のコマンドを実行して、すべてのボリュームがオンラインであることを確認します。 _not_online

```
volume show -state !online
```

メジャーアップグレードまたはリバートの実行前と実行後に、すべてのボリュームがオンラインになっている必要があります。

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 整合性のないボリュームがないことを確認します。

```
volume show -is-inconsistent true
```

参照"NetAppナレッジベース: ボリュームにWAFLの不整合が表示される"不一致なボリュームに対処する方法について。

クライアントアクセスの確認（**SMB**と**NFS**）

設定されているプロトコルについて、SMBクライアントとNFSクライアントからのアクセスをテストして、クラスタにアクセスできることを確認します。

関連情報

- "ディスクおよびアグリゲートの管理"
- "storage disk show"

ONTAPリバート後に**MetroCluster**構成の自動スイッチオーバーを有効にする

ONTAP MetroCluster構成をリバートしたら、自動計画外スイッチオーバーを有効にして、MetroCluster構成が完全に動作するようにする必要があります。

手順

1. 自動計画外スイッチオーバーを有効にします。

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

2. MetroCluster 構成を検証します。

```
metrocluster check run
```

ONTAPのリバート後に**LIF**を有効にしてホームポートにリバートする

リブート時に、割り当てられているフェイルオーバーポートに一部のLIFが移行されることがあります。ONTAPクラスタをリバートしたあと、ホームポートにないLIFを有効にしてリバートする必要があります。

network interface revertコマンドを実行すると、ホームポートにないLIFがホームポートにリバートされます（ホームポートが稼働している場合）。LIFのホームポートはLIFの作成時に指定します。指定されているホームポートは、network interface showコマンドを使用して確認できます。

手順

1. すべてのLIFのステータスを表示します。

```
network interface show
```

Storage Virtual Machine（SVM）のすべてのLIFのステータスを表示する例を次に示します。

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

Status AdminステータスがdownになっているLIFやIs homeステータスがfalseになっているLIFがある場合は、次の手順に進みます。

2. データLIFを有効にします。

```
network interface modify {-role data} -status-admin up
```

3. LIFをそれぞれのホームポートにリバートします。

```
network interface revert *
```

4. すべてのLIFがそれぞれのホームポートにあることを確認します。

```
network interface show
```

次の例では、SVM vs0のすべてのLIFがそれぞれのホームポートにあります。

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0          e0e
true
            data002      up/up    192.0.2.121/24     node0          e0f
true
            data003      up/up    192.0.2.122/24     node0          e2a
true
            data004      up/up    192.0.2.123/24     node0          e2b
true
            data005      up/up    192.0.2.124/24     node1          e0e
true
            data006      up/up    192.0.2.125/24     node1          e0f
true
            data007      up/up    192.0.2.126/24     node1          e2a
true
            data008      up/up    192.0.2.127/24     node1          e2b
true
8 entries were displayed.
```

関連情報

- "ネットワークインターフェイス"

ONTAPのリバート後に**Snapshot**ポリシーを有効にする

以前のバージョンのONTAPにリバートした場合、Snapshotの作成を再開するには、Snapshotポリシーを有効にする必要があります。

以前のバージョンのONTAPにリバートする前に無効にしたSnapshotスケジュールを再度有効にします。

手順

1. すべてのデータSVMのSnapshotポリシーを有効にします。

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. 各ノードについて、ルートボリュームのSnapshotポリシーを有効にします。

```
run -node <node_name> vol options <volume_name> nosnap off
```

ONTAPリバート後の**IPv6**ファイアウォールエントリの確認

ONTAP 9 のいずれかのバージョンからのリバートを実行すると、ファイアウォールポリシーの一部のサービスのデフォルトの IPv6 ファイアウォールエントリが失われる可能性があります。必要なファイアウォールエントリがシステムにリストアされていることを確認する必要があります。

手順

1. すべてのファイアウォールポリシーをデフォルトのポリシーと比較して、正しいことを確認します。

```
system services firewall policy show
```

次の例は、デフォルトのポリシーを示しています。

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. 新しいファイアウォールポリシーを作成して、不足しているデフォルトのIPv6ファイアウォールエントリを手動で追加します。

```
system services firewall policy create -policy <policy_name> -service
ssh -action allow -ip-list <ip_list>
```

3. 新しいポリシーをLIFに適用してネットワークサービスへのアクセスを許可します。

```
network interface modify -vserve <svm_name> -lif <lif_name> -firewall
-policy <policy_name>
```

ONTAP 9.8へのリバート後にサービスプロセッサにアクセスできるユーザアカウントを確認する

ONTAP 9.9.1以降では `-role`、ユーザアカウントのパラメータがに変更されまし `admin`た。ONTAP 9.8以前でユーザアカウントを作成したあとにONTAP 9.9.1以降にアップグレードしてONTAP 9.8にリバートした場合、 `-role`パラメータは元の値にリストアされます。変更した値が許容可能であることを確認する必要があります。

リバート時にSPユーザのロールが削除されると、「rbac.spuser.role.notfound" EMSメッセージが記録されま

す。

詳細については、を参照してください "SPにアクセスできるアカウント"。

クラスタの管理

System Managerでのクラスタ管理

ONTAP System Managerを使用したクラスタ管理について学習します

System Managerは、HTML5ベースのグラフィカルな管理インターフェイスで、ストレージシステムとストレージオブジェクト（ディスク、ボリューム、ストレージ階層など）の管理やストレージシステムに関連する一般的な管理タスクの実行にWebブラウザを使用できます。

- System ManagerはWebサービスとしてONTAPソフトウェアに搭載されており、デフォルトで有効になっていて、ブラウザからアクセスできます。
- ONTAP 9では、System Managerの名前が変更されています。6.ONTAP 9 .5以前ではOnCommand System Managerと呼ばれていた。ONTAP 9 .6以降では、System Managerと呼ばれています。
- 従来のSystem Manager（ONTAP 9.7以前でのみ使用可能）を使用している場合は、"System Managerクラシック（ONTAP 9 .0 ~ 9.7）"

System Managerのダッシュボードでは、重要なアラートと通知、ストレージ階層とボリュームの効率性と容量、クラスタで使用可能なノード、HAペアを構成するノードのステータス、最もアクティブなアプリケーションとオブジェクト、クラスタやノードのパフォーマンス指標に関する情報を一目で確認できます。

ONTAP 9.7以降のSystem Managerでは、次のような多くの一般的なタスクを実行できます。

- クラスタを作成し、ネットワークを設定し、クラスタのサポート情報を設定します。
- ディスク、ローカル階層、ボリューム、qtree、クォータなどのストレージオブジェクトを設定および管理します。
- SMBやNFSなどのプロトコルを設定し、ファイル共有をプロビジョニングする。
- FC、FCoE、NVMe、iSCSIなどのプロトコルをブロックアクセス用に設定する。
- サブネット、ブロードキャストドメイン、データインターフェイスと管理インターフェイス、インターフェイスグループなどのネットワークコンポーネントを作成および設定します。
- ミラー関係とバックアップ関係をセットアップおよび管理する。
- クラスタ管理、ストレージノード管理、およびStorage Virtual Machine（Storage VM）管理の処理を実行する。
- Storage VMの作成と設定、Storage VMに関連付けられたストレージオブジェクトの管理、およびStorage VMサービスの管理を行う。
- クラスタのハイアベイラビリティ（HA）構成を監視および管理します。
- サービスプロセッサを設定して、ノードの状態に関係なく、ノードへのログイン、管理、監視、および管理を行う。

System Managerの用語

ONTAPキーの一部の機能については、System Managerで使用される用語がCLIとは異なります。

- ローカル階層：データを格納する一連の物理ソリッドステートドライブまたはハードディスクドライブ。アグリゲートと呼ばれることもあります。ONTAP CLIでは、ローカル階層を表すために_aggregate_usedという用語が引き続き使用されます。
- クラウド階層：いくつかの理由で一部のデータをオフプレミスに配置する場合に、ONTAPで使用されるクラウド内のストレージ。FabricPoolのクラウド部分について考えている場合は、すでに理解しています。また、StorageGRIDシステムを使用している場合は、クラウドがオフプレミスであるとは限りません。（オンプレミスでのクラウドレベルのエクスペリエンスは、 *private_cloud* と呼ばれています）。
- * Storage VM *：クライアントにストレージとデータサービスを提供する、ONTAP内で実行される仮想マシン。これは「*SVM*」や「*Vserver*」と呼ばれます。
- ネットワーク インターフェイス: 物理ネットワーク ポートに割り当てられたアドレスとプロパティ。以前は「論理インターフェイス（*LIF*）」と呼んでいました。
- 一時停止：処理を停止するアクション。ONTAP9.8より前のバージョンのSystem Managerでは、「休止」と呼んでいた可能ONTAPがあります。

System Managerを使用してONTAPクラスタにアクセスする

コマンドラインインターフェイス（CLI）ではなくグラフィカルインターフェイスを使用してクラスタにアクセスして管理するには、System Managerを使用します。System ManagerはONTAPに搭載されているWebサービスでデフォルトで有効になっており、ブラウザを使用してアクセスできます。

> ONTAP 9.12.1 以降、System Manager はNetAppコンソールと完全に統合されています。
>
> コンソールを使用すると、使い慣れたシステム マネージャー ダッシュボードを維持しながら、単一のコントロール プレーンからハイブリッド マルチクラウド インフラストラクチャを管理できます。
>
> 見る"System Manager とNetAppコンソールの統合" 。

タスクの内容

System Managerには、クラスタ管理ネットワークインターフェイス（LIF）またはノード管理ネットワークインターフェイス（LIF）を使用してアクセスできます。System Managerに無停止でアクセスするには、クラスタ管理ネットワークインターフェイス（LIF）を使用する必要があります。

開始する前に

- 「admin」ロールと「http」アプリケーションタイプおよび「console」アプリケーションタイプで構成されたクラスタユーザアカウントが必要です。
- ブラウザでクッキーとサイトのデータを有効にしておく必要があります。

手順

1. Webブラウザで、クラスタ管理ネットワークインターフェイスのIPアドレスを指定します。
    - IPv4を使用する場合： **`https://cluster-mgmt-LIF`**

◦ IPv6を使用する場合： **`https://[cluster-mgmt-LIF]`**

System Managerのブラウザアクセスでサポートされるのはhttpsのみです。

自己署名デジタル証明書がクラスタで使用されている場合、信頼されていない証明書であることを示す警告がブラウザに表示されることがあります。リスクを承認してアクセスを続行するか、認証局（CA）の署名があるデジタル証明書をクラスタにインストールしてサーバを認証します。

2. * オプション： * CLI を使用してアクセスバナーを設定している場合は、 * 警告 * ダイアログボックスに表示されるメッセージを読み、必要なオプションを選択して続行します。

   このオプションは、Security Assertion Markup Language（SAML）認証が有効になっているシステムではサポートされません。

   ◦ 続行しない場合は、 * Cancel * をクリックしてブラウザを閉じます。

   ◦ 続行する場合は、 * OK * をクリックして System Manager のログインページに移動します。

3. クラスタ管理者のクレデンシャルを使用してSystem Managerにログインします。

   ONTAP 9.11.1以降では、System Managerにログインするときにロケールを指定できます。ロケールは、言語、通貨、時刻と日付の形式など、特定のローカライズ設定を指定します。ONTAP 9.10.1以前では、System Managerのロケールはブラウザから検出されます。System Managerのロケールを変更するには、ブラウザのロケールを変更する必要があります。

4. オプション: ONTAP 9.12.1以降では、System Managerの外観を指定できます。

   a. System Managerの右上にあるをクリックし てユーザオプションを管理します。

   b. 「システムテーマ」トグルスイッチを希望の位置に合わせます。

位置を切り替えます	外観の設定
（左）	ライトテーマ（ダークテキストの背景）
OS（中央）	デフォルトでは、オペレーティングシステムのアプリケーションに設定されたテーマの設定（通常はSystem Managerへのアクセスに使用されるブラウザのテーマの設定）です。
（右）	ダークテーマ（明るいテキストの背景が暗い）

関連情報

"Webサービスへのアクセスの管理"

"Webブラウザを使用したノードのログファイル、コアダンプファイル、およびMIBファイルへのアクセス"

ONTAPクラスタでプロトコルを設定する

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

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します" System Manger を使用して ONTAP クラスタをセットアップします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ステップ

1. を選択し、[プロトコルの設定]*をクリックします。
   - NASプロトコルを有効にするには、* NFS または SMB *を選択します。
   - SANプロトコルを有効にするには、* iSCSI または FC *を選択します。
   - NVMeプロトコルを有効にするには、*[NVMe]*を選択します。

ONTAP System Managerでライセンスキーを追加して新機能を有効にする

ONTAP 9 .10.1より前のリリースでは、ONTAP機能はライセンスキーで有効になり、ONTAP 9 .10.1以降の機能はNetAppライセンスファイルで有効になります。System Managerを使用して、ライセンスキーとNetAppライセンスファイルを追加できます。

ONTAP 9 .10.1以降では、System Managerを使用してNetAppライセンスファイルをインストールし、複数のライセンスされた機能をすべて一度に有効にします。NetAppライセンスファイルを使用すると、個別の機能ライセンスキーを追加する必要がなくなるため、ライセンスのインストールが簡単になります。NetAppライセンスファイルはNetAppサポートサイトからダウンロードします。

一部の機能のライセンスキーをすでにお持ちで、ONTAP 9 10.1にアップグレードする場合は、引き続きそれらのライセンスキーを使用できます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ライセンス]*で、を選択します →。
3. [* 参照 *] を選択します。ダウンロードしたNetAppライセンスファイルを選択します。
4. 追加するライセンスキーがある場合は、「 * 28 文字のライセンスキーを使用する * 」を選択して、キーを入力します。

ONTAP System Managerを使用してクラスタ構成をダウンロードする

ONTAP 9 .11.1以降では、System Managerを使用してクラスタとそのノードに関する設定の詳細をダウンロードできます。この情報は、インベントリ管理、ハードウェア交換、およびライフサイクルアクティビティに使用できます。この情報は、AutoSupport（ASUP）データを送信しないサイトで特に役立ちます。

クラスタ構成の詳細には、クラスタ名、クラスタONTAPのバージョン、クラスタ管理LIF、ボリューム、LIF数などがあります。

ノード設定の詳細には、ノード名、システムシリアル番号、システムID、システムモデル、ONTAPバージョン、MetroCluster情報、SP / BMCネットワーク情報、暗号化設定情報などがあります。

手順

1. [クラスタ]>[概要]*をクリックします。
2. をクリックし

てドロップダウンメニューを表示します。
3. [Download configuration]*を選択します。
4. HAペアを選択し、*[ダウンロード]*をクリックします。

   設定はExcelスプレッドシートとしてダウンロードされます。

   - 最初のシートにはクラスタの詳細が含まれています。
   - 他のシートにはノードの詳細が含まれています。

ONTAP System Managerを使用してクラスタにタグを割り当てる

ONTAP 9 14.1以降では、System Managerを使用してクラスタにタグを割り当て、プロジェクトやコストセンターなどのオブジェクトをカテゴリに属するオブジェクトとして識別できます。

タスクの内容

クラスタにタグを割り当てることができます。まず、タグを定義して追加する必要があります。その後、タグを編集または削除することもできます。

タグは、クラスタの作成時に追加することも、あとから追加することもできます。

タグを定義するには、キーを指定し、"`key:value`"の形式で値を関連付けます。たとえば、「`dept:engineering`」や「`location:san-jose`」などです。

タグを作成するときは、次の点を考慮する必要があります。

- キーの長さは1文字以上で、nullにすることはできません。値にはnullを指定できます。
- キーは、値をカンマで区切って複数の値とペアにすることができます（例："`location:san-jose, Toronto"'）。
- タグは複数のリソースに使用できます。
- キーの先頭は小文字にする必要があります。

手順

タグを管理するには、次の手順を実行します。

1. System Managerで、*[クラスタ]*をクリックして概要ページを表示します。

   タグは* Tags *セクションに表示されます。

2. [タグの管理]*をクリックして、既存のタグを変更するか、新しいタグを追加します。

   タグを追加、編集、または削除できます。

実行する処理	実行する手順
タグの追加	a. [タグの追加]*をクリックします。 b. キーとその値を指定します（複数の値はカンマで区切ります）。 c. [保存（ Save ）] をクリックします。
タグの編集	a. 「* Key 」および「 Values（オプション）*」フィールドの内容を変更します。 b. [保存（ Save ）] をクリックします。
タグの削除	a. 削除するタグの横にあるをクリックし ます。

ONTAP System Manager を使用してサポートケースを表示および送信する

ONTAP 9.9.1以降では、クラスタに関連付けられているActive IQ Digital Advisor（単にDigital Advisorとも呼ばれる）からサポート ケースを表示できます。NetApp サポート サイトで新しいサポート ケースを送信するために必要なクラスタの詳細をコピーすることもできます。ONTAP 9.10.1以降では、サポート担当者による問題のトラブルシューティングに役立つように、テレメトリ ログを有効にできます。

ファームウェアの更新に関するアラートを受信するには、Active IQ Unified Managerに登録する必要があります。を参照してください "Active IQ Unified Managerのドキュメントリソース"。

手順

1. System Manager で、 * Support * を選択します。

   このクラスタに関連付けられている未解決のサポートケースのリストが表示されます。

2. 次のリンクをクリックして手順を実行します。
   - * ケース番号 * ：ケースの詳細を参照してください。
   - * NetApp Support Siteにアクセス * ：NetApp Support Siteの「 My AutoSupport 」ページに移動して、ナレッジベースの記事を参照したり、新しいサポートケースを送信したりできます。
   - * My Cases * ：NetApp Support Siteの * My Cases * ページに移動します。
   - * クラスタの詳細を表示 * ：新しいケースを送信するときに必要な情報を表示してコピーします。

テレメトリログを有効にする

ONTAP 9 .10.1以降では、System Managerを使用してテレメトリログを有効にすることができます。テレメトリログを許可すると、System Managerによってログに記録されるメッセージに、メッセージをトリガーし

た正確なプロセスを示す特定のテレメトリIDが付与されます。そのプロセスに関連して発行されるすべてのメッセージは、操作ワークフローの名前と番号で構成される同じ識別子を持ちます（例：「add-volume-1941290」）。

パフォーマンスに問題が発生した場合は、テレメトリログを有効にして、サポート担当者がメッセージが発行された特定のプロセスを簡単に識別できるようにすることができます。テレメトリ識別子がメッセージに追加された場合、ログファイルはわずかに拡大されます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. [* UI設定*（UI Settings）]セクションで、[テレメータのログを許可する（Allow Telemetry logging *）]チェックボックスをオンにし

ONTAP System ManagerでストレージVMの最大容量制限を管理する

ONTAP 9 .13.1以降では、System Managerを使用して、Storage VMの最大容量制限を有効にし、使用済みストレージが最大容量の一定の割合に達したときにアラートをトリガーするしきい値を設定できます。

Storage VMの最大容量制限を有効にする

ONTAP 9 .13.1以降では、Storage VM内のすべてのボリュームに割り当てることができる最大容量を指定できます。最大容量は、Storage VMを追加するとき、または既存のStorage VMを編集するときに有効にすることができます。

手順

1. >[Storage VMs]*を選択します。
2. 次のいずれかを実行します。
   - Storage VMを追加するには、をクリックし + Add ます。
   - Storage VMを編集するには、Storage VM名の横にあるをクリックし ⋮ 、*[編集]*をクリックします。
3. Storage VMの設定を入力または変更し、[最大容量制限を有効にする]チェックボックスを選択します。
4. 最大容量サイズを指定します。
5. アラートをトリガーするしきい値として使用する最大容量の割合を指定します。
6. [保存（ Save ）] をクリックします。

Storage VMの最大容量制限を編集する

ONTAP 9 .13.1以降では、既存のStorage VMの最大容量制限を編集できます（既存のStorage VMがある場合）最大容量制限が有効になりました。

手順

1. >[Storage VMs]*を選択します。
2. Storage VMの名前の横にあるをクリックし ⋮ 、*[編集]*をクリックします。

   [最大容量制限を有効にする]チェックボックスはすでにオンになっています。

3. 次のいずれかの手順を実行します。

アクション	手順
最大容量制限を無効にする	1. チェックボックスをオフにします。 2. [保存（ Save ）] をクリックします。
最大容量制限を変更します	1. 新しい最大容量サイズを指定します。（Storage VMにすでに割り当てられているスペースよりも小さいサイズを指定することはできません）。 2. アラートをトリガーするしきい値として使用する最大容量の新しいパーセンテージを指定します。 3. [保存（ Save ）] をクリックします。

関連情報

- "Storage VMの最大容量制限を表示する"
- "System Managerでの容量測定"
- "SVMの容量制限を管理します。"

ONTAP System Managerでクラスタ、階層、SVMの容量を監視する

System Managerを使用して、使用済みのストレージ容量と、クラスタ、ローカル階層、またはStorage VMで使用可能な残りの容量を監視できます。

ONTAPの各バージョンでは、より堅牢な容量監視情報が提供されます。

- ONTAP 9 .13.1以降では、Storage VMの最大容量制限を有効にし、使用済みストレージが最大容量の一定の割合に達したときにアラートをトリガーするしきい値を設定できます。
- ONTAP 9 12.1以降では、ローカル階層のコミット済み容量が表示されます。
- ONTAP 9.10.1以降のSystem Managerでは、クラスタの容量に関する履歴データと、使用済みまたは使用可能な容量に関する予測を表示できます。ローカル階層やボリュームの容量を監視することもできます。

使用済み容量の測定値は、ONTAPのバージョンによって表示されます。詳細は、を"System Managerでの容量測定"参照してください。

クラスタの容量を表示する

System Managerのダッシュボードで、クラスタの容量測定値を確認できます。

開始する前に

クラウドの容量に関連するデータを表示するには、Digital Advisorのアカウントがあり、接続されている必要があります。

手順

1. System Manager で、 * ダッシュボード * をクリックします。

2. 容量 * セクションでは、次の情報を確認できます。
   - クラスタの合計使用容量
   - クラスタの合計使用可能容量
   - 使用済み容量と使用可能容量の割合。
   - データ削減率：
   - クラウドで使用されている容量。
   - 使用容量の履歴。
   - 容量使用量の予測

   System Managerでは、容量表現にルートストレージ階層（アグリゲート）の容量は考慮されません。

3. グラフをクリックすると、クラスタの容量に関する詳細が表示されます。

   容量測定値は2つの棒グラフで表示されます。

   - 上部のグラフには、物理容量（使用済みの物理スペース、リザーブスペース、使用可能なスペース）が表示されます。
   - 下部のグラフには、論理容量（クライアントデータ、Snapshot、クローンのサイズ）、および使用済み論理スペースの合計が表示されます。

   棒グラフの下には、データ削減の測定値が表示されます。

   - クライアントデータのみのデータ削減率（スナップショットとクローンは含まれません）。
   - 全体的なデータ削減率。

詳細については、を参照してください "System Managerでの容量測定"。

ローカル階層の容量を表示する

ローカル階層の容量に関する詳細を表示できます。ONTAP 9.12.1 以降では、容量 ビューにローカル ティアのコミット済み容量も含まれるようになりました。これにより、コミット済み容量に対応して空き容量不足を回避するために、ローカル ティアに容量を追加する必要があるかどうかを判断できます。

手順

1. [ストレージ] 、 [階層] の順にクリックします。
2. ローカル階層の名前を選択します。
3. ［概要］ページの［容量］セクションでは、次の3つの測定値が棒グラフに表示されます。
   - 使用済み容量とリザーブ容量
   - 使用可能容量
   - コミット済み容量（ONTAP 9.12.1以降）
4. グラフをクリックして、ローカル階層の容量に関する詳細を確認します。

容量測定値は2つの棒グラフで表示されます。

- 上部の棒グラフには、物理容量（使用済みの物理スペース、リザーブスペース、使用可能なスペース）が表示されます。
- 下部の棒グラフには、論理容量（クライアントデータ、Snapshot、クローンのサイズ）、および使用済み論理スペースの合計が表示されます。

棒グラフの下には、データ削減のための測定比率が表示されます。

- クライアントデータのみのデータ削減率（スナップショットとクローンは含まれません）。
- 全体的なデータ削減率。

詳細については、を参照してください "System Managerでの容量測定"。

オプションのアクション

- コミット済み容量がローカル階層の容量よりも大きい場合は、空きスペースが不足する前にローカル階層に容量を追加することを検討してください。を参照して "ローカル階層への容量の追加（アグリゲートへのディスクの追加）"
- 特定のボリュームがローカル階層で使用しているストレージを確認するには、*[ボリューム]*タブを選択します。

Storage VM内のボリュームの容量を表示する

Storage VMのボリュームで使用されているストレージの容量と、まだ使用可能な容量を確認できます。使用済みストレージと使用可能なストレージの合計測定値を「ボリューム間の容量」と呼びます。

手順

1. **>**[Storage VMs]*を選択します。
2. Storage VMの名前をクリックします。
3. [Capacity]*セクションまでスクロールします。このセクションには、次の測定値を含む棒グラフが表示されます。
   - 使用済み物理容量：このStorage VMのすべてのボリュームの使用済み物理ストレージの合計。
   - 使用可能：このStorage VMのすべてのボリュームで使用可能な容量の合計。
   - 使用済み論理容量：このStorage VMのすべてのボリュームの使用済み論理ストレージの合計。

測定値の詳細については、を参照してください"System Managerでの容量測定"。

Storage VMの最大容量制限を表示する

Storage.13.1以降では、ONTAP 9 VMの最大容量制限を表示できます。

開始する前に

表示するには、事前に確認しておく必要があります"Storage VMの最大容量制限を有効にする"。

手順

1. **>**[Storage VMs]*を選択します。

最大容量測定値は次の2つの方法で表示できます。

- Storage VMの行で、*[最大容量]*列を確認します。この列には、使用済み容量、使用可能容量、および最大容量を示す棒グラフが表示されます。
- Storage VMの名前をクリックします。[概要]*タブをスクロールして、左側の列に最大容量、割り当て容量、および容量のアラートしきい値を確認します。

関連情報

- "Storage VMの最大容量制限を編集する"
- "System Managerでの容量測定"

ONTAP System Managerでハードウェア構成を表示して問題を特定します

ONTAP 9 8以降では、System Managerを使用してネットワーク上のハードウェア構成を表示し、ハードウェアシステムの健全性とケーブル構成を確認できます。

手順

ハードウェア構成を表示するには、次の手順を実行します。

1. System Manager で、 * Cluster > Hardware * を選択します。
2. コンポーネントの上にマウスを置くと、ステータスやその他の詳細が表示されます。

   さまざまなタイプの情報を表示できます。

   - [コントローラに関する情報]
   - [ディスクシェルフに関する情報]
   - [ストレージスイッチに関する情報]
3. System.12.1以降では、ONTAP 9 Managerでケーブル接続情報を表示できます。ケーブルを表示するには、*ケーブルを表示*チェックボックスをクリックし、ケーブルの上にカーソルを置くと接続情報が表示されます。
   - [ケーブル接続に関する情報]

コントローラに関する情報

次の情報を表示できます。

ノード

- 正面図と背面図を表示できます。
- ディスクシェルフを内蔵したモデルの場合は、前面ビューでもディスクレイアウトを確認できます。
- 次のプラットフォームを表示できます。

プラットフォーム	ONTAPバージョンのSystem Managerでサポート								
	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8（プレビューモードのみ）
AFF A20用	○								
AFF A30用	○								
AFF A50用	○								
AFF A70用		○							
AFF A90用		○							
AFF A1K用		○							
AFF A150用		○	○	○					
AFF A220用		○	○	○	○	○	○	○	○
AFF A250用		○	○	○	○	○	○	○	
AFF A300用		○	○	○	○	○	○	○	○
AFF A320用		○	○	○	○	○	○	○	
AFF A400		○	○	○	○	○	○	○	○

AFF A700用		○	○	○	○	○	○	○	○
AFF A700s用		○	○	○	○	○	○	○	
AFF A800用		○	○	○	○	○	○	○	
AFF C30用	○								
AFF C60用	○								
AFF C80用	○								
AFF C190用		○	○	○	○	○	○	○	○
AFF C250用		○	○	○	はい*	はい*	はい*		
AFF C400用		○	○	○	はい*	はい*	はい*		
AFF C800用		○	○	○	はい*	はい*	はい*		
ASA A150		○	○	○					
ASA A250		○	○	○					
ASA A400		○	○	○					
ASA A800		○	○	○					
ASA A900		○	○	○					
ASA C250		○	○	○					

ASA C400		○	○	○					
ASA C800		○	○	○					
FAS70		○							
FAS90		○							
FAS500f		○	○	○	○	○	○	○	
FAS2720		○	○	○	○	○			
FAS2750		○	○	○	○	○			
FAS8300		○	○	○	○	○			
FAS8700		○	○	○	○	○			
FAS9000		○	○	○	○	○			
FAS9500		○	○	○	○	○			

ポート

- ダウンしている場合は、ポートが赤で強調表示されます。
- ポートにカーソルを合わせると、ポートのステータスやその他の詳細が表示されます。
- コンソールポートは表示できません。

  注：

  - ONTAP 9 .11.1以降では、SASポートがエラー状態にある場合、または使用中のケーブル接続済みポートがオフラインになった場合にのみ、SASポートが赤で強調表示されます。ポートがオフラインで接続されていない場合は白で表示されます。
  - ONTAP 9 .10.1以前では、SASポートが無効になると赤で強調表示されます。

FRU

FRUに関する情報は、FRUの状態が最適でない場合にのみ表示されます。

- ノードまたはシャーシのPSUに障害が発生しました。
- ノードで高温が検出されました。
- ノードまたはシャーシのファンで障害が発生しました。

アダプタカードアダプタカード

- 外部カードが挿入されている場合は、部品番号フィールドが定義されているカードがスロットに表示されます。
- ポートがカードに表示されます。
- サポートされているカードの場合は、そのカードの画像を表示できます。カードがサポートされているパーツ番号のリストに含まれていない場合は、一般的な図が表示されます。

ディスクシェルフに関する情報

次の情報を表示できます。

ディスクシェルフ

- 正面図と背面図を表示できます。
- 次のディスクシェルフモデルを確認できます。

システムで実行しているバージョン	これで、 System Manager を使用した表示
ONTAP 9.9.1以降	「サービス終了」または「販売終了」に指定されているすべてのシェルフ
ONTAP 9.8	DS4243、DS4486、DS212C、DS2246、DS224C、およびNS224

シェルフポート

- ポートのステータスを表示できます。
- ポートが接続されている場合は、リモートポートの情報を表示できます。

シェルフ**FRU**

- PSU障害情報が表示されます。

ストレージスイッチに関する情報

次の情報を表示できます。

ストレージスイッチ

- ディスプレイには、シェルフとノードの接続に使用されるストレージスイッチとして機能するスイッチが表示されます。
- ONTAP 9 .9.1以降では、ストレージスイッチとクラスタの両方として機能するスイッチに関する情報が表示されます。この情報はHAペアのノード間で共有することもできます。
- 次の情報が表示されます。
  - スイッチ名
  - IPアドレス
  - シリアル番号
  - SNMPバージョン
  - システムバージョン
- 次のストレージスイッチモデルを確認できます。

システムで実行しているバージョン	これで、 System Manager を使用した表示
ONTAP 9 .11.1以降	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 NVIDIA SN2100
ONTAP 9.10.1 および 9.9.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
ONTAP 9.8	Cisco Nexus 3232C

ストレージスイッチポート

- 次の情報が表示されます。
  - ID名
  - IDインデックス
  - 都道府県
  - リモート接続
  - その他の詳細

ケーブル接続に関する情報

ONTAP 9.12.1以降では、次のケーブル接続情報を表示できます。

- ストレージブリッジを使用しない場合は、コントローラ、スイッチ、シェルフ間の配線
- * Connectivity *。ケーブルの両端にあるポートのIDとMACアドレスを示します

ONTAP System Managerを使用してノードを管理する

System Managerを使用して、クラスタにノードを追加して名前を変更できます。また、ノードをリブート、テイクオーバー、ギブバックすることもできます。

クラスタにノードを追加

新しいノードを追加してクラスタのサイズと容量を拡張できます。

開始する前に

新しいノードをクラスタにケーブル接続しておく必要があります。

タスクの内容

ONTAP 9.8 以降、またはONTAP 9.7 で System Manager を操作するには、別々のプロセスがあります。

ONTAP 9 .8以降の手順

- System Managerを使用したクラスタへのノードの追加（ONTAP 9.8以降）*

手順

1. [*Cluster] > [Overview] を選択します。

   新しいコントローラは、クラスタネットワークに接続されたノードとして表示されますが、クラスタには含まれません。

2. 「 * 追加」を選択します。
   - ノードがクラスタに追加されます。
   - ストレージは暗黙的に割り当てられます。

ONTAP 9.7での手順

- System Managerを使用したクラスタへのノードの追加（ONTAP 9.7）*

手順

1. *（クラシックバージョンに戻る）*を選択します。
2. [構成]>[クラスタの拡張]*を選択します。

   新しいノードはSystem Managerで自動的に検出されます。

3. [新しいエクスペリエンスに切り替える]*を選択します。
4. [クラスタ]>[概要]*を選択して、新しいノードを表示します。

サービスプロセッサのシャットダウン、再起動、または編集

ノードをリブートまたはシャットダウンすると、ノードのHAパートナーによって自動的にテイクオーバーが実行されます。

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"ノードをシャットダウンして再起動します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

手順

1. [*Cluster] > [Overview] を選択します。
2. [ノード]*で、を選択します ⋮。
3. ノードを選択し、**[**シャットダウン**]**、**[**リブート**]**、または*[サービスプロセッサの編集]*を選択します。

   ノードがリブートされてギブバックを待機している場合は、* giveback *オプションも使用できます。

   を選択した場合は、[手動]を選択して**IP**アドレス、サブネットマスク、およびゲートウェイを入力するか、 DHCP *を選択して動的ホスト設定を指定できます。

ノードの名前変更

ONTAP 9.14.1以降では、クラスタの概要ページでノードの名前を変更できます。

> この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"ノードの名前を変更します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

手順

1. [クラスタ]*を選択します。クラスタの概要ページが表示されます。
2. [ノード]*セクションまで下にスクロールします。
3. 名前を変更するノードの横にあるを選択し ⋮、*[名前の変更]*を選択します。
4. ノード名を変更し、*[名前の変更]*を選択します。

ライセンス管理

ONTAPライセンスの概要

ライセンスには、ソフトウェアの使用権が1つ以上記録されています。ONTAP 9.10.1以降では、すべてのライセンスがNetAppライセンス ファイル（NLF）として提供されます。これは、複数の機能を有効にする単一のファイルです。2023年5月以降、すべてのAFFシステム（AシリーズとCシリーズの両方）とFASシステムが、ONTAP ONEソフトウェア スイートまたはONTAP Baseソフトウェア スイートのいずれかとともに販売され、2023年6月以降、すべてのASAシステムがONTAP ONE for SANとともに販売されています。ONTAP 9.10.1で初めて導入された個別のNLFバンドルに代わって、各ソフトウェア スイートが単一のNLFとして提供されています。

ONTAP Oneに含まれるライセンス

ONTAP Oneには、すべての利用可能なライセンス機能が含まれています。表に示すように、従来のCore Bundle、Data Protection Bundle、Security and Compliance Bundle、Hybrid Cloud Bundle、Encryption Bundleで提供していた内容の組み合わせが含まれています。Encryptionは一部の国では使用できません。

以前のバンドル名	含まれるONTAPキー

Core Bundle	FlexClone
	SnapRestore
	NFS、SMB、S3
	FC、iSCSI
	NVMe-oF
Security and Compliance Bundle	自律型ランサムウェア対策
	MTKM
	SnapLock
Data Protection Bundle	SnapMirror（非同期、同期、アクティブ同期）
	SnapCenter
	NetAppターゲット用のSnapMirror S3
Hybrid Cloud Bundle	SnapMirrorクラウド
	NetApp以外のターゲット用のSnapMirror S3
暗号化バンドル	NetAppボリューム暗号化
	Trusted Platformモジュール

ONTAP Oneに含まれていないライセンス

ONTAP Oneには、以下をはじめとするNetAppのクラウド提供サービスは含まれていません。

- NetAppクラウド階層化
- データインフラの分析情報
- NetAppバックアップとリカバリ
- データ ガバナンス

既存システム向けの**ONTAP One**

現在NetAppのサポートは受けているもののONTAP Oneにアップグレードされていない既存のシステムがある場合、これらのシステムの既存のライセンスは引き続き有効であり、期待どおりに機能します。たとえば、既存のシステムにSnapMirrorライセンスがすでにインストールされている場合、ONTAP Oneにアップグレードして新しいSnapMirrorライセンスを取得する必要はありません。ただし、既存のシステムにSnapMirrorライセンスがインストールされていない場合、そのライセンスを取得するには、追加料金でONTAP Oneにアップグレードする必要があります。

2023年6月以降、28文字のライセンスキーを使用するONTAPシステムでも使用できます"ONTAP OneまたはONTAP Base互換性バンドルへのアップグレード"。

ONTAP Baseに含まれるライセンス

ONTAP BaseはONTAPシステム向けのオプション ソフトウェア スイートで、ONTAP Oneの代替として提供されます。SnapMirrorやSnapCenterなどのデータ保護テクノロジが不要で、自律型ランサムウェア対策のようなセキュリティ機能も要求されないユースケース（テスト / 開発専用環境などの非本番システム）に特化したバンドルです。ONTAP Baseにライセンスを追加することはできません。SnapMirrorなどの追加ライセンス

が必要な場合は、ONTAP Oneにアップグレードする必要があります。

以前のバンドル名	含まれるONTAPキー
Core Bundle	FlexClone
	SnapRestore
	NFS、SMB、S3
	FC、iSCSI
	NVMe-oF
暗号化バンドル	NetAppボリューム暗号化
	Trusted Platformモジュール

ONTAP One for SANに含まれるライセンス

ONTAP One for SANは、ASA AシリーズおよびCシリーズのシステムで使用できます。これは、SANで使用できる唯一のソフトウェア スイートです。ONTAP One for SANには、次のライセンスが含まれています。

含まれるONTAPキー
FlexClone
SnapRestore
FC、iSCSI
NVMe-oF
MTKM
SnapLock
SnapMirror（非同期、同期、アクティブ同期）
SnapCenter
SnapMirrorクラウド
NetAppボリューム暗号化
Trusted Platformモジュール

その他のライセンス提供方法

ONTAP 8.2～9.9.1では、ライセンス キーは28文字の文字列の形で提供され、ONTAPの機能ごとに1つのキーが存在します。ONTAP 8.2からONTAP 9.9.1を使用している場合は、ONTAP CLIを使用してライセンス キーをインストールします。

ONTAP 9.10.1では、System ManagerまたはCLIを使用して28文字のライセンス キーをインストールできます。ただし、NetAppライセンス ファイルがインストールされている機能に対して、さらに28文字のライセンス キーをインストールすることはできません。System Managerを使用したNLFまたはライセンスキーのインストールについては、を参照してください"ONTAPライセンスのインストール"。

関連情報

"システムにすでにNLFがある場合にONTAP Oneライセンスを取得する方法"

"サポートサイトを使用してONTAPソフトウェアの使用権と関連ライセンスキーを確認する方法"

"NetApp：ONTAP使用権リスクステータス"

NetAppサポートサイトから**NetApp**ライセンスファイル（**NLF**）をダウンロードします。

ONTAP 9 .10.1以降を実行しているシステムの場合は、NetAppサポートサイトからONTAP OneまたはONTAP Core用NLFをダウンロードして、既存のシステムのバンドルライセンスファイルをアップグレードできます。

SnapMirrorクラウドとSnapMirror S3のライセンスは、ONTAP ONEには含まれていません。これらはONTAP One Compatibilityバンドルの一部であり、ONTAP Oneとをお持ちの場合は無料で入手できます"個別にリクエスト"。

手順

ONTAP ONEライセンスファイルは、既存のNetAppライセンスファイルバンドルがあるシステム、および28文字のライセンスキーがONTAP 9 .10.1以降を実行するシステムでNetAppライセンスファイルに変換されたシステム用にダウンロードできます。また、ONTAPベースからONTAP Oneにシステムをアップグレードすることもできます。

既存の**NLF**をアップグレード

1. アップグレードまたは変換するライセンスファイルバンドル（ONTAP BaseからONTAP One、Core BundleおよびデータProtectionバンドルからONTAP Oneなど）は、NetApp営業チームにお問い合わせください。

   リクエストが処理されると、件名が「SO#[SO番号]のNetAppソフトウェアライセンス通知」と記載されたメールがnetappsw@netapp.comから送信されます。メールには、ライセンスのシリアル番号が記載されたPDF添付ファイルが添付されています。

2. にログインし "NetAppサポートサイト"ます。
3. [システム]>[ソフトウェアライセンス]*を選択します。
4. メニューから*シリアル番号*を選択し、受け取ったシリアル番号を入力して*新規検索*をクリックします。
5. 変換するライセンスバンドルを探します。
6. 各ライセンスバンドルの[Get NetApp License File]*をクリックし、NLFが利用可能になったらダウンロードします。
7. "インストール"ONTAP Oneファイル。

ライセンスキーから変換された**NLF**のアップグレード

1. にログインし "NetAppサポートサイト"ます。
2. [システム]>[ソフトウェアライセンス]*を選択します。
3. メニューから*シリアル番号*を選択し、システムのシリアル番号を入力して*新規検索*をクリックします。
4. 変換するライセンスを探し、* Eligibility 列で Check *をクリックします。
5. [Check Eligibility]フォーム*で、*[Generate Licenses for 9.10.x and later]*をクリックします。
6. [Check Eligibility]フォーム*を閉じます。

   ライセンスが生成されるまで少なくとも2時間待つ必要があります。

7. 手順1～3を繰り返します。
8. ONTAP Oneライセンスを探し、*[Get NetApp License File]*をクリックして配信方法を選択します。
9. "インストール"ONTAP Oneファイル。

ONTAPへのNetAppライセンスのインストール

NetAppライセンス ファイル（NLF）とライセンス キーはSystem Managerを使用してインストールできます（NLFのインストールの推奨方法）。また、ONTAP CLIを使用してライセンス キーをインストールすることもできます。ONTAP 9.10.1以降では、機能はNetAppライセンス ファイルで有効になり、ONTAP 9.10.1より前のリリースでは、ONTAP機能はライセンス キーで有効になります。

手順

"ダウンロードしたNetAppライセンスファイル"またはのライセンスキーをすでに使用している場合は、System ManagerまたはONTAP CLIを使用してNLFと28文字のライセンスキーをインストールできます。

System Manager - ONTAP 9.8以降

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ライセンス]*で、を選択します →。
3. [* 参照 *] を選択します。ダウンロードしたNetAppライセンスファイルを選択します。
4. 追加するライセンスキーがある場合は、「 * 28 文字のライセンスキーを使用する * 」を選択して、キーを入力します。

System Manager - ONTAP 9.7以前

1. [設定]>[クラスタ]>[ライセンス]*を選択します。
2. [ライセンス]*で、を選択します →。
3. [* パッケージ *] ウィンドウで、 [* 追加] をクリックします。
4. [* ライセンスパッケージの追加 *] ダイアログボックスで、 [* ファイルの選択 *] をクリックしてダウンロードしたネットアップライセンスファイルを選択し、 [* 追加] をクリックしてファイルをクラスタにアップロードします。

CLI

1. 1つ以上のライセンスキーを追加します。

   ```
   system license add
   ```

   次の例では、ローカルノード「/mroot/etc/lic_file」からライセンスをインストールします（ファイルがこの場所にある場合）。

   ```
   cluster1::> system license add -use-license-file true
   ```

   次に、AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAおよびBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBというキーを持つライセンスのリストをクラスタに追加する例を示します。

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBB
   ```

   リンクhttps://docsの詳細については、ONTAPコマンドリファレンスを参照してください。NetApp.com /us-en/ ONTAP -CLI/ system-license-add.html[`system license add`^]コマンドを参照してください。

ONTAPライセンスを管理します。

System ManagerまたはONTAP CLIを使用して、ライセンスシリアル番号の表示、ライセンスのステータスの確認、ライセンスの削除など、システムにインストールされているライセンスを表示および管理できます。

ライセンスの詳細を表示する

手順

ライセンスに関する詳細の表示方法は、使用しているONTAPのバージョン、およびSystem ManagerとONTAP CLIのどちらを使用しているかによって異なります。

System Manager - ONTAP 9.8以降

1. 特定の機能ライセンスに関する詳細を表示するには、*[クラスタ]>[設定]*を選択します。
2. [ライセンス]*で、を選択します →。
3. [機能]*を選択します。
4. 表示するライセンス機能を探し、を選択して ⌄ ライセンスの詳細を表示します。

System Manager - ONTAP 9.7以前

1. [設定]>[クラスタ]>[ライセンス]*を選択します。
2. [**Licenses**] ウィンドウで、適切なアクションを実行します。
3. [* 詳細 *] タブをクリックします。

CLI

1. インストールされているライセンスに関する詳細を表示します。

```
system license show
```

ライセンスの削除

System Manager - ONTAP 9.8以降

1. ライセンスを削除するには、*[クラスタ]>[設定]*を選択します。
2. [ライセンス]*で、を選択します →。
3. [機能]*を選択します。
4. 削除するライセンス機能を選択し、*レガシーキーを削除*を選択します。

System Manager - ONTAP 9.7以前

1. [設定]>[クラスタ]>[ライセンス]*を選択します。
2. [**Licenses**] ウィンドウで、適切なアクションを実行します。

状況	操作
ノード上の特定のライセンスパッケージまたはマスターライセンスを削除する	[* 詳細 *] タブをクリックします。
クラスタ内のすべてのノードから特定のライセンスパッケージを削除する	[* パッケージ *] タブをクリックします。

3. 削除するソフトウェアライセンスパッケージを選択し、 * 削除 * をクリックします。

   ライセンスパッケージは一度に1つだけ削除できます。

4. 確認のチェックボックスをオンにし、 * 削除 * をクリックします。

CLI

1. ライセンスを削除します。

```
system license delete
```

次の例は、CIFSという名前でシリアル番号1-81-000000000000000000000123456のライセンスをクラスタから削除するものです。

```
cluster1::> system license delete -serial-number 1-81-
000000000000000000000123456 -package CIFS
```

次の例は、シリアル番号123456789のインストール済みライセンス「Core Bundle」に含まれるすべてのライセンスをクラスタから削除するものです。

```
cluster1::> system license delete { -serial-number 123456789
-installed-license "Core Bundle" }
```

関連情報

"ライセンスの管理用ONTAP CLIコマンド"

"ONTAPコマンド リファレンス"

ライセンスタイプとライセンス方式

ライセンスタイプとライセンス方式について理解しておくと、クラスタのライセンスを管理する際に役立ちます。

ライセンスタイプ

パッケージには、クラスタにインストールされる次のライセンスタイプが1つ以上含まれます。コマンドは、`system license show`パッケージにインストールされているライセンスタイプを表示します。

- ヒョウジュンライセンス(`license`

  標準ライセンスはノードロックライセンスです。特定のシステムシリアル番号（別名「 *controller serial number* 」）を持つノードに対して発行されます。標準ライセンスは、シリアル番号が一致するノードに対してのみ有効です。

  標準のノードロックライセンスをインストールすると、ノードでライセンスされた機能を使用できるようになります。ライセンスされた機能をクラスタで使用するには、少なくとも1つのノードでその機能のライセンスが有効になっている必要があります。ライセンスされた機能の使用権がないノードでライセンスされた機能を使用すると、ライセンス違反になる可能性があります。

- サイトライセンス(`site`）

  サイトライセンスは、特定のシステムシリアル番号には関連付けられません。サイトライセンスをインストールすると、クラスタ内のすべてのノードで、ライセンスされた機能を使用できるようになります。コマンドは `system license show`、指定したクラスタシリアル番号のサイトライセンスを表示します。

  サイトライセンスがあるクラスタからノードを削除した場合、そのノードはサイトライセンスを保持できず、ライセンスされた機能を使用できなくなります。サイトライセンスのあるクラスタにノードを追加すると、そのノードには自動的にサイトライセンスが付与され、その機能を使用できるようになります。

- 評価用ライセンス(`demo`）

  評価用ライセンスは、一定期間（コマンドで表示）が経過すると失効する一時的なライセンス `system license show`です。これにより、使用権を購入せずに特定のソフトウェア機能を試すことができます。このライセンスはクラスタ全体のライセンスであり、ノードの特定のシリアル番号には関連付けられません。

  パッケージの評価用ライセンスがあるクラスタからノードを削除した場合、そのノードは評価用ライセンスを保持できません。

ライセンス方式

パッケージには、クラスタ全体のライセンス（または `demo`タイプ）とノードロックライセンス（ `license`タイプ）の両方をインストールできます `site`。したがって、インストールされたパッケージには、クラスタ内で複数のライセンスタイプが含まれている可能性があります。ただし、パッケージのライセン

ス方式はクラスタに対して 1 つだけです。コマンドのフィールドに `system license status show`は、`licensed method`パッケージに使用されている使用権が表示されます。このコマンドは、ライセンス方式を次のように決定します。

- クラスタにインストールされているライセンスタイプがパッケージに1つしかない場合は、ライセンス方式がインストールされます。
- クラスタにインストールされているライセンスがパッケージにない場合、ライセンス方式はです `none`。
- パッケージに複数のライセンスタイプがクラスタにインストールされている場合、ライセンス方式は、、`license`およびの `demo`ライセンスタイプの優先順位に従って決定されます-`site`。

  例：

  - パッケージにサイトライセンス、標準ライセンス、および評価用ライセンスがある場合、クラスタでのパッケージのライセンス方式はです。 `site`
  - パッケージに標準ライセンスと評価用ライセンスがある場合、クラスタでのパッケージのライセンス方式はです。 `license`
  - パッケージに評価用ライセンスしかない場合、クラスタでのパッケージのライセンス方式はです。 `demo`

ONTAPテノライセンスノカンリヨウコマント

クラスタの機能のライセンスを管理するには、ONTAP CLIコマンドを使用し `system license`ます。機能の使用状況を監視するには、コマンドを使用し `system feature-usage`ます。

このトピックで説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

次の表に、ライセンスを管理するための一般的なCLIコマンドの一部を示します。詳細については、コマンドのマニュアルページへのリンクを参照してください。

状況	使用するコマンド
ライセンスが必要なすべてのパッケージと、次のようなパッケージの現在のライセンスステータスを表示する • パッケージ名 • ライセンス方式 • 有効期限（存在する場合）	"system license show-status"
期限切れのライセンスまたは未使用のライセンスを表示または削除する	"system license clean-up"

状況	使用するコマンド
クラスタでの機能の使用状況の概要をノード単位で表示する	"system feature-usage show-summary"
クラスタでの機能の使用ステータスをノード単位および週単位で表示する	"system feature-usage show-history"
各ライセンス パッケージのライセンス使用権リスク ステータスを表示する	"system license entitlement-risk show"

関連情報

- "ONTAPコマンド リファレンス"
- "NetAppナレッジベース: ONTAP 9.10.1 以降のライセンスの概要"
- "System Managerを使用してNetAppライセンスファイルをインストールする"
- "システム機能"

CLIを使用したクラスタ管理

ONTAP CLIを使用したクラスタ管理について

ONTAPシステムは、コマンドラインインターフェイス（CLI）を使用して管理できます。ONTAP管理インターフェイスの使用、クラスタへのアクセス、ノードの管理などが可能です。

これらの手順は、次の状況で使用する必要があります。

- ONTAP管理者の権限の範囲について理解する必要がある。
- System Managerや自動スクリプトツールではなく、CLIを使用する必要がある。

関連情報

CLIの構文と使用方法の詳細については、のドキュメントを参照して "ONTAPコマンド リファレンス" ください。

クラスタ管理者とSVM管理者

ONTAPのクラスタ管理者とSVM管理者のロールについて

クラスタ管理者は、クラスタ全体と、クラスタに含まれるStorage Virtual Machine（SVM、旧Vserver）を管理します。SVM 管理者は、自身が担当するデータ SVM だけを管理します。

クラスタ管理者は、クラスタ全体とそのリソースを管理できます。また、データ SVM をセットアップし、

SVM の管理を SVM 管理者に委譲することもできます。クラスタ管理者固有の権限は、それぞれのアクセス制御ロールによって異なります。デフォルトでは、「 admin 」というアカウント名またはロール名を持つクラスタ管理者は、クラスタと SVM を管理するためのあらゆる権限を持っています。

SVM 管理者は、ボリューム、プロトコル、 LIF 、サービスなど、自身が担当する SVM のストレージおよびネットワークリソースだけを管理できます。SVM 管理者固有の権限は、クラスタ管理者によって割り当てられた、それぞれのアクセス制御ロールによって異なります。

ONTAPのコマンドラインインターフェイス（CLI）では、コマンドやパラメータ名が変更されていないため、の出力には引き続き_SVM_と表示され `vserver`ます。

ONTAP System Managerへの**Web**ブラウザアクセスの有効化または無効化

WebブラウザからSystem Managerへのアクセスを有効または無効にすることができます。System Managerのログを表示することもできます。

WebブラウザからSystem Managerへのアクセスは [`true`|`false`、[]を使用して制御できます `vserver services web modify -name sysmgr -vserver <cluster_name> -enabled`。

System Managerのロギングは、System Managerがアクセスされたときにクラスタ管理LIFをホストしているノードのファイルに記録され `/mroot/etc/log/mlog/sysmgr.log`ます。ログファイルはブラウザを使用して表示できます。System ManagerのログはAutoSupportメッセージにも含まれます。

ONTAPクラスタ管理サーバの詳細

クラスタ管理サーバは *admin_* SVM とも呼ばれる、クラスタを 1 つの管理可能なエンティティとして扱う特別な Storage Virtual Machine （ SVM ）です。クラスタ管理サーバは最上位の管理ドメインとして機能するとともに、データ SVM に論理的に属さないリソースを所有します。

クラスタ管理サーバは、クラスタ上で常に使用できます。クラスタ管理サーバには、コンソールまたはクラスタ管理 LIF からアクセスできます。

ホームネットワークポートに障害が発生すると、クラスタ管理 LIF がクラスタ内の別のノードに自動的にフェイルオーバーします。使用している管理プロトコルの接続特性に応じて、ユーザがフェイルオーバーを認識できる場合とできない場合があります。コネクションレス型プロトコル（ SNMP など）を使用している場合、または接続が限定されている場合（ HTTP など）には、フェイルオーバーを認識する可能性は低くなります。ただし、長期的な接続（ SSH など）を使用している場合は、フェイルオーバー後にクラスタ管理サーバに再接続する必要があります。

クラスタを作成した場合は、 IP アドレス、ネットマスク、ゲートウェイ、ポートなど、クラスタ管理 LIF のすべての特性を設定します。

データSVMやノードSVMとは異なり、クラスタ管理サーバにはルートボリュームやホストユーザボリュームはありません（システムボリュームをホストすることは可能です）。さらに、クラスタ管理サーバで使用できるのはクラスタ管理タイプの LIF だけです。

コマンドを実行する `vserver show`と、そのコマンドの出力リストにクラスタ管理サーバが表示されます。

ONTAPクラスタ内の**SVM**のタイプ

クラスタは、クラスタとそのリソースの管理、およびクライアントとアプリケーションへのデータアクセスを支援する 4 種類の SVM で構成されます。

クラスタには、次の種類の SVM が含まれます。

- 管理SVM

  クラスタのセットアッププロセスでは、クラスタ用の管理 SVM が自動的に作成されます。管理 SVM はクラスタを表します。

- ノードSVM

  ノード SVM は、ノードがクラスタに追加されると作成され、ノード SVM はクラスタの個別のノードを表します。

- システムSVM（アドバンスト）

  システム SVM は、クラスタレベルの通信用に IPspace 内に自動的に作成されます。

- データSVM

  データ SVM は SVM を提供するデータを表します。クラスタのセットアップ後、クラスタ管理者はデータ SVM を作成し、作成した SVM にボリュームを追加して、クラスタからのデータアクセスを可能にする必要があります。

  クラスタがクライアントにデータを提供するためには、少なくとも 1 つのデータ SVM が必要です。

> 特に指定がないかぎり、 SVM という用語はデータ（データ提供用） SVM を指します。
>
> CLI では、 SVM は Vserver と表示されます。

CLIを使用したクラスタへのアクセス（クラスタ管理者のみ）

ノードシリアルポートを使用した**ONTAP**クラスタへのアクセス

クラスタには、ノードのシリアルポートに接続されたコンソールから直接アクセスできます。

手順

1. コンソールで、Enterキーを押します。

   ログインプロンプトが表示されます。

2. ログインプロンプトで、次のいずれかを実行します。

クラスタにアクセスするアカウント	入力するアカウント名
テフオルトノクラスタアカウント	**admin**
別の管理ユーザアカウント	*username*

パスワードプロンプトが表示されます。

3. adminまたは管理ユーザアカウントのパスワードを入力し、Enterキーを押します。

SSH要求を使用した**ONTAP**クラスタへのアクセス

ONTAPクラスタにSSH要求を発行して管理タスクを実行できます。SSHはデフォルトで有効になっています。

開始する前に

- アクセス方法としてを使用するように設定されたユーザアカウントが必要 `ssh`です。

  コマンドのパラメータ `security login`は、 `-application`ユーザアカウントのアクセス方法を指定します。の詳細については `security login`、を"ONTAPコマンド リファレンス"参照してください。

- Active Directory（AD）のドメインユーザアカウントを使用してクラスタにアクセスする場合は、CIFS対応のStorage VMでクラスタの認証トンネルが設定されている必要があり、さらにADのドメインユーザアカウントがアクセス方式および `domain`認証方式としてを使用してクラスタに追加されている必要があり`ssh`ます。

タスクの内容

- OpenSSH 5.7以降のクライアントを使用する必要があります。
- サポートされているプロトコルはSSH v2だけです。SSH v1はサポートされていません。
- ONTAPでは、1つのノードで同時に最大64のSSHセッションがサポートされています。

  クラスタ管理LIFがノード上にある場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。

  着信接続のレートが1秒あたり10を超える場合、サービスは60秒間一時的に無効になります。

- ONTAP は、 SSH に対して AES および 3DES 暗号化アルゴリズム（ *cipher* とも呼ばれる）のみをサポートしています。

  AESは、128ビット、192ビット、および256ビットのキー長でサポートされます。3DESのキー長は元のDESと同様に56ビットですが、3回繰り返されます。

- FIPSモードが有効な場合、SSHクライアントを接続するには、Elliptic Curve Digital Signature Algorithm（ECDSA）公開鍵アルゴリズムとネゴシエートする必要があります。
- WindowsホストからONTAP CLIにアクセスする場合は、PuTTYなどのサードパーティのユーティリティを使用できます。
- Windows ADユーザ名を使用してONTAPにログインする場合は、ONTAPでADユーザ名とドメイン名が作成されたときと同じ大文字または小文字を使用する必要があります。

ADのユーザ名とドメイン名では大文字と小文字は区別されません。ただし、ONTAPユーザ名では大文字と小文字が区別されます。ONTAPで作成されたユーザ名とADで作成されたユーザ名の大文字小文字表記が一致しないと、ログインに失敗します。

SSH認証オプション

- ONTAP 9 .3以降では、ローカル管理者アカウントを使用できます"SSH多要素認証を有効にします"。

  SSH多要素認証が有効な場合、ユーザは公開鍵とパスワードを使用して認証されます。

- ONTAP 9 .4以降では、LDAPおよびNISのリモートユーザに対応できます"SSH多要素認証を有効にします"。
- ONTAP 9.13.1以降では、必要に応じてSSH認証プロセスに証明書の検証を追加して、ログインのセキュリティを強化できます。これを行うには、"X.509証明書を公開鍵に関連付けます"アカウントが使用します。SSH公開鍵とX.509証明書の両方を使用してSSHを使用してログインすると、ONTAPは、SSH公開鍵で認証する前にX.509証明書の有効性をチェックします。証明書の有効期限が切れているか失効している場合、SSHログインは拒否され、SSH公開鍵は自動的に無効になります。
- ONTAP 9 .14.1以降では、ONTAP管理者はログインセキュリティを強化できます"SSH認証プロセスへのCisco Duo 2要素認証の追加"。Cisco Duo認証を有効にした後の最初のログイン時に、ユーザはSSHセッションのオーセンティケータとして機能するデバイスを登録する必要があります。
- ONTAP 9 .15.1以降では、管理者は、ユーザの信頼スコアに基づいて、SSHユーザに追加の適応認証を提供でき"動的許可の設定"ます。

手順

1. ONTAPクラスタのネットワークにアクセスできるホストから、次のいずれかの形式でコマンドを入力し`ssh`ます。
   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

ADのドメインユーザアカウントを使用している場合は、（ドメイン名のあとにバックスラッシュ2つ）または"*domainname**AD_accountname*"（二重引用符で囲み、ドメイン名のあとにバックスラッシュ1つ）の形式で *domainname**AD_accountname*`指定する必要があります `*username*。

`*hostname_or_IP*`は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4またはIPv6アドレスを使用できます。

`*command*`SSHインタラクティブセッションでは必要ありません。

SSH要求の例

次の例は、「 joe 」という名前のユーザアカウントで、クラスタ管理 LIF が 10.72.137.28 のクラスタにアクセスする SSH 要求を問題で実行する方法を示しています。

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

次の例は、「 `DOMAIN1' 」という名前のドメインの「 John 」という名前のユーザアカウントが、クラスタ管理 LIF が 10.72.137.28 であるクラスタにアクセスするための SSH 要求を問題で できることを示しています。

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

次の例は、「 joe 」という名前のユーザアカウントで SSH MFA 要求を問題で実行し、クラスタ管理 LIF が 10.72.137.32 のクラスタにアクセスする方法を示しています。

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

関連情報

"カンリシヤニンシヨウトRBAC"

ONTAP SSHログインのセキュリティ

ONTAP 9 .5以降では、過去のログイン、失敗したログイン、および前回のログイン後のPrivilegesに対する変更に関する情報を表示できます。

セキュリティ関連の情報は、SSH adminユーザとしてログインした場合に表示されます。次の状態に関するアラートが表示されます。

- アカウント名が最後にログインされた時刻。
- 前回のログイン成功後にログインに失敗した回数。
- 前回のログイン後にロールが変更されたかどうか（adminアカウントのロールが「admin」から「backup」に変更された場合など）。
- 前回のログイン後にロールの追加、変更、または削除機能が変更されたかどうか。

疑わしい情報が表示された場合は、ただちにセキュリティ部門に連絡してください。

ログイン時にこの情報を取得するには、次の前提条件を満たしている必要があります。

- SSHユーザアカウントがONTAPでプロビジョニングされている必要があります。
- SSHセキュリティログインが作成されている必要があります。
- ログインに成功する必要があります。

SSHログインのセキュリティに関する制限事項およびその他の考慮事項

SSHログインのセキュリティ情報には、次の制限事項と考慮事項が適用されます。

- この情報は、SSHベースのログインの場合にのみ表示されます。
- グループベースの管理者アカウント（LDAP / NISおよびADアカウントなど）の場合、自分が属しているグループがONTAPで管理者アカウントとしてプロビジョニングされていれば、ユーザはSSHログイン情報を表示できます。

  ただし、これらのユーザについては、ユーザアカウントのロールの変更に関するアラートを表示できませ

ん。また、ONTAPで管理者アカウントとしてプロビジョニングされたADグループに属するユーザは、前回のログイン以降にログインに失敗した回数を表示できません。

- ユーザについて保持されている情報は、ユーザアカウントがONTAPから削除されると削除されます。
- SSH以外のアプリケーションへの接続に関する情報は表示されません。

SSHログインのセキュリティ情報の例

次の例は、ログイン後に表示される情報の種類を示しています。

- 次のメッセージは、ログインに成功するたびに表示されます。

```
Last Login : 7/19/2018 06:11:32
```

- 前回のログインに成功してからログインに失敗した場合は、次のメッセージが表示されます。

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- 前回のログイン後に失敗したログインがあり、権限が変更されている場合、次のメッセージが表示されます。

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

ONTAPクラスタへのTelnetアクセスまたはRSHアクセスを有効にする

セキュリティのベストプラクティスとして、TelnetとRSHはデフォルトで無効になっています。クラスタがTelnet要求またはRSH要求を受け入れることができるようにするには、デフォルトの管理サービスポリシーでサービスを有効にする必要があります。

TelnetとRSHはセキュアなプロトコルではありません。SSHを使用してクラスタにアクセスすることを検討してください。SSHは、セキュアなリモートシェルおよび対話型ネットワークセッションを提供します。詳細については、を参照してください "SSHを使用したクラスタへのアクセス"。

タスクの内容

- ONTAPでは、1つのノードで同時に最大50のTelnetセッションまたはRSHセッションがサポートされます。

  クラスタ管理LIFがノード上にある場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。

  着信接続のレートが1秒あたり10を超える場合、サービスは60秒間一時的に無効になります。

- rshコマンドにはadvanced権限が必要です。

ONTAP 9 .10.1以降

手順

1. RSHまたはTelnetセキュリティプロトコルが有効になっていることを確認します。

   ```
   security protocol show
   ```

   a. RSHまたはTelnetセキュリティプロトコルが有効になっている場合は、次の手順に進みます。

   b. RSHまたはTelnetセキュリティプロトコルが有効になっていない場合は、次のコマンドを使用して有効にします。

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

   および `security protocol modify`の詳細については `security protocol show`、を"ONTAPコマンド リファレンス"参照してください。

2. またはサービスが管理LIFに存在することを確認し `management-rsh-server` `management-telnet-server` ます。

   ```
   network interface show -services management-rsh-server
   ```

   または

   ```
   network interface show -services management-telnet-server
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

   a. またはサービスが存在する場合は `management-rsh-server` `management-telnet-server` 、次の手順に進みます。

   b. またはサービスが存在しない場合は `management-rsh-server` `management-telnet-server` 、次のコマンドを使用して追加します。

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server

      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   の詳細については `network interface service-policy add-service`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 9 .9以前

タスクの内容

ONTAPでは、事前定義されているファイアウォールポリシーは変更できませんが、事前定義されている`mgmt`管理ファイアウォールポリシーをクローニングし、そのポリシーでTelnetまたはRSHを有効にすることで、新しいポリシーを作成できます。

手順

1. advanced権限モードに切り替えます。

   ```
   set advanced
   ```

2. セキュリティプロトコル（RSHまたはTelnet）を有効にします。

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. `mgmt`管理ファイアウォールポリシーに基づいて新しい管理ファイアウォールポリシーを作成します。

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. 新しい管理ファイアウォールポリシーでTelnetまたはRSHを有効にします。

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   すべてのIPアドレスを許可するには、次のように指定します。 `-ip-list 0.0.0.0/0`

5. 新しいポリシーをクラスタ管理LIFに関連付けます。

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

Telnet要求を使用した**ONTAP**クラスタへのアクセス

管理タスクを実行するために、クラスタへの問題 Telnet 要求を行うことができます。Telnet はデフォルトでは無効になっています。

TelnetとRSHはセキュアなプロトコルではありません。SSHを使用してクラスタにアクセスすることを検討してください。SSHは、セキュアなリモートシェルおよび対話型ネットワークセッションを提供します。詳細については、を参照してください "SSHを使用したクラスタへのアクセス"。

開始する前に

Telnet を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- アクセス方法として Telnet を使用するように設定されたクラスタローカルユーザアカウントを持っている必要があります。

  コマンドのパラメータ `security login`は、 `-application`ユーザアカウントのアクセス方法を指定します。の詳細については `security login`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

- ONTAP では、 1 つのノードについて同時に最大 50 の Telnet セッションがサポートされています。

クラスタ管理LIFがノード上にある場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。

着信接続数が 1 秒あたり 10 を超えると、サービスは一時的に 60 秒間無効になります。

- WindowsホストからONTAP CLIにアクセスする場合は、PuTTYなどのサードパーティのユーティリティを使用できます。
- rshコマンドにはadvanced権限が必要です。

ONTAP 9 .10.1以降

手順

1. Telnetセキュリティプロトコルが有効になっていることを確認します。

   ```
   security protocol show
   ```

   a. Telnetセキュリティプロトコルが有効になっている場合は、次の手順に進みます。

   b. Telnetセキュリティプロトコルが有効になっていない場合は、次のコマンドを使用して有効にします。

      ```
      security protocol modify -application telnet -enabled true
      ```

   および `security protocol modify`の詳細については `security protocol show`、を"ONTAPコマンド リファレンス"参照してください。

2. 管理LIFにサービスが存在することを確認し `management-telnet-server` ます。

   ```
   network interface show -services management-telnet-server
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

   a. サービスが存在する場合は `management-telnet-server` 、次の手順に進みます。

   b. サービスが存在しない場合は `management-telnet-server` 、次のコマンドを使用して追加します。

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   の詳細については `network interface service-policy add-service`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 9 .9以前

開始する前に

Telnet を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- Telnet 要求がファイアウォールを通過できるように、クラスタ管理 LIF またはノード管理 LIF によって使用される管理ファイアウォールポリシーで Telnet が有効になっている必要があります。

  デフォルトでは、 Telnet は無効になっています。 `system services firewall policy show`コマンドで `-service telnet`パラメータを指定すると、ファイアウォールポリシーで`Telnet`が有効になっているかどうかが表示されます。の詳細については `system services firewall policy`、を"ONTAPコマンド リファレンス"参照してください。

- IPv6接続を使用する場合は、クラスタでIPv6が設定されて有効になっている必要があり、ファイアウォールポリシーにIPv6アドレスが設定されている必要があります。

`network options ipv6 show`コマンドは、IPv6が有効になっているかどうかを表示します。の詳細については `network options ipv6 show`、をlink:https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html["ONTAPコマンド リファレンス"^]参照してください。`system services firewall policy show`コマンドは、ファイアウォールポリシーを表示します。

手順

1. 管理ホストで次のコマンドを入力します。

   ```
   telnet hostname_or_IP
   ```

   `hostname_or_IP`は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4またはIPv6アドレスを使用できます。

Telnet要求の例

次の例は、Telnet アクセスが設定されている「joe」というユーザーが、クラスタ管理 LIF が 10.72.137.28 であるクラスタにアクセスするために Telnet 要求を発行する方法を示しています。

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

RSH要求を使用した**ONTAP**クラスタへのアクセス

クラスタに対してRSH要求を発行して管理タスクを実行できます。RSH はセキュアなプロトコルではなく、デフォルトでは無効になっています。

TelnetとRSHはセキュアなプロトコルではありません。SSHを使用してクラスタにアクセスすることを検討してください。SSHは、セキュアなリモートシェルおよび対話型ネットワークセッションを提供します。詳細については、を参照してください "SSHを使用したクラスタへのアクセス"。

開始する前に

RSH を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- アクセス方法として RSH を使用するように設定された、クラスタのローカルユーザアカウントを持っている必要があります。

  コマンドのパラメータ `security login`は、 `-application`ユーザアカウントのアクセス方法を指定します。の詳細については `security login`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

- ONTAPでは、1つのノードで同時に最大50のRSHセッションがサポートされます。

  クラスタ管理LIFがノード上にある場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。

  着信接続のレートが1秒あたり10を超える場合、サービスは60秒間一時的に無効になります。

- rshコマンドにはadvanced権限が必要です。

ONTAP 9 .10.1以降

手順

1. RSHセキュリティプロトコルが有効になっていることを確認します。

   ```
   security protocol show
   ```

   a. RSHセキュリティプロトコルが有効になっている場合は、次の手順に進みます。

   b. RSHセキュリティプロトコルが有効になっていない場合は、次のコマンドを使用して有効にします。

      ```
      security protocol modify -application rsh -enabled true
      ```

   および `security protocol modify`の詳細については `security protocol show`、を"ONTAPコマンド リファレンス"参照してください。

2. 管理LIFにサービスが存在することを確認し `management-rsh-server` ます。

   ```
   network interface show -services management-rsh-server
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

   a. サービスが存在する場合は `management-rsh-server` 、次の手順に進みます。

   b. サービスが存在しない場合は `management-rsh-server` 、次のコマンドを使用して追加します。

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   の詳細については `network interface service-policy add-service`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 9 .9以前

開始する前に

RSH を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- RSH 要求がファイアウォールを通過できるように、クラスタ管理 LIF またはノード管理 LIF によって使用される管理ファイアウォールポリシーで RSH がすでに有効になっている必要があります。

  デフォルトでは、RSHは無効になっています。 `-service rsh`パラメータを指定して`system services firewall policy show`コマンドを実行すると、ファイアウォールポリシーで`RSH`が有効になっているかどうかが表示されます。の詳細については `system services firewall policy`、を"ONTAPコマンド リファレンス"参照してください。

- IPv6接続を使用する場合は、クラスタでIPv6が設定されて有効になっている必要があり、ファイアウォールポリシーにIPv6アドレスが設定されている必要があります。

`network options ipv6 show`コマンドは、IPv6が有効になっているかどうかを表示します。の詳細については `network options ipv6 show`、をlink:https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html["ONTAPコマンド リファレンス"^]参照してください。
`system services firewall policy show`コマンドは、ファイアウォールポリシーを表示します。

手順

1. 管理ホストで次のコマンドを入力します。

   ```
   rsh hostname_or_IP -l username:passwordcommand
   ```

   `hostname_or_IP`は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4またはIPv6アドレスを使用できます。

   `command`は、RSH経由で実行するコマンドです。

RSH要求の例

次の例は、RSHアクセスを使用するように設定された「joe」というユーザが、コマンドを実行するRSH要求を発行する方法を示してい `cluster show`ます。

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPコマンドライン インターフェイスの使用

ONTAPコマンドラインインターフェイスの詳細

ONTAPコマンドラインインターフェイス（CLI）は、管理インターフェイスのコマンドベースのビューを提供します。ストレージ・システム・プロンプトでコマンドを入力すると、コマンド結果がテキストで表示されます。

CLIコマンドプロンプトは、のように表示され `cluster_name::>`ます。

権限レベル（コマンドのパラメータ `set`）をに `advanced`設定する `-privilege`と、次のように、プロンプト

にアスタリスク（*）が含まれます。

```
cluster_name::*>
```

の詳細については `set`、を"ONTAPコマンド リファレンス"参照してください。

CLIコマンド用のさまざまな**ONTAP**シェルについて説明します。

クラスタには、 CLI コマンド用の異なる 3 つのシェルとして、 _clustershell _ 、 _nodeshell _ 、 _systemshell _ があります。シェルは目的が異なり、それぞれに異なるコマンドセットがあります。

- クラスタシェルは、クラスタにログインすると自動的に開始されるネイティブシェルです。

  クラスタの設定と管理に必要なコマンドがすべて含まれています。クラスタシェルのCLIヘルプ（クラスタシェルプロンプトでと入力するとトリガーされる `?`）には、使用可能なクラスタシェルコマンドが表示されます。は `man`クラスタシェルのコマンド、指定したクラスタシェルコマンドのマニュアルページを表示し(`man <command_name>`ます）。の詳細については `man`、を"ONTAPコマンド リファレンス"参照してください。

- ノードシェルは、ノードレベルでのみ有効になるコマンド用の特別なシェルです。

  ノードシェルには、コマンドを使用してアクセスでき `system node run`ます。の詳細については `system node run`、を"ONTAPコマンド リファレンス"参照してください。

  ノードシェルのCLIヘルプ（または `help`でトリガー）に `?`は、使用可能なノードシェルコマンドが表示されます。ノードシェルのコマンドは `man`、指定したノードシェルコマンドのマニュアルページを表示します。

  よく使用されるノードシェルのコマンドとオプションの多くは、クラスタシェルにトンネリングまたはエイリアスされ、クラスタシェルからも実行できます。

- システムシェルは、診断とトラブルシューティングの目的でのみ使用される下位レベルのシェルです。

  システムシェルと関連する `diag` アカウントは、簡単な診断を目的としています。アクセスには診断権限レベルが必要であり、トラブルシューティング タスクを実行するテクニカル サポート専用に予約されています。

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

クラスタシェルでのノードシェルのコマンドおよびオプションへのアクセス

ノードシェルのコマンドとオプションには、ノードシェルからアクセスできます。

```
system node run -node nodename
```

よく使用されるノードシェルのコマンドとオプションの多くは、クラスタシェルにトンネリングまたはエイリアスされ、クラスタシェルからも実行できます。

クラスタシェルでサポートされているノードシェルオプションには、コマンドを使用してアクセスでき `vserver options clustershell`ます。これらのオプションを表示するには、次のいずれかを実行します。

- を使用してクラスタシェルCLIを照会する `vserver options -vserver _nodename_or_clustername_ -option-name ?`
- の詳細については `vserver options`、を"ONTAPコマンド リファレンス"参照してください。

クラスタシェルでノードシェルまたはレガシーのコマンドまたはオプションを入力し、そのコマンドまたはオプションに相当するクラスタシェルコマンドがある場合は、そのクラスタシェルコマンドを使用するようにONTAPから通知されます。

クラスタシェルでノードシェルまたはレガシーのコマンドまたはオプションを入力した場合、そのコマンドまたはオプションについて「 not supported 」ステータスが ONTAP から通知されます。

使用可能なノードシェルコマンドを表示します。

ノードシェルからCLIヘルプを使用すると、使用可能なノードシェルコマンドのリストを取得できます。

手順

1. ノードシェルにアクセスするには、クラスタシェルのシステムプロンプトで次のコマンドを入力します。

   `system node run -node {`*`nodename`*`|local}`

   `local`は、クラスタへのアクセスに使用したノードです。

   この `system node run`コマンドには、エイリアスコマンド、が `run`あります。

2. 使用可能なノードシェルコマンドの一覧を表示するには、ノードシェルで次のコマンドを入力します。

   `[`*`commandname`*`] help`

   `_commandname_`は、可用性を表示するコマンドの名前です。を指定しないと、`_commandname_`使用可能なすべてのノードシェルコマンドが表示されます。

   クラスタシェルCLIに戻るには、Ctrl+Dを入力するか入力し `exit`ます。

   の詳細については `exit`、を"ONTAPコマンド リファレンス"参照してください。

利用可能なノードシェルコマンドを表示する例

次の例は、node2という名前のノードのノードシェルにアクセスし、ノードシェルコマンドの情報を表示します `environment`。

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

ONTAP CLIコマンドディレクトリの移動方法

CLIのコマンドは、コマンドディレクトリごとに階層化されています。階層内でコマンドを実行するには、完全なコマンドパスを入力するか、ディレクトリ構造内を移動します。

CLIを使用している場合は、プロンプトにディレクトリの名前を入力してEnterキーを押すと、コマンドディレクトリにアクセスできます。その後、ディレクトリ名がプロンプトテキストに表示され、適切なコマンドディレクトリを操作していることが示されます。コマンド階層の下位に移動するには、コマンドサブディレクトリの名前を入力し、Enterキーを押します。その後、サブディレクトリ名がプロンプトテキストに含まれ、コンテキストがそのサブディレクトリに移動します。

コマンド全体を入力すると、複数のコマンドディレクトリを移動できます。たとえば、ディスクドライブに関する情報を表示するには、プロンプトでコマンドを入力し `storage disk show`ます。次の例に示すように、一度に1つのコマンドディレクトリに移動してコマンドを実行することもできます。

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

の詳細については `storage disk show`、を"ONTAPコマンド リファレンス"参照してください。

コマンドに最小文字数だけを入力することで、コマンドを現在のディレクトリに一意にすることができます。たとえば、前の例のコマンドを省略するには、と入力し `st d sh`ます。Tabキーを使用して、省略されたコマンドを展開したり、デフォルトのパラメータ値を含むコマンドのパラメータを表示したりすることもできます。

コマンドを使用するとコマンド階層の最上位に移動でき、コマンドまたは `..`コマンドを使用するとコマンド階層の1つ上のレベルに移動 `up`できます `top`。

CLI でアスタリスク（ * ）を付けたコマンドおよびコマンドオプションは、 advanced 権限レベル以上でのみ実行できます。

関連情報

- "上へ"
- "上"

ONTAP CLIで値を指定するルールについて理解する

ほとんどのコマンドには、 1 つ以上の必須またはオプションのパラメータが含まれています。多くのパラメータでは、値を指定する必要があります。CLI で値を指定するには、いくつかのルールがあります。

- 値には、数値、ブール指定子、事前に定義された値の列挙リストからの選択、またはテキスト文字列を指定できます。

  一部のパラメータでは、 2 つ以上の値をカンマで区切って指定できます。値をカンマで区切って指定したリストは、引用符（ "" ）で囲む必要はありません。テキスト、スペース、またはクエリ文字（クエリを意図していない場合、または小なり記号または大なり記号で始まるテキスト）を指定する場合は、必ずエンティティを引用符で囲む必要があります。

- CLIは疑問符(?）をコマンドと解釈し、特定のコマンドのヘルプ情報を表示します。
- コマンド名、パラメータ、特定の値などの CLI に入力するテキストの一部では、大文字と小文字が区別されません。

  たとえば、コマンドのパラメータ値を入力した場合、 `vserver cifs`大文字と小文字の区別は無視されます。ただし、ノード、Storage Virtual Machine（SVM）、アグリゲート、ボリューム、論理インターフェイスの名前などのほとんどのパラメータ値では大文字と小文字が区別されます。

- 文字列またはリストをとるパラメータの値をクリアする場合は、空の一連の引用符（ "" ）またはダッシュ（ "-" ）を指定します。
- ハッシュ記号(#）はシャープ記号とも呼ばれ、コマンドライン入力のコメントを示します。使用する場合は、コマンドラインの最後のパラメータのあとに表示されます。

  CLIでは、と行末の間のテキストは無視され `#`ます。

次の例では、テキストコメント付きでSVMが作成されます。次に、 SVM が変更されてコメントが削除されます。

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

次の例では、記号を使用したコマンドラインコメント `#`は、コマンドの動作を示しています。

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPコマンド履歴を表示し、履歴から任意のコマンドを再実行します。

各CLIセッションには、実行されたすべてのコマンドの履歴が保持されます。現在のセッションのコマンド履歴を表示できます。コマンドを再実行することもできます。

コマンド履歴を表示するには、コマンドを使用し `history`ます。

コマンドを再発行するには、次のいずれかの引数を指定してコマンドを使用し `redo`ます。

- 前のコマンドの一部に一致する文字列

  たとえば、実行したコマンドがのみの `volume show`場合は `volume`、コマンドを使用してコマンドを再実行できます `redo volume`。

- コマンドで表示された前のコマンドの数値ID。 `history`

  たとえば、コマンドを使用すると、履歴リストの4番目のコマンドを再発行できます `redo 4`。

- 履歴リストの末尾からの負のオフセット

  たとえば、コマンドを使用して、2つ前に実行したコマンドを再発行できます `redo -2`。

たとえば、コマンド履歴の最後から3番目のコマンドをやり直すには、次のコマンドを入力します。

```
cluster1::> redo -3
```

関連情報

- "履歴"
- "やり直し（Redo）"
- "ボリューム"

CLIコマンドを編集するための**ONTAP**キーボードショートカット

現在のコマンドプロンプトのコマンドは、アクティブなコマンドです。キーボードショートカットを使用して、アクティブなコマンドをすばやく編集できます。UNIX tsch シェルや Emacs エディタと同様のショートカットを使用できます。

次の表に、CLIコマンドを編集するためのキーボードショートカットを示します。 `Ctrl-`Ctrlキーを押したま

ま、そのあとに指定した文字を入力することを示します。 `Esc-`Escキーを押して放し、その後に指定した文字を入力することを示します。

状況	使用するキーボードショートカット
カーソルを 1 文字左に移動します	• Ctrl+B キーを押下 • 戻る矢印
カーソルを 1 文字右に移動します	• Ctrl+F • 右矢印
カーソルを 1 単語分左に移動します	ESC-B
カーソルを 1 単語分右に移動します	ESC-F
カーソルを行頭に移動します	Ctrl+A
カーソルを行末へ移動します	Ctrl+E
行の先頭からカーソルまでコマンドラインの内容を削除し、カットバッファに保存します。切り取りバッファは ' 一部のプログラムでは *clipboard* と呼ばれるのと同様に ' 一時的なメモリのように機能します	Ctrl+U キーを押下
カーソルから行末までの入力内容を切り取ってバッファに保存する	Ctrl+K キーを押下
カーソルから次の単語の末尾までを切り取ってバッファに保存する	ESC-D
カーソルの前の単語を削除し、切り取りバッファに保存します。	Ctrl+W キーを押下
切り取りバッファの内容を取得し、カーソルのコマンドラインに挿入します	Ctrl+Y キーを押下
カーソルの前の文字を削除します	• Ctrl+H • バックスペース
カーソル位置の文字を削除します	Ctrl+D を使用します
行をクリアします	Ctrl+C キーを押します
画面をクリアします	Ctrl+L キーを押下

状況	使用するキーボードショートカット
コマンドラインの現在の内容を、履歴リストの前のエントリに置き換えます。 このキーボードショートカットを押すたびに履歴カーソルが 1 つ前のエントリに移動します。	• Ctrl+P キーを押下 • ESC-P • 上矢印
コマンドラインの現在の内容を、履歴リストの次のエントリに置き換えます。このキーボードショートカットを押すたびに履歴カーソルが次のエントリに移動します。	• Ctrl+N キーを押下 • ESC-N • 下矢印
部分的に入力されたコマンドを展開するか、現在の編集位置から有効な入力のリストを表示します	• タブ • Ctrl+I
状況に応じたヘルプを表示します	?
疑問符 ?）文字の特殊マッピングをエスケープします。たとえば、コマンドの引数に疑問符を入力するには、Escキーを押してから文字を押し `?` ます。	ESC - ？
TTY 出力を開始します	Ctrl+Q キーを押下
TTY 出力を停止します	Ctrl+S

ONTAP CLIコマンドの権限レベルについて理解する

ONTAP のコマンドとパラメータは、 *admin*、 *advanced*、 *ddiagnostic* の 3 つの権限レベルで定義されます。権限レベルは、タスクの実行に必要なスキルレベルを反映しています。

- * admin *

  このレベルではほとんどのコマンドとパラメータを使用できます。これらは、一般的なタスクまたはルーチンタスクに使用されます。

- * 詳細 *

  このレベルのコマンドとパラメータは高度な知識を必要とし、あまり使用されません。不適切に使用すると、原因の問題につながる可能性があります。

  高度なコマンドまたはパラメータを使用する場合は、必ずサポート担当者のアドバイスを受けてください。

- * 診断 *

  診断コマンドおよびパラメータは、システム停止の原因になる可能性がありますこれらのコマンドは、サポート担当者が問題の診断と修正を行う場合にのみ使用します。

ONTAP CLIでの権限レベルの設定

CLIで権限レベルを設定するには、コマンドを使用し `set`ます。権限レベルの設定変更は、現在のセッションにのみ適用され、新しいセッションでは適用されません。

手順

1. CLIで権限レベルを設定するには、コマンドにパラメータを指定して `-privilege`使用し `set`ます。

権限レベルの設定例

次の例では、権限レベルをadvancedに設定してからadminに設定します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

の詳細については `set`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP CLIの表示環境設定の設定

CLIセッションの表示環境を設定するには、コマンドと `rows`コマンドを使用し `set`ます。設定した環境は、現在のセッションにのみ適用されます。セッションをまたいで持続することはありません。

タスクの内容

次の CLI 表示環境を設定できます。

- コマンドセッションの権限レベル
- システムを停止させる可能性のあるコマンドについては確認を発行するかどうか
- コマンドですべてのフィールドを表示するかどうか `show`
- フィールド区切り文字として使用する文字
- データサイズを報告するときのデフォルトの単位
- インターフェイスが出力を一時的に停止する前に、現在の CLI セッションで画面に表示する行数

  行数を指定しない場合、端末の実際の高さに基づいて自動的に調整されます。実際の高さが定義されていない場合、デフォルトの行数は24です。

- デフォルトのStorage Virtual Machine（SVM）またはノード
- エラーが発生した場合に続行中のコマンドを停止するかどうか

手順

1. CLIの表示環境を設定するには、コマンドを使用し `set`ます。

   現在のCLIセッションで画面に表示する行数を設定するには、コマンドを使用することもできます `rows`。

および `rows` の詳細については `set`、を"ONTAPコマンド リファレンス"参照してください。

CLIでの表示環境の設定の例

次の例では、フィールド区切り文字としてカンマを設定し、デフォルトのデータサイズ単位としてを設定し、行数を50に設定し`GB`ます。

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

関連情報

- "表示"
- "設定"
- "行"

ONTAP CLIでのクエリ演算子の使用

管理インターフェイスでは、クエリ、UNIX形式のパターンおよびワイルドカードがサポートされており、コマンドパラメータ引数の複数の値を照合できます。

次の表に、サポートされるクエリ演算子を示します。

運用者	説明
*	すべてのエントリに一致するワイルドカード。 たとえば、コマンドを `volume show -volume *tmp*`実行すると、名前にが含まれるすべてのボリュームのリストが表示され `tmp`ます。
なんだ?	NOT演算子。 一致しない値を示します。たとえば、は値と一致しないことを `vs0`示します。 `**!vs0**`
OR演算子。 比較する2つの値を区切ります。たとえば、は `*vs0	vs2*`vs0またはvs2のいずれかに一致します。複数のORステートメントを指定できます。たとえば、は `a
b*	*c*エントリ、で始まるエントリ `b`、を含むエントリに `c`一致します `a`。

運用者	説明
..	範囲演算子。 たとえば、は **5..10**`任意の値のfromから `10`inclusiveに一致します `5。
<	less-than演算子。 たとえば、は、 **<20**`より小さい任意の値に一致します `20。
>	greater-than演算子。 たとえば、は、 **>5**`より大きい任意の値に一致します `5。
<=	less-than-or-equal-to演算子。 たとえば、は **⇐5**`次の値以下の値に一致します `5。
>=	以上演算子。 たとえば、は、 **>=5**`以上の任意の値に一致します `5。
{query}	拡張クエリ。 拡張クエリは、コマンド名に続けて、他のパラメータの前に最初の引数として指定する必要があります。 たとえば、コマンドは `volume modify {-volume *tmp*} -state offline`、名前に文字列が含まれるすべてのボリュームをオフラインに設定し`tmp`ます。

クエリ文字をリテラルとして解析する場合は、 `"*abc*"`正しい結果が返されるように、文字を二重引用符（、、 `"0..100"`、、など `"a|b"`）で囲む必要があります `"<10"`。

特殊文字が解釈されないように、rawファイル名は二重引用符で囲む必要があります。これは、クラスタシェルで使用される特殊文字にも当てはまります。

1つのコマンドラインで複数のクエリ演算子を使用できます。たとえば、 `volume show -size >1GB -percent-used <50 -vserver !vs1`「vs1」という名前のStorage Virtual Machine（SVM）に含まれていない、サイズが1GBを超え、使用率が50%未満のすべてのボリュームが表示されます。

関連情報

"CLIコマンドを編集するためのキーボードショートカット"

ONTAP CLIでの**modify**コマンドと**delete**コマンドの使用

拡張クエリを使用すると、指定した値を持つオブジェクトに対して処理を照合して実行できます。

拡張クエリを指定するには、中括弧（{}）で囲みます。拡張クエリは、コマンド名のあとの最初の引数として、他のパラメータの前に指定する必要があります。たとえば、名前に文字列が含まれるすべてのボリュームをオフラインに設定するには `tmp`、次の例のコマンドを実行します。

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

一般に、拡張クエリはコマンドと `delete`コマンドでのみ有効です `modify`。コマンドまたは `show`コマンドでは意味があり `create`ません。

クエリと変更操作の組み合わせは便利なツールです。ただし、正しく実装しないと混乱やエラーが発生する可能性があります。たとえば、（advanced権限）コマンドを使用して `system node image modify`ノードのデフォルトのソフトウェアイメージを自動的に設定すると、他のソフトウェアイメージがデフォルトにならないように設定されます。次の例のコマンドは、実質的にはnull操作です。

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

このコマンドは、現在のデフォルトイメージをデフォルト以外のイメージとして設定し、新しいデフォルトイメージ（以前のデフォルト以外のイメージ）をデフォルト以外のイメージに設定します。これにより、元のデフォルト設定が保持されます。正しく処理を実行するには、次の例のようにコマンドを使用します。

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

fieldsパラメータを使用して、**ONTAP show**コマンドの出力を制限します。

コマンドでパラメータを `show`使用し `-instance`て詳細を表示すると、出力に時間がかかり、必要以上の情報が含まれることがあります。コマンドのパラメータ `show`を `-fields`使用すると、指定した情報のみを表示できます。

たとえば、を実行すると、 `volume show -instance`複数の画面に情報が表示される可能性があります。を使用すると、（常に表示されるデフォルトのフィールドに加えて）指定したフィールドのみが含まれるように出力をカスタマイズできます `volume show -fields *fieldname[,fieldname…]*`。を使用すると、コマンドの有効なフィールドを表示 `show`できます `-fields ?`。

次の例は、パラメータと `-fields`パラメータの出力の違いを示してい `-instance`ます。

```
cluster1::> volume show -instance

                                    Vserver Name: cluster1-1
                                     Volume Name: vol0
                                  Aggregate Name: aggr0
                                     Volume Size: 348.3GB
                              Volume Data Set ID: -
                       Volume Master Data Set ID: -
                                    Volume State: online
                                     Volume Type: RW
                                    Volume Style: flex
                                              ...
                           Space Guarantee Style: volume
                       Space Guarantee in Effect: true
                                              ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- ----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

コマンド入力で**ONTAP CLI**の位置指定パラメータを使用する

ONTAP CLI の位置指定パラメータ機能を活用して、効率的にコマンドを入力することができます。あるコマンドの位置指定パラメータは、そのコマンドのヘルプで特定できます。

位置指定パラメータとは何ですか

- 位置指定パラメータは、値を指定する前にパラメータ名を指定する必要のないパラメータです。
- 位置指定パラメータは、コマンド入力に位置指定パラメータとそれ以外のパラメータを組み合わせて指定できます。ただし、コマンド内の他の位置指定パラメータとの相対的な順序（の出力）に従っている必要

があり `**_command_name ?_**`ます。

- 位置指定パラメータは、必須パラメータの場合とオプションパラメータの場合があります。
- あるパラメータが 1 つのコマンドでは位置指定パラメータで、別のコマンドでは位置指定パラメータでない場合もあります。

> 位置指定パラメータ機能をスクリプトで使用することは、特に位置指定パラメータがオプションパラメータである場合や、位置指定パラメータの前にオプションパラメータを指定する場合には推奨されません。

位置指定パラメータを特定する

位置指定パラメータは、コマンドの出力で特定できます **_command_name ?_**。位置指定パラメータは、次のいずれかの形式で、パラメータ名が角かっこで囲まれています。

- [*-parameter_name*] `*parameter_value*`に、必須の位置指定パラメータを示します。
- [][*-parameter_name* `*parameter_value*`に、オプションの位置指定パラメータを示します。

たとえば、次の出力では **_command_name ?_**、パラメータは該当するコマンドの位置指定パラメータです。

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

ただし、次の出力では、パラメータは該当するコマンドの位置指定パラメータではありません。

- `-lif <lif-name>`
- `[-lif <lif-name>]`

位置指定パラメータの使用例

次の出力例では **_volume create ?_**、コマンドの3つのパラメータ（、、） `-aggregate`が位置指定パラメータであることが示されています `-volume -size`。

```
cluster1::> volume create ?
   -vserver <vserver name>                 Vserver Name
    [-volume] <volume name>                Volume Name
    [-aggregate] <aggregate name>          Aggregate Name
   [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
   [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
   [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
   [ -policy <text> ]                      Export Policy
   [ -user <user name> ]                   User ID
   ...
   [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
   [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
   ...
```

次の例では `volume create`、位置指定パラメータ機能を使用せずにコマンドを指定しています。

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

次の例では、位置指定パラメータ機能を使用して効率的にコマンドを入力しています。位置指定パラメータとそれ以外のパラメータの両方を使用してコマンドを実行 `volume create`し、位置指定パラメータの値はパラメータ名なしで指定されます。位置指定パラメータは、の出力と同じ順序で指定されます `volume create ?`。つまり、の値はの値の前に指定され `-aggregate`、の値 `-volume`の前に指定され `-size`ます。

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

ONTAP CLIのマニュアルページへのアクセス方法

ONTAPのマニュアル（マニュアル）ページでは、ONTAP CLIコマンドの使用方法が説明されています。これらのページはコマンドラインから入手でき、リリース固有の_コマンドリファレンス_でも公開されています。

ONTAPのコマンドラインで、コマンドを使用し `man <command_name>`て、指定したコマンドのマニュアルページを表示します。コマンド名を指定しない場合は、マニュアルページインデックスが表示されます。コマンドを使用すると、コマンド自体に関する情報を表示 `man`できます `man man`。マニュアルページを終了するには、と入力し `q`ます。

ご使用のリリースで使用できる管理者レベルおよびアドバンスレベルのONTAPコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ONTAP CLIセッションの記録と記録されたセッションの管理

CLIセッションを指定した名前とサイズの上限を指定してファイルに記録し、FTPまたはHTTPの保存先にアップロードできます。以前に記録したCLIセッションのファイルを表示または削除することもできます。

CLIセッションの記録

CLIセッションの記録は、記録を停止するかCLIセッションを終了するか、ファイルが指定されたサイズ制限に達すると終了します。デフォルトのファイルサイズの上限は1MBです。ファイルサイズの上限は2GBです。

CLIセッションを記録すると、問題をトラブルシューティングして詳細情報を保存する場合や、特定の時点でのスペース使用量の永続的なレコードを作成する場合などに役立ちます。

手順

1. 現在のCLIセッションのファイルへの記録を開始します。

   ```
   system script start
   ```

   の詳細については `system script start`、を"ONTAPコマンド リファレンス"参照してください。

   ONTAPは、指定したファイルへのCLIセッションの記録を開始します。

2. CLIセッションを続行します。
3. 終了したら、セッションの記録を停止します。

   ```
   system script stop
   ```

   の詳細については `system script stop`、を"ONTAPコマンド リファレンス"参照してください。

   ONTAPはCLIセッションの記録を停止します。

CLIセッションのレコードの管理用コマンド

CLIセッションのレコードを管理するには、コマンドを使用し `system script`ます。

状況	使用するコマンド
指定したファイルへの現在のCLIセッションの記録を開始します。	`system script start`
現在のCLIセッションの記録を停止する	`system script stop`
CLIセッションのレコードに関する情報を表示する	`system script show`

状況	使用するコマンド
CLIセッションのレコードをFTPまたはHTTPの宛先にアップロードする	`system script upload`
CLIセッションのレコードを削除する	`system script delete`

関連情報

"ONTAPコマンド リファレンス"

CLIセッションの自動タイムアウト時間の管理用コマンド

タイムアウト値は、CLIセッションが自動的に終了するまでアイドル状態を維持する時間を指定します。CLIタイムアウト値はクラスタ全体に適用されます。つまり、クラスタ内のすべてのノードで同じCLIタイムアウト値が使用されます。

デフォルトでは、CLIセッションの自動タイムアウト時間は30分です。

CLIセッションの自動タイムアウト時間を管理するには、コマンドを使用し `system timeout`ます。

状況	使用するコマンド
CLIセッションの自動タイムアウト時間を表示します。	`system timeout show`
CLIセッションの自動タイムアウト時間を変更する	`system timeout modify`

関連情報

"ONTAPコマンド リファレンス"

クラスタ管理（クラスタ管理者のみ）

ONTAPクラスタのノードレベルの詳細を表示する

ノード名、ノードが正常かどうか、およびノードがクラスタへの参加条件を満たしているかどうかを確認できます。advanced権限レベルでは、ノードにイプシロンが設定されているかどうかも表示できます。

手順

1. クラスタ内のノードに関する情報を表示するには、コマンドを使用し `cluster show`ます。

   ノードにイプシロンが設定されているかどうかを出力に表示するには、advanced権限レベルでコマンドを実行します。

   の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。

クラスタ内のノードを表示する例

次の例は、4ノードクラスタ内のすべてのノードに関する情報を表示します。

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

次の例は、 advanced 権限レベルで「 node1 」という名前のノードに関する詳細情報を表示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

ONTAPクラスタレベルの詳細の表示

クラスタの一意の識別子（UUID）、名前、シリアル番号、場所、連絡先情報を表示できます。

手順

1. クラスタの属性を表示するには、コマンドを使用し `cluster identity show`ます。

クラスタ属性を表示する例

次の例は、クラスタの名前、シリアル番号、場所、および連絡先情報を表示します。

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

の詳細については `cluster identity show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPクラスタ属性を変更します。

クラスタ名、場所、および連絡先情報などのクラスタ属性を必要に応じて変更できます。

タスクの内容

クラスタの作成時に設定されたクラスタの UUID は変更できません。

手順

1. クラスタの属性を変更するには、コマンドを使用し `cluster identity modify`ます。

   `-name`パラメータは、クラスタの名前を指定します。およびでクラスタ名を指定する際のルールの詳細については、`link:https://docs.netapp.com/us-en/ontap-cli/cluster-identity-modify.html["ONTAPコマンド リファレンス"^]`を参照してください `cluster identity modify`。

   `-location`パラメータは、クラスタの場所を指定します。

   パラメータは、 `-contact`名前やEメールアドレスなどの連絡先情報を指定します。

クラスタ名の変更例

次のコマンドは、現在のクラスタ名（「 cluster1 」）を「 cluster2 」に変更します。

```
cluster1::> cluster identity modify -name cluster2
```

ONTAPクラスタリングのレプリケーションステータスを表示する

クラスタレプリケーションリングのステータスを表示して、クラスタ全体の問題の診断に役立てることができます。クラスタに問題が発生している場合は、トラブルシューティングの際にサポート担当者からこのタスクを実行するように依頼されることがあります。

手順

1. クラスタレプリケーションリングのステータスを表示するには、advanced権限レベルでコマンドを使用し `cluster ring show`ます。

クラスタリングレプリケーションステータスの表示例

次の例は、node0という名前のノードのVLDBレプリケーションリングのステータスを表示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

の詳細については `cluster ring show`、を"ONTAPコマンド リファレンス"参照してください。

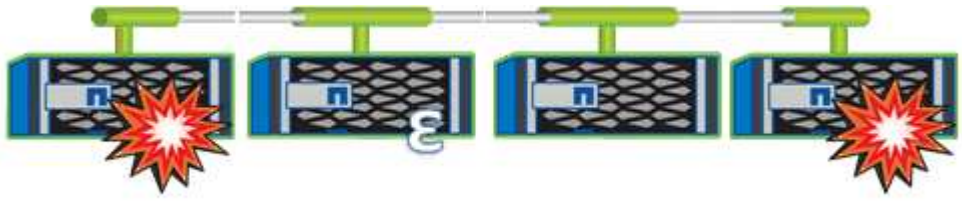
クォーラムとイプシロンを使用した**ONTAP**クラスタの健全性評価

クォーラムとイプシロンは、クラスタの健全性と機能の重要な指標であり、通信や接続に関する潜在的な課題にクラスタがどのように対処するかを示します。

_Quorum _ は、クラスタが完全に機能するための前提条件です。クラスタがクォーラムを構成している場合は、過半数のノードが正常で、相互に通信できます。クォーラムが失われると、クラスタは通常のクラスタ処理を実行できなくなります。すべてのノードがまとめてデータの単一のビューを共有するため、一度にクォーラムを持つことができるノードの集まりは1つだけです。したがって、通信していない2つのノードが異なる方法でデータを変更できる場合、データを単一のデータビューに調整することはできなくなります。

クラスタ内の各ノードはノードマスターを選出する投票プロトコルに属しており、残りの各ノードは *secondary_* です。マスターノードは、クラスタ全体で情報を同期する役割を果たします。形成されたクォーラムは継続的な投票によって維持されます。マスターノードがオフラインになり、クラスタがクォーラムに参加している場合は、オンラインのノードによって新しいマスターが選出されます。

ノード数が偶数のクラスタの場合は同票となる可能性があるため、 1 つのノードに _epsilon _ という名前の投票荷重が追加で設定されます。大規模なクラスタの同じ数のノード間で接続障害が発生した場合、すべてのノードが正常であることを前提として、イプシロンが設定されたノードのグループがクォーラムを維持します。たとえば、次の図は、2つのノードで障害が発生した4ノードクラスタを示しています。ただし、サバイバーノードの1つにイプシロンが設定されているため、正常なノードが過半数ではないにもかかわらず、クラスタはクォーラムを維持します。



クラスタが作成されると、自動的に最初のノードにイプシロンが割り当てられます。イプシロンを保持しているノードが正常な状態にならなくなった場合、ハイアベイラビリティパートナーをテイクオーバーした場合、またはハイアベイラビリティパートナーにテイクオーバーされた場合、イプシロンは別のHAペアの正常なノードに自動的に再割り当てされます。

ノードをオフラインにすると、クラスタがクォーラムを維持できるかどうかに影響することがあります。そのため、クラスタのクォーラムが失われたり、あと1つの停止によってクォーラムが失われる処理を実行しようとすると、ONTAPで警告メッセージが表示されます。クォーラムに関する警告メッセージを無効にするには、advanced権限レベルでコマンドを使用し `cluster quorum-service options modify`ます。の詳細については `cluster quorum-service options modify`、を"ONTAPコマンド リファレンス"参照してください。

一般に、クラスタのノード間で信頼性の高い接続が確立されていれば、小規模なクラスタよりも大規模なクラスタの方が安定します。半分のノードの過半数とイプシロンを組み合わせたクォーラムの要件は、2ノードのクラスタよりも24ノードのクラスタで簡単に管理できます。

2ノードクラスタには、クォーラムの維持に固有の課題がいくつかあります。2 ノードクラスタでは、どちらのノードにもイプシロンが設定されていない *cluster ha_* を使用します。代わりに、両方のノードを継続的にポーリングすることで、一方のノードで障害が発生した場合にデータに対する読み取り / 書き込みのフルアクセスと、論理インターフェイスおよび管理機能へのアクセスが許可されます。

ONTAPクラスタ内のシステムボリュームのストレージ容量利用率の表示

システムボリュームとは、ファイルサービスや監査ログのメタデータなど、特別なメタデータを格納する FlexVol です。クラスタ内のストレージの使用をすべて把握できるように、システムボリュームはクラスタ内で表示することができます。

システムボリュームはクラスタ管理サーバ（管理 SVM ）によって所有され、ファイルサービスの監査が有効になっている場合に自動的に作成されます。

コマンドを使用してシステムボリュームを表示でき `volume show`ますが、それ以外のほとんどのボリューム処理は実行できません。たとえば、コマンドを使用してシステムボリュームを変更することはできません `volume modify`。

次の例は、管理SVM上にある4つのシステムボリュームを示しています。これらのボリュームは、クラスタでデータSVMのファイルサービスの監査が有効になっているときに自動的に作成されたものです。

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

ノードの管理

ONTAPクラスタへのノードの追加

クラスタを作成したら、ノードを追加してクラスタを拡張できます。一度に追加できるノードは1つだけです。

開始する前に

- 複数ノードクラスタにノードを追加する場合は、クラスタ内のすべての既存ノードが正常である必要があります（で確認可能 `cluster show`）。の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。
- 2ノードスイッチレスクラスタにノードを追加する場合は、NetAppでサポートされるクラスタスイッチを使用して、2ノードスイッチレスクラスタをスイッチ接続クラスタに変換する必要があります。

  スイッチレスクラスタ機能は、2ノードクラスタでのみサポートされます。
- シングルノードクラスタに2つ目のノードを追加する場合は、2つ目のノードがインストールされていて、クラスタネットワークが設定されている必要があります。
- クラスタでSPの自動設定が有効になっている場合、追加するノードが指定したサブネットを使用してSPを自動的に設定できるように、SP用に指定したサブネットに使用可能なリソースがある必要があります。
- 新しいノードのノード管理LIFに関する次の情報を収集しておく必要があります。
  - ポート
  - IPアドレス
  - ネットマスク

- デフォルトゲートウェイ

タスクの内容

ノードは、HAペアを形成できるように偶数である必要があります。クラスタへのノードの追加を開始したら、その処理を完了する必要があります。別のノードの追加を開始するには、そのノードがクラスタに属している必要があります。

手順

1. クラスタに追加するノードに電源を入れます。

   ノードがブートし、ノードのセットアップウィザードがコンソールで起動されます。

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.

   Enter the node management interface port [e0M]:
   ```

2. ノードのセットアップウィザードを終了します。 `exit`

   ノードのセットアップウィザードが終了し、セットアップタスクが完了していないという警告がログインプロンプトに表示されます。

   の詳細については `exit`、を"ONTAPコマンド リファレンス"参照してください。

3. ユーザ名を使用してadminアカウントにログインし `admin`ます。
4. クラスタセットアップウィザードを開始します。

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

セットアップGUIを使用したクラスタのセットアップの詳細については、"ノード管理ドキュメント"。の詳細については `cluster setup`、を"ONTAPコマンド リファレンス"参照してください。

5. CLIを使用してこのタスクを完了するには、Enterキーを押します。新しいクラスタを作成するか既存のクラスタに参加するかを確認するメッセージが表示されたら、と入力し `**join**`ます。

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

新しいノードで実行されているONTAPのバージョンが既存のクラスタで実行されているバージョンと異なる場合は、エラーが報告され `System checks Error: Cluster join operation cannot be performed at this time`ます。これは想定される動作です。続行するには、クラスタ内の既存のノードからadvanced権限レベルでコマンドを実行し `cluster add-node -allow-mixed-version-join true -cluster-ips <IP address> -node -names <new_node_name>`ます。

6. プロンプトに従ってノードをセットアップし、クラスタに追加します。
   - プロンプトのデフォルト値を受け入れるには、Enterキーを押します。
   - プロンプトに独自の値を入力するには、値を入力してEnterキーを押します。
7. 追加するノードごとに前述の手順を繰り返します。

終了後

クラスタにノードを追加したら、各HAペアのストレージフェイルオーバーを有効にする必要があります。

関連情報

- "ONTAPソフトウェアのアップグレードでサポートされるバージョンの混在クラスタ"
- "クラスタ追加-ノード"

ONTAPクラスタからノードを削除する

クラスタから不要なノードを一度に1つずつ削除できます。ノードを削除したら、フェイルオーバーパートナーも削除する必要があります。ノードを削除すると、そのノードのデータはアクセスできなくなるか、消去されます。

開始する前に

クラスタからノードを削除するには、次の条件を満たしている必要があります。

- クラスタ内のノードのうち半数を上回るノードが健全である必要があります。
- すべてのデータ、ボリューム、およびルート以外のアグリゲートがノードから再配置または削除されている。
  - 削除するノード上のすべてのデータを退避しておく必要があります。これには以下が含まれ"暗号化されたボリュームからのデータのパージ"ます。
  - ルート以外のボリュームはすべて、ノードが所有するアグリゲートに含まれている"移動しました"必要があります。
  - ルート以外のすべてのアグリゲートがノードから作成されている"削除済み"。
- すべてのLIFとVLANがノードから再配置または削除されている。
  - データLIFはノードまたは"再配置済み"ノードから実行されている"削除済み"必要があります。
  - クラスタ管理LIFがノードから削除され"再配置済み"、ホームポートが変更されている。
  - すべてのクラスタ間LIFがになっている"削除済み"。クラスタ間LIFを削除する際に表示される警告は無視してかまいません。
  - ノード上のすべてのVLANがになっている"削除済み"。
- ノードがフェイルオーバー関係に参加していません。
  - ノードに対してストレージフェイルオーバーが実行されている必要があり"無効"ます。
  - すべてのLIFフェイルオーバールールでノードのポートを削除しておき"変更済み"ます。
- ノードが連邦情報処理標準（FIPS）ディスクまたは自己暗号化ディスク（SED）を所有している場合は"ディスク暗号化が削除されました"、ディスクを非保護モードに戻します。
  - 必要な場合もあり"FIPS ドライブまたは SED を完全消去します"ます。
- 削除するノードにLUNがある場合は、ノードを削除する前に実行する必要があります"選択的LUNマップ（SLM）のレポートノードリストを変更します"。

  SLMのレポートノードリストからノードとそのHAパートナーを削除しないと、LUNを含むボリュームを別のノードに移動しても、そのノードで以前に実行していたLUNへのアクセスが失われる可能性があります。

AutoSupportメッセージを発行して、ノードを削除中であることをNetAppテクニカルサポートに通知することを推奨します。

`cluster unjoin`ONTAPの自動アップグレードの実行中は、、、 `node rename`などの処理を実行しないで `cluster remove-node`ください。

タスクの内容

- バージョンが混在したクラスタを実行している場合は、ONTAP 9以降のadvanced権限のコマンドを使用して、バージョンが低い最後のノードを削除できます。3：
  - ONTAP 9 .3： `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9 .4以降： `cluster remove-node -skip-last-low-version-node-check`
- 4ノードクラスタから2つのノードを分離すると、残りの2つのノードでクラスタHAが自動的に有効になります。

クラスタからノードを削除する前に、ノードに接続されているすべてのディスクのすべてのシステムデータとユーザデータにユーザがアクセスできないようにする必要があります。ノードをクラスタから誤って分離した場合は、NetAppサポートにリカバリのオプションについて問い合わせてください。

手順

1. 権限レベルをadvancedに変更します。

```
set -privilege advanced
```

2. クラスタのノードにイプシロンが設定されているかどうかを確認します。

```
cluster show -epsilon true
```

3. イプシロンが設定されているクラスタ ノードを削除する場合は、削除しないノードにイプシロンを移動します。
   a. 削除するノードからイプシロンを移動します。

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

   b. 削除しないノードにイプシロンを移動します。

```
cluster modify -node <node_name> -epsilon true
```

4. 現在のマスター ノードを特定します。

```
cluster ring show
```

マスターノードは、 `vldb`、、 `vifmgr`、 `bcomd`などのプロセスを保持するノードです `mgmt crs`。

5. 削除するノードが現在のマスターノードである場合は、クラスタ内の別のノードがマスターノードとして選出されるようにします。

   a. 現在のマスターノードをクラスタに参加できないようにします。

   ```
   cluster modify -node <node_name> -eligibility false
   ```

   そのため、次の手順で適格性が回復するまで、ノードはunhealthyとマークされます。マスターノードが参加資格を得られなくなると、残りのノードの1つがクラスタクォーラムによって新しいマスターとして選出されます。

   b. 以前のマスターノードを再びクラスタに参加できるようにします。

   ```
   cluster modify -node <node_name> -eligibility true
   ```

6. 削除するノードとは別のノードのリモートノード管理LIFまたはクラスタ管理LIFにログインします。

7. クラスタからノードを削除します。

ONTAPバージョン	使用するコマンド
ONTAP 9.3	`cluster unjoin`

ONTAP 9.4以降	ノード名を使用：
	`cluster remove-node -node <node_name>`
	ノードIPを使用：
	`cluster remove-node -cluster_ip <node_ip>`

   バージョンが混在したクラスタでバージョンが低い最後のノードを削除する場合は、次のコマンドでパラメータを使用し `-skip-last-low-version-node-check`ます。

   次の情報が表示されます。

   - また、ノードのフェイルオーバーパートナーをクラスタから削除する必要があります。
   - ノードを削除したあと、クラスタに再追加する前に、ブートメニューオプション[（4）Clean configuration and initialize all disks]またはオプション[（9）Configure Advanced Drive Partitioning]を使用して、ノードの設定を消去してすべてのディスクを初期化する必要があります。

ノードを削除する前に対処する必要がある条件がある場合は、エラーメッセージが生成されます。メッセージの内容は、たとえば、ノードに削除が必要な共有リソースがある、ノードがクラスタHA構成またはストレージフェイルオーバー構成に含まれているため無効にする必要があるなどの場合があります。

ノードがクォーラムマスターの場合、クラスタは一時的に失われてからクォーラムに戻ります。クォーラムが失われるのは一時的であり、データの操作には影響しません。

8. エラーメッセージにエラー状態が示された場合は、その状態に対処し、コマンドまたは `cluster unjoin`コマンドを再実行し `cluster remove-node`ます。

   ノードは、クラスタから削除されると自動的にリブートされます。

9. ノードを転用する場合は、ノードの設定を消去し、すべてのディスクを初期化します。
   a. ブートプロセス中に、プロンプトが表示されたらCtrl+Cキーを押してブートメニューを表示します。
   b. ブートメニューオプション[（4）Clean configuration and initialize all disks]を選択します。
10. admin権限レベルに戻ります。

```
set -privilege admin
```

11. クラスタからフェイルオーバーパートナーを削除するには、上記の手順を繰り返します。

関連情報

- "クラスタ削除ノード"

Webブラウザを使用して**ONTAP**ノードログ、コアダンプ、**MIB**ファイルにアクセスする

サービスプロセッサインフラ(spi）Webサービスはデフォルトで有効になっており、クラスタ内のノードのログファイル、コアダンプファイル、MIBファイルにWebブラウザからアクセスできます。ノードが停止しても（パートナーにテイクオーバーされていれば）ファイルに引き続きアクセスできます。

開始する前に

- クラスタ管理LIFが稼働している必要があります。

  Webサービスには、クラスタまたはノードの管理LIFを使用してアクセスできます spi。ただし、クラスタ管理LIFを使用することを推奨します。

```
`network interface show`コマンドは、クラスタ内のすべての
LIFのステータスを表示します。
```

  の詳細については network interface show、を"ONTAPコマンド リファレンス"参照してください。

- Webサービスにアクセスするにはローカルユーザアカウントを使用する必要があり `spi`ます。ドメインユーザアカウントはサポートされません。

- ユーザーアカウントに `admin`ロール（ `spi`デフォルトではウェブサービスにアクセスできませんが、アクセス制御ロールに `spi`ウェブサービス。

  `vserver services web access show`コマンドは、どのロールにどのWebサービスへのアクセスが許可されているかを表示します。

- 使用していない場合 `admin`ユーザーアカウント（ `http`デフォルトのアクセス方法を使用する場合、ユーザーアカウントは `http`アクセス方法。

  `security login show`コマンドは、ユーザアカウントのアクセス方法とログイン方法、およびアクセス制御ロールを表示します。

  の詳細については `security login show`、を"ONTAPコマンド リファレンス"参照してください。

- セキュアなWebアクセスにHTTPSを使用する場合は、SSLを有効にし、デジタル証明書をインストールする必要があります。

  `system services web show`コマンドは、クラスタレベルのWebプロトコルエンジンの設定を表示します。

タスクの内容

`spi`Webサービスはデフォルトで有効になっており、サービスは手動で無効にすることができ（`vserver services web modify -vserver * -name spi -enabled false`ます）。

その `admin`役割には、 `spi`デフォルトではウェブサービスであり、アクセスは手動で無効にすることができます（`services web access delete -vserver *cluster_name* -name spi -role admin`）。

手順

1. Webブラウザで、次のいずれかの形式でWebサービスURLを指定し `spi`ます。

   - `http://`*`cluster-mgmt-LIF`*`/spi/`
   - `https://`*`cluster-mgmt-LIF`*`/spi/`

   `cluster-mgmt-LIF`は、クラスタ管理LIFのIPアドレスです。

2. ブラウザにプロンプトが表示されたら、ユーザアカウントとパスワードを入力します。

   アカウントが認証されると、クラスタ内の各ノードの、 `/mroot/etc/crash/`および `/mroot/etc/mib/`ディレクトリへのリンクがブラウザに表示されます `/mroot/etc/log/`。

ブートメニューまたはブート環境のプロンプトでハングしているノードには、システムコンソール（ *serial console*） 経由でのみアクセスできます。ノードのシステムコンソールには、ノードの SP またはクラスタへの SSH 接続からアクセスできます。

タスクの内容

SP と ONTAP はどちらもシステムコンソールにアクセスするためのコマンドを提供しています。ただし、SP からはそのノードのシステムコンソールにしかアクセスできません。クラスタから（ローカルノードを除く）クラスタ内の他のノードのシステムコンソールにアクセスできます。

手順

1. ノードのシステムコンソールにアクセスします。

使用する環境	入力するコマンド
ノードの SP CLI	`system console`
ONTAP CLI	`system node run-console`

2. プロンプトが表示されたら、システムコンソールにログインします。
3. システムコンソールを終了するには、 Ctrl+D を押します

システムコンソールへのアクセスの例

次の例は、「SP node2」プロンプトでコマンドを入力した結果を示して `system console`います。システムコンソールに、 node2 がブート環境のプロンプトでハングしていることが示されています。 `boot_ontap`コンソールでコマンドを入力して、ノードをONTAPでブートします。続いて Ctrl+D を押してコンソールを終了し、 SP に戻ります。

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

（Ctrl+Dを押してシステムコンソールを終了します。）

```
Connection to 123.12.123.12 closed.
SP node2>
```

次の例は、ブート環境のプロンプトでハングしているnode2のシステムコンソールにアクセスするためにONTAPからコマンドを入力した結果を示して `system node run-console`います。 `boot_ontap`コンソールでコマンドを入力してnode2をONTAPでブートします。続いて Ctrl+D を押してコンソールを終了し、ONTAP に戻ります。

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

（Ctrl+Dを押してシステムコンソールを終了します。）

```
Connection to 123.12.123.12 closed.
cluster1::>
```

ONTAPノードのルートボリュームとルートアグリゲートを管理します。

ノードのルートボリュームは、工場出荷時またはセットアップソフトウェアによってインストールされたFlexVol volumeです。システムファイル、ログファイル、コアファイル用に予約されています。ディレクトリ名はで `/mroot`、テクニカルサポートからのみシステムシェルからアクセスできます。ノードのルートボリュームの最小サイズは、プラットフォームモデルによって異なります。

ノードのルートボリュームとルートアグリゲートに関するルールの概要

ノードのルートボリュームには、そのノードの特別なディレクトリとファイルが格納されています。ルートアグリゲートにはルートボリュームが含まれます。ノードのルートボリュームとルートアグリゲートには、いくつかのルールが適用されます。

- ノードのルートボリュームには次のルールが適用されます。
  - テクニカルサポートから指示がないかぎり、ルートボリュームの構成またはコンテンツを変更しない

でください。

- ユーザデータはルートボリュームに格納しないでください。

  ユーザデータをルートボリュームに格納すると、HAペアのノード間でのストレージのギブバックに時間がかかります。

- ルートボリュームを別のアグリゲートに移動できます。を参照して [relocate-root]

- ルートアグリゲートは、ノードのルートボリューム専用です。

  ONTAPでは、ルートアグリゲートに他のボリュームを作成することはできません。

"NetApp Hardware Universe"

ノードのルートボリュームのスペースを解放する

ノードのルートボリュームがフルまたはほぼフルになると、警告メッセージが表示されます。ルートボリュームがいっぱいになると、ノードは正常に動作しません。ノードのルートボリュームのスペースを解放するには、コアダンプファイル、パケットトレースファイル、およびルートボリュームのSnapshotを削除します。

手順

1. ノードのコアダンプファイルとその名前を表示します。

   ```
   system node coredump show
   ```

2. 不要なコアダンプファイルをノードから削除します。

   ```
   system node coredump delete
   ```

3. ノードシェルにアクセスします。

   system node run -node *nodename*

   `*nodename*`は、ルートボリュームのスペースを解放するノードの名前です。

4. ノードシェルからノードシェルのadvanced権限レベルに切り替えます。

   priv set advanced

5. ノードのパケットトレースファイルをノードシェルから表示および削除します。

   a. ノードのルートボリューム内のすべてのファイルを表示します。

      ls /etc

   b. (`*.trc`ノードのルートボリュームにパケットトレースファイルがある場合は、それらを個別に削除します。

      rm /etc/log/packet_traces/*file_name.trc*

6. ノードシェルからノードのルートボリュームSnapshotを特定して削除します。

   a. ルートボリューム名を特定します。

vol status

ルートボリュームは、コマンド出力の「Options」列に「root」と表示され `vol status`ます。

次の例では、ルートボリュームはです `vol0`。

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

a. ルートボリュームのSnapshotを表示します。

   `snap list root_vol_name`

b. 不要なルートボリュームのSnapshotを削除します。

   `snap delete root_vol_namesnapshot_name`

7. ノードシェルを終了してクラスタシェルに戻ります。

   exit

新しいアグリゲートへのルートボリュームの再配置

ルートの交換手順では、現在のルートアグリゲートを、システムを停止することなく別のディスクセットに移行します。

タスクの内容

ルートボリュームを再配置するには、ストレージフェイルオーバーを有効にする必要があります。フェイルオーバーを有効にするには、コマンドを使用し `storage failover modify -node *nodename* -enable true`ます。

次のシナリオでは、ルートボリュームの場所を新しいアグリゲートに変更できます。

- ルートアグリゲートが希望するディスク上にない場合
- ノードに接続されているディスクの配置を変更する場合
- EOSディスクシェルフを交換する場合

手順

1. 権限レベルをadvancedに設定します。

   set privilege advanced

2. ルートアグリゲートを再配置します。

   system node migrate-root -node *nodename* -disklist *disklist* -raid-type *raid-type*

- * -node *

  移行するルートアグリゲートを所有しているノードを指定します。

- *-disklist *

  新しいルートアグリゲートを作成するディスクのリストを指定します。すべてのディスクはスペアであり、同じノードが所有している必要があります。必要なディスクの最小数は、RAIDタイプによって異なります。

- * -raid-type *

  ルートアグリゲートのRAIDタイプを指定します。デフォルト値はです `raid-dp`。

3. ジョブの進捗状況を監視します。

   job show -id *jobid* -instance

結果

すべての事前確認に成功すると、ルートボリューム交換ジョブが開始されてコマンドが終了します。ノードが再起動することを想定します。

関連情報

- "storage failover modify"

メンテナンスまたはトラブルシューティングのための**ONTAP**ノードの起動または停止

メンテナンスまたはトラブルシューティングの目的で、ノードの起動または停止が必要になることがあります。これは、ONTAP CLI、ブート環境プロンプト、またはSP CLIから実行できます。

SP CLIのコマンドまたは `system power cycle`を使用し `system power off`てノードの電源をオフにするか再投入すると、ノードが誤ってシャットダウンされる（*dirty shutdown*）ことがあります。この方法は、`ONTAP`のコマンドを使用した正常なシャットダウンの代わりにはなりません。 `system node halt`

システムプロンプトでノードをリブートする

ノードは、システムプロンプトから通常モードでリブートできます。ノードは、PC CompactFlashカードなどのブートデバイスからブートするように設定されています。

手順

1. クラスタにノードが4つ以上ある場合は、リブートするノードにイプシロンが設定されていないことを確認します。

   a. 権限レベルをadvancedに設定します。

      set -privilege advanced

   b. イプシロンが設定されているノードを特定します。

cluster show

次の例では 'node1 にイプシロンが設定されています

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

a. リブートするノードにイプシロンが設定されている場合は、そのノードからイプシロンを削除します。

cluster modify -node *node_name* -epsilon false

b. 稼働したままにする別のノードにイプシロンを割り当てます。

cluster modify -node *node_name* -epsilon true

c. admin権限レベルに戻ります。

set -privilege admin

2. コマンドを使用し `system node reboot`て、ノードをリブートします。

パラメータを指定しない場合、 `-skip-lif-migration`リブートの前に、別のノードへのデータおよびクラスタ管理LIFの同期的移行が試行されます。LIFの移行が失敗した場合、またはタイムアウトした場合、リブートプロセスは中止され、LIFの移行の失敗を示すエラーがONTAPに表示されます。

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

ノードのリブートプロセスが開始されます。ONTAPログインプロンプトが表示され、リブートプロセスが完了したことが示されます。

ブート環境プロンプトでのブート**ONTAP**

ノードのブート環境プロンプトから、ONTAPの現在のリリースまたはバックアップリリースをブートできます。

手順

1. ストレージシステムプロンプトから、コマンドを使用してブート環境のプロンプトにアクセスします `system node halt`。

ストレージシステムコンソールにブート環境のプロンプトが表示されます。

2. ブート環境のプロンプトで、次のいずれかのコマンドを入力します。

ブート対象	入力するコマンド
ONTAPの現在のリリース	`boot_ontap`
ブートデバイスからのONTAPプライマリイメージ	`boot_primary`
ブートデバイスのONTAPバックアップイメージ	`boot_backup`

使用するイメージが不明な場合は、最初にを使用して `boot_ontap`ください。

ノードをシャットダウンします。

ノードが応答しなくなった場合や、サポート担当者からトラブルシューティング対応の一環として実行するように指示された場合は、ノードをシャットダウンできます。

手順

1. クラスタのノードが4つ以上の場合は、シャットダウンするノードにイプシロンが設定されていないことを確認します。

   a. 権限レベルをadvancedに設定します。

      `set -privilege advanced`

   b. イプシロンが設定されているノードを特定します。

      `cluster show`

      次の例では 'node1 にイプシロンが設定されています

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   a. シャットダウンするノードにイプシロンが設定されている場合は、そのノードからイプシロンを削除します。

      `cluster modify -node node_name -epsilon false`

   b. 稼働したままにする別のノードにイプシロンを割り当てます。

```
cluster modify -node node_name -epsilon true
```

c. admin権限レベルに戻ります。

```
set -privilege admin
```

2. コマンドを使用し `system node halt`て、ノードをシャットダウンします。

パラメータを指定しない場合、 `-skip-lif-migration`シャットダウンの前に、別のノードへのデータおよびクラスタ管理LIFの同期的移行が試行されます。LIFの移行が失敗した場合、またはタイムアウトした場合、シャットダウンプロセスは中止され、LIFの移行の失敗を示すエラーがONTAPに表示されます。

パラメータを両方使用すると、シャットダウン時にコアダンプを手動でトリガーできます `-dump`。

次の例は、ハードウェアのメンテナンスのために「 node1 」という名前のノードをシャットダウンします。

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

ブートメニューを使用した**ONTAP**ノードの管理

ブートメニューを使用して、ノードの設定の問題の修正、管理パスワードのリセット、ディスクの初期化、ノード構成のリセット、およびノード構成情報のブートデバイスへのリストアを行うことができます。

HAペアでを使用している場合は"SAS ドライブまたは NVMe ドライブの暗号化（ SED 、 NSE 、 FIPS ）"、システムを初期化する前に、HAペア内のすべてのドライブに対応するトピックの手順に従う必要があります"FIPSドライブまたはSEDを非保護モードに戻す"（ブートオプション4または9）。これを行わないと、ドライブを転用した場合にデータが失われる可能性があります。

手順

1. システムプロンプトでコマンドを使用してノードをリブートし、ブートメニューにアクセスし `system node reboot`ます。

ノードのリブートプロセスが開始されます。

2. リブートプロセス中にプロンプトが表示されたら、Ctrl+Cキーを押してブートメニューを表示します。

ノードに次のブートメニューオプションが表示されます。

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

ブートメニューオプション[（2）Boot without /etc/rc]は廃止され、システムには影響しません。

3. 対応する番号を入力して、次のいずれかのオプションを選択します。

目的	選択するオプション
通常モードでノードを引き続きブートする	1）ノーマルブート
ノードのパスワードを変更しますこれは 'admin' アカウント・パスワードでもあります	3)パスワードの変更

目的	選択するオプション
ノードのディスクを初期化し、ノードのルートボリュームを作成	4）設定を消去し、すべてのディスクを初期化 このメニューオプションを選択すると、ノードのディスク上のすべてのデータが消去され、ノード構成が工場出荷時のデフォルト設定にリセットされます。 このメニュー項目は、ノードがクラスタから削除され（分離され）、別のクラスタに追加されていない場合にのみ選択してください。 内蔵または外付けのディスクシェルフがあるノードの場合は、内蔵ディスクのルートボリュームが初期化されます。内蔵ディスクシェルフがない場合は、外付けディスクのルートボリュームが初期化されます。 初期化するノードにルートデータのパーティショニング用にパーティショニングされたディスクがある場合は、ノードを初期化する前にディスクのパーティショニングを解除する必要があります（* 9）アドバンストドライブパーティショニングの設定*およびを参照）"ディスクとアグリゲートの管理"。
アグリゲートとディスクのメンテナンス処理を実行し、アグリゲートとディスクの詳細な情報を取得する。	5）メンテナンスモードブート 保守モードを終了するには、コマンドを使用し `halt`ます。
ノードのルートボリュームからPC CompactFlashカードなどのブートデバイスに構成情報をリストア	6）バックアップ構成からフラッシュを更新 ONTAPは、一部のノード構成情報をブートデバイスに格納します。ノードがリブートすると、ブートデバイス上の情報がノードのルートボリュームに自動的にバックアップされます。ブートデバイスが破損したり交換が必要になった場合は、このメニューオプションを使用して構成情報をノードのルートボリュームからブートデバイスにリストアする必要があります。
ノードに新しいソフトウェアをインストールする	7)最初に新しいソフトウェアをインストールする ブートデバイス上のONTAPソフトウェアにルートボリュームに使用するストレージアレイのサポートが含まれていない場合は、このメニューオプションを使用して、ストレージアレイをサポートするソフトウェアのバージョンを取得してノードにインストールします。 このメニューオプションは、ONTAPソフトウェアの新しいバージョンをルートボリュームがインストールされていないノードにインストールする場合にのみ使用します。DO_not_ ONTAP をアップグレードするには ' このメニュー・オプションを使用します
ノードをリブートする	8)ノードのリブート

目的	選択するオプション

すべてのディスクのパーティショニングを解除してディスクの所有権情報を削除するか、設定を消去してディスク全体またはパーティショニングされたディスクでシステムを初期化する	9）アドバンストドライブパーティショニングの設定
	
	高度なドライブパーティショニングオプションは、ルートデータまたはルートデータデータパーティショニング用に構成されたディスクに対して追加の管理機能を提供します。ブートオプション9から以下のオプションが利用可能です。
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

ONTAPクラスタ内のノードの属性を表示する

クラスタ内の1つ以上のノードの属性（名前、所有者、場所、モデル番号、シリアル番号、ノードの稼働時間、健全性の状態、クラスタへの参加資格など）を表示できます。

手順

1. 指定したノードまたはクラスタ内のすべてのノードに関する属性を表示するには、コマンドを使用し`system node show`ます。

ノードに関する情報を表示する例

次の例は、node1に関する詳細な情報を表示します。

```
cluster1::> system node show -node node1
                            Node: node1
                           Owner: Eng IT
                        Location: Lab 5
                           Model: model_number
                   Serial Number: 12345678
                       Asset Tag: -
                          Uptime: 23 days 04:42
                NVRAM System ID: 118051205
                       System ID: 0118051205
                          Vendor: NetApp
                          Health: true
                     Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

ONTAPノードの属性を変更する

必要に応じて、ノードの属性を変更できます。変更できる属性は、ノードの所有者情報、場所情報、資産タグ、クラスタへの参加資格です。

タスクの内容

ノードのクラスタへの参加資格は、advanced権限レベルで、コマンドまたは `cluster modify`コマンドのパラメータを `system node modify`使用して変更でき `–eligibility`ます。に設定したノードは、 `false`クラスタ内で非アクティブになります。

ノードの参加資格をローカルで変更することはできません。別のノードから変更する必要があります。また、クラスタHA構成ではノード参加資格を変更することもできません。

ノード設定をリストアする場合やノードのメンテナンスが長引いている場合などを除き、ノードの参加資格はに設定しないで `false`ください。ノードにクラスタ参加資格がないと、そのノードへの SAN および NAS のデータアクセスが影響を受ける可能性があります。

手順

1. コマンドを使用し `system node modify`て、ノードの属性を変更します。

ノード属性を変更する例

次のコマンドでは、「 node1 」ノードの属性を変更します。ノードの所有者は「ジョー・スミス」に設定され、その資産タグは「 js1234 」に設定されています。

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

関連情報

- "システムノードの変更"
- "cluster modifyの追加"

ONTAPノードの名前を変更します。

ノード名は必要に応じて変更できます。

手順

1. ノードの名前を変更するには、コマンドを使用し `system node rename`ます。

   パラメータは、 `-newname`ノードの新しい名前を指定します。の詳細については `system node rename`、を"ONTAPコマンド リファレンス"参照してください。

   クラスタ内の複数のノードの名前を変更する場合は、ノードごとにこのコマンドを実行する必要があります。

   「 all 」はシステム予約名なので、ノード名を「 all 」にすることはできません。

ノード名の変更例

次のコマンドでは ' ノード名を "node1 `" から "node1a `" に変更します

```
cluster1::> system node rename -node node1 -newname node1a
```

シングルノード**ONTAP**クラスタを管理します。

シングルノードクラスタは、スタンドアロンノード上でクラスタを実行する特殊な実装です。シングルノードクラスタは冗長性を提供しないため、推奨されません。ノードが停止すると、データアクセスが失われます。

フォールトトレランスとノンストップオペレーションを実現するためには、を使用してクラスタを設定することを推奨し"ハイアベイラビリティ（HAペア）"ます。

シングルノードクラスタを構成またはアップグレードする場合は、次の点に注意してください。

- シングルノードクラスタではルートボリュームの暗号化はサポートされません。
- ノードを削除してシングルノードクラスタにする場合は、データトラフィックを処理するようにクラスタポートを変更する必要があります。そのためには、クラスタポートがデータポートになるように変更し、そのデータポートにデータLIFを作成します。
- シングルノードクラスタの場合は、ソフトウェアのセットアップ時に構成のバックアップ先を指定できます。セットアップ後、ONTAPコマンドを使用してこれらの設定を変更できます。

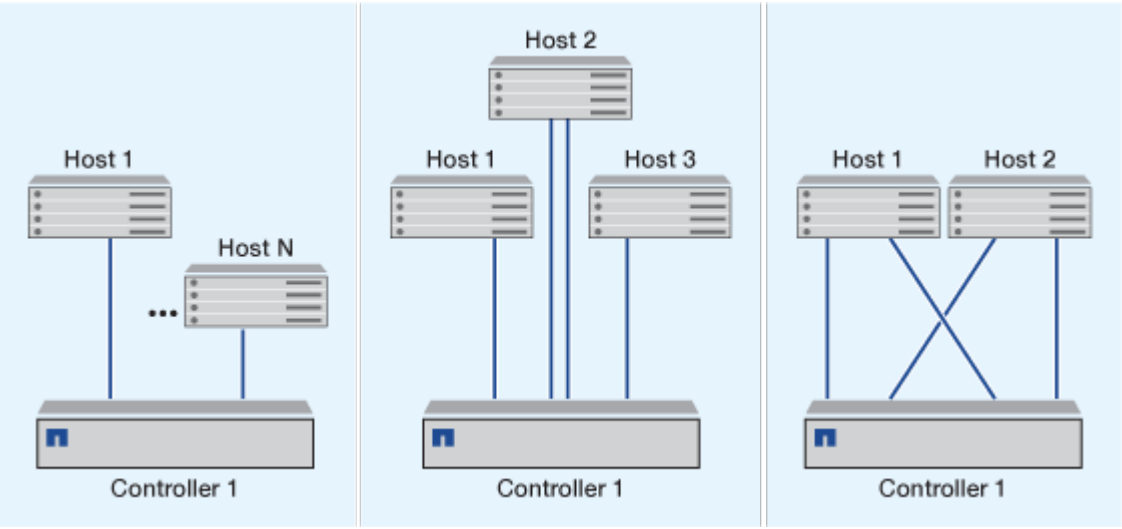
- ノードに接続するホストが複数ある場合は、各ホストでオペレーティングシステム（WindowsやLinuxなど）を設定できます。ホストからコントローラへのパスが複数ある場合は、ホストでALUAを有効にする必要があります。

シングルノードを使用する**iSCSI SAN**ホストの構成方法

iSCSI SANホストは、単一のノードに直接接続するように設定することも、1つ以上のIPスイッチを介して接続するように設定することもできます。ノードからスイッチに複数のiSCSI接続を確立できます。

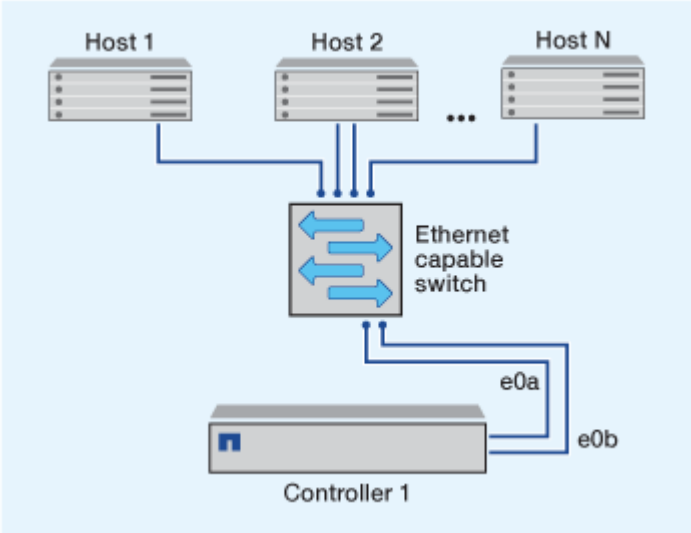
直接接続型のシングルノード構成

直接接続型のシングルノード構成では、1つまたは複数のホストをノードに直接接続します。



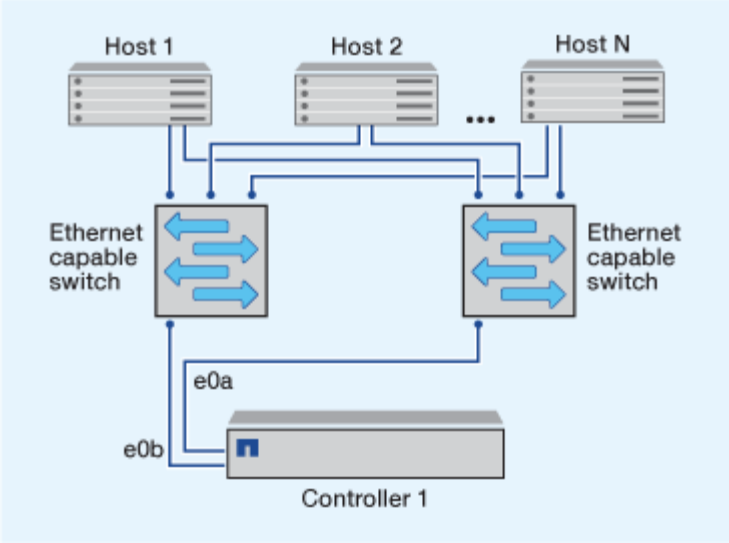
シングルネットワークのシングルノード構成

単一ネットワークのシングルノード構成では、1つのノードを1つのスイッチで1つ以上のホストに接続します。スイッチが1台しかないため、この構成では完全な冗長性は確保されません。



マルチネットワークのシングルノード構成

マルチネットワークのシングルノード構成では、1つのノードを複数のスイッチで1つまたは複数のホストに接続します。スイッチが複数あるため、この構成では完全な冗長性が確保されます。



シングルノードを使用する**FC**および**FC-NVMe SAN**ホストの構成方法

シングルノードのFCおよびFC-NVMe SANホストは、1つ以上のファブリック経由で構成できます。N-Port ID Virtualization（NPIV）が必要であり、ファブリック内のすべてのFCスイッチで有効にする必要があります。FCまたはFC-NMVE SANホストをFCスイッチを使用せずにシングルノードに直接接続することはできません。

単一ファブリックのシングルノード構成

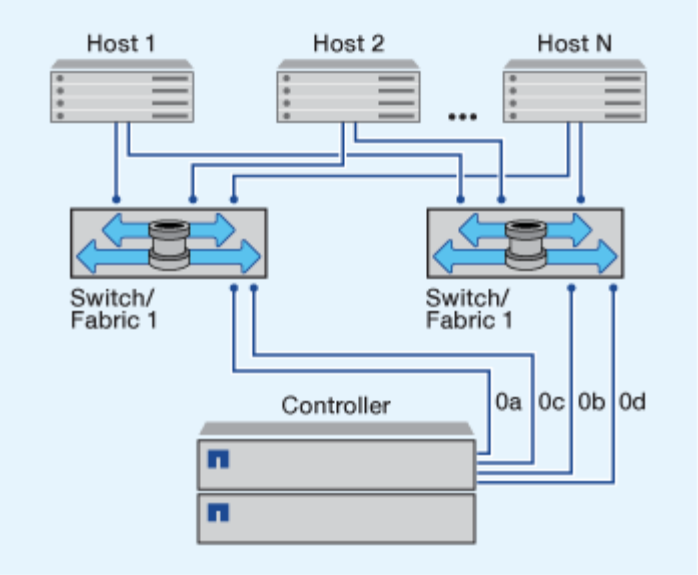
単一ファブリックのシングルノード構成では、1つのノードを1台のスイッチで1つまたは複数のホストに接続します。スイッチが1台しかないため、この構成では完全な冗長性は確保されません。

単一ファブリックのシングルノード構成では、ホストからノードへのパスが1つの場合、マルチパス ソフトウェアは必要ありません。

マルチファブリックのシングルノード構成

マルチファブリックのシングルノード構成では、1つのノードを複数のスイッチで1つまたは複数のホストに接続します。次の図は、マルチファブリックのシングルノード構成を示しています。わかりやすいように、この図ではファブリックが2つだけになっていますが、マルチファブリック構成は2つ以上の任意の数のファブリックで構成できます。この図では、上のシャーシにストレージ コントローラが取り付けられています。下のシャーシは、この例のように空けておくか、IOMXモジュールを使用できます。

次の図のFCターゲット ポート（0a、0c、0b、0d）は一例です。実際のポート番号は、使用しているストレージ ノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。



関連情報

"NetAppテクニカルレポート4684：『Implementing and Configuring Modern SANs with NVMe-oF』"

シングルノードクラスタでの**ONTAP**のアップグレード

ONTAP CLIを使用して、シングルノードクラスタの自動更新を実行できます。シングルノードクラスタは冗長性がないため、更新時には常にシステムの停止を伴います。SystemManagerを使用してシステムの停止を伴うアップグレードを実行することはできません。

開始する前に

アップグレード手順を完了する必要があり"準備"ます。

手順

1. 以前のONTAPソフトウェアパッケージを削除します。

```
cluster image package delete -version <previous_package_version>
```

2. ターゲットのONTAPソフトウェアパッケージをダウンロードします。

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

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

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

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

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

4. クラスタをアップグレードする準備が完了していることを確認します。

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7

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

5. 検証の進捗を監視します。

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

6. 検証で特定された必要なアクションをすべて完了します。
7. 必要に応じて、ソフトウェア アップグレードの見積もりを生成します。

```
cluster image update -version <package_version_number> -estimate-only
```

ソフトウェア アップグレードの見積もりには、更新対象の各コンポーネントの詳細とアップグレードの推定期間が表示されます。

8. ソフトウェアのアップグレードを実行します。

```
cluster image update -version <package_version_number>
```

問題が発生した場合は、更新が一時停止し、措置を講じるように求められます。問題の詳細や更新の進捗を確認するには、cluster image show-update-progressコマンドを使用します。問題を修正したら、cluster image resume-updateコマンドを使用して更新を再開できます。

9. クラスタの更新の進捗を表示します。

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

ノードは更新の一環として再起動され、再起動中にアクセスすることはできません。

10. 通知を送信します。

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

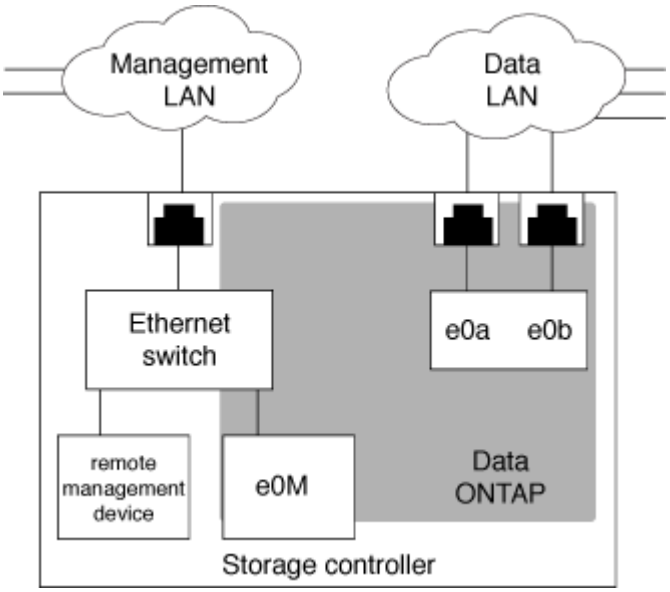
メッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

SP / BMCネットワークの設定

ネットワーク内の**ONTAP**管理トラフィックの分離

SP / BMC と e0M 管理インターフェイスは、管理トラフィック専用のサブネット上に設定することを推奨します。管理ネットワーク上でデータトラフィックを実行すると、原因のパフォーマンスの低下やルーティングの問題が発生する可能性があります。

ほとんどのストレージコントローラの管理イーサネットポート（シャーシ背面にあるレンチマークの付いたポート）は、内部イーサネットスイッチに接続されます。内部スイッチは、 SP / BMC および e0M 管理インターフェイスへの接続を提供します。これらを使用して、 Telnet 、 SSH 、 SNMP などの TCP/IP プロトコル経由でストレージシステムにアクセスできます。



リモート管理デバイスと e0M の両方を使用する場合は、同じ IP サブネット上に設定する必要があります。これらは低帯域幅のインターフェイスであるため、 SP / BMC と e0M は管理トラフィック専用のサブネット上に設定することを推奨します。

管理トラフィックを分離できない場合や、専用の管理ネットワークの規模が非常に大きい場合は、ネットワークトラフィックをできるだけ少なく抑える必要があります。イングレスブロードキャストまたはマルチキャストトラフィックが大量になると、 SP / BMC のパフォーマンスが低下する可能性があります。

AFF A800 などの一部のストレージコントローラには、外部ポートが 2 つあります。 1 つは BMC 用、もう 1 つは e0M 用です。これらのコントローラの場合、 BMC と e0M を同じ IP サブネット上に設定する必要はありません。

ONTAP SP / BMCネットワーク設定の詳細

SP に対してクラスタレベルの自動ネットワーク設定を有効にできます（推奨）。SP の自動ネットワーク設定を無効なままにし（デフォルト）、 SP ネットワーク設定をノードレベルで手動で管理することもできます。それぞれのケースについて、いくつかの考慮事項があります。

このトピックは、SPとBMCの両方に適用されます。

SP の自動ネットワーク設定を有効にすると、指定したサブネットのアドレスリソース（ IP アドレス、サブネットマスク、ゲートウェイアドレスなど）を使用してネットワークが自動的にセットアップされます。SP の自動ネットワーク設定を使用すると、各ノードの SP に IP アドレスを手動で割り当てる必要がなくなります。SP の自動ネットワーク設定を有効にするには、まず設定に使用するサブネットが先にクラスタに定義されている必要があるため、デフォルトでは、自動ネットワーク設定は無効になっています。

SP の自動ネットワーク設定を有効にした場合、次のシナリオと考慮事項が該当します。

- これまでに一度も SP が設定されていない場合、 SP ネットワークは、 SP の自動ネットワーク設定に指定したサブネットに基づいて自動的に設定されます。
- 以前に SP が手動で設定されている場合、または別のサブネットに基づく既存の SP ネットワーク設定がある場合、クラスタ内のすべてのノードの SP ネットワークが、 SP の自動ネットワーク設定で指定したサブネットに基づいて再設定されます。

  再設定によって SP に別のアドレスが割り当てられると、 DNS 設定に影響し、 SP のホスト名を解決できなくなる可能性があります。そのため、 DNS 設定の更新が必要になる場合があります。

- クラスタに参加するノードでは、指定したサブネットを使用してSPネットワークが自動的に設定されます。
- `system service-processor network modify`コマンドでは、SP IPアドレスを変更できません。

  SP 自動ネットワーク設定が有効になっている場合、このコマンドで実行できるのは SP ネットワークインターフェイスの有効化または無効化のみです。

  - SP の自動ネットワーク設定が以前に有効になっていた場合、 SP ネットワークインターフェイスを無効にすると、割り当てられたアドレスリソースが解放されてサブネットに戻されます。
  - SP ネットワークインターフェイスを無効にし、その後再度有効にすると、 SP は別のアドレスで再設定されることがあります。

SP の自動ネットワーク設定を無効にした場合（デフォルト）、次のシナリオと考慮事項が該当します。

- これまでに一度も SP が設定されていない場合、 SP IPv4 ネットワーク設定は、 IPv4 DHCP を使用するデフォルトの設定になり、 IPv6 は無効になります。

  クラスタに参加するノードの SP ネットワーク設定も、デフォルトで IPv4 DHCP に設定されます。

- `system service-processor network modify`コマンドを使用して、ノードのSP IPアドレスを設定できます。

  サブネットに割り当てられているアドレスを使用して SP ネットワークを手動で設定しようとすると、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、重複するアドレスが割り当てられる可能性があります。

一度有効にした SP の自動ネットワーク設定を無効にした場合、次のシナリオと考慮事項が該当します。

- SPの自動ネットワーク設定でIPv4アドレスファミリーが無効になっている場合、SP IPv4ネットワークはDHCPを使用するデフォルトの設定になります。また、 `system service-processor network modify`コマンドを使用して、個 々 のノードのSP IPv4設定を変更できます。
- SPの自動ネットワーク設定でIPv6アドレスファミリーが無効になっている場合は、SP IPv6ネットワークも無効になります。また、 `system service-processor network modify`コマンドを使用して、個 々 のノードのSP IPv6設定を有効にしたり変更したりできます。

ONTAP SP / BMCの自動ネットワーク設定を有効にする

SP ネットワークを手動で設定するよりも、自動ネットワーク設定を使用するように SP を設定することを推奨します。SPの自動ネットワーク設定はクラスタ全体で行われるため、個 々 のノードのSPネットワークを手動で管理する必要はありません。

このタスクは、SPとBMCの両方に適用されます。

- SPの自動ネットワーク設定に使用するサブネットは、クラスタで定義済みであり、SPネットワークインターフェイスとリソースが競合していない必要があります。

  コマンドは `network subnet show`、クラスタのサブネット情報を表示します。

  の詳細については `network subnet show`、を"ONTAPコマンド リファレンス"参照してください。

  サブネットの関連付けを強制するパラメータ（ `-force-update-lif-associations`コマンドのパラメータ `network subnet`）は、ネットワークLIFでのみサポートされ、SPネットワークインターフェイスではサポートされません。

- SP に IPv6 接続を設定する場合、 ONTAP に対して IPv6 が設定済みで、有効になっている必要があります。

  `network options ipv6 show`コマンドは、ONTAPのIPv6設定の現在の状態を表示します。の詳細については `network options ipv6 show`、をlink:https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html["ONTAPコマンド リファレンス"^]参照してください。

手順

1. コマンドを使用して、SPで使用するサブネットのIPv4またはIPv6アドレスファミリーと名前を指定します `system service-processor network auto-configuration enable`。
2. コマンドを使用して、SPの自動ネットワーク設定を表示します `system service-processor`

network auto-configuration show。

3. その後、クォーラム内のすべてのノードに対してSP IPv4またはIPv6ネットワークインターフェイスを無効または再度有効にする場合は、コマンドで [IPv4|IPv6] [true|false`パラメータと `-enable]パラメータを指定して `-address-family`使用し `system service-processor network modify`ます。

   SP 自動ネットワーク設定が有効になっている場合、クォーラム内のノードの SP IP アドレスを変更することはできません。実行できるのは、 SP IPv4 または IPv6 ネットワークインターフェイスの有効化または無効化だけです。

   ノードがクォーラムのメンバーでない場合は、ノードからを実行し、そのノードのSP自動ネットワーク設定を上書きすることを確認して、SP IPアドレスを含むノードのSPネットワーク設定を変更できます。`system service-processor network modify`ただし、ノードがクォーラムに参加すると、指定したサブネットに基づいてノードに対して SP の自動再設定が実行されます。

ONTAP SP / BMCネットワークの手動設定

SP に自動ネットワーク設定が設定されていない場合、 IP アドレスを使用して SP にアクセスできるように、ノードの SP ネットワークを手動で設定する必要があります。

開始する前に

SP に IPv6 接続を設定する場合、 ONTAP に対して IPv6 が設定済みで、有効になっている必要があります。コマンドは、 network options ipv6`ONTAPのIPv6設定を管理します。の詳細については `network options ipv6、を"ONTAPコマンド リファレンス"参照してください。

> このタスクは、SPとBMCの両方に適用されます。

SP は、 IPv4 、 IPv6 、またはその両方を使用するように設定できます。SPのIPv4設定では静的アドレス指定とDHCPアドレス指定がサポートされ、SPのIPv6設定では静的アドレス指定のみがサポートされます。

SPの自動ネットワーク設定が設定されている場合は、個 々 のノードのSPネットワークを手動で設定する必要はなく、`system service-processor network modify`コマンドで実行できるのはSPネットワークインターフェイスの有効化と無効化のみです。

手順

1. コマンドを使用して、ノードのSPネットワークを設定し `system service-processor network modify`ます。
   - パラメータは、 `-address-family`SPのIPv4とIPv6のどちらの設定を変更するかを指定します。
   - パラメータは -enable、指定したIPアドレスファミリーのネットワークインターフェイスを有効にします。
   - パラメータは、 `-dhcp`DHCPサーバのネットワーク設定を使用するか、指定したネットワークアドレスを使用するかを指定します。

     IPv4を使用している場合にのみ、DHCPを有効にできます（をに v4`設定 `-dhcp）。IPv6設定の場合、DHCPを有効にすることはできません。

   - パラメータは、 `-ip-address`SPのパブリックIPアドレスを指定します。

     サブネットに割り当てられているアドレスを使用して SP ネットワークを手動で設定しようとすると、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、重複

するアドレスが割り当てられる可能性があります。

- パラメータは `-netmask`、SPのネットマスクを指定します（IPv4を使用している場合）。
- パラメータは、 `-prefix-length`SPのサブネットマスクのネットワークプレフィックス長を指定します（IPv6を使用している場合）。
- パラメータは `-gateway`、SPのゲートウェイIPアドレスを指定します。

2. 手順1を繰り返して、クラスタ内の残りのノードのSPネットワークを設定します。
3. コマンドでまたは `-field setup-status`パラメータを指定して `-instance`、SPネットワーク設定を表示し、SPのセットアップステータスを確認します `system service-processor network show`。

   ノードの SP のセットアップステータスは、次のいずれかになります。

   - `not-setup`--未設定
   - `succeeded`--設定に成功しました
   - `in-progress`--設定が進行中
   - `failed`--設定に失敗しました

SPネットワークの設定例

次の例では、ノードの SP を設定して IPv4 を使用し、 SP を有効化してから SP ネットワーク設定を表示して設定内容を確認します。

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

ONTAPサービスプロセッサ**API**の設定を変更します。

SP API は、 ONTAP がネットワークを介して SP と通信できるようにするセキュアなネットワーク API です。SP API サービスで使用されるポートを変更したり、サービスが内部通信に使用する証明書を更新したり、サービス全体を無効にしたりできます。設定の変更が必要になることはほとんどありません。

タスクの内容

- SP APIサービスでは、デフォルトでポートが使用され `50000`ます。

  ポートが別のネットワークアプリケーションによる通信に使用されているネットワーク設定の場合や、他のアプリケーションからのトラフィックとSP APIサービスによって生成されるトラフィックを区別する場合など、ポートの値を変更できます 50000。

- SP API サービスが使用する SSL 証明書および SSH 証明書は、クラスタ内専用であり、外部に配布されることはありません。

証明書のセキュリティが侵害されることはほとんどありませんが、侵害された場合には証明書を更新できます。

- SP API サービスは、デフォルトで有効になっています。

  SP API サービスを無効にする必要があるのは、 SP が設定または使用されていないプライベート LAN でサービスを無効にする場合など、例外的な場合だけです。

  SP API サービスを無効にすると、 API は着信接続を受け付けません。また ' ネットワーク・ベースの SP ファームウェア・アップデートやネットワーク・ベースの SP ログ収集などの機能は使用できなくなりますシステムはシリアルインターフェイスの使用に切り替わります。

手順

1. コマンドを使用して、advanced権限レベルに切り替えます `set -privilege advanced`。
2. SP APIサービス設定を変更します。

状況	使用するコマンド
SP API サービスで使用されるポートを変更する	`system service-processor api-service modify`を使用します `-port {49152。.65535}` パラメータ
SP APIサービスで内部通信に使用するSSL証明書とSSH証明書を更新する	• ONTAP 9 .5以降での使用 `system service-processor api-service renew-internal-certificate` • ONTAP 9 .4以前の場合 • `system service-processor api-service renew-certificates` パラメータを指定しない場合は、ホスト証明書（クライアント証明書とサーバ証明書を含む）のみが更新されます。 `-renew-all true`パラメータを指定すると、ホスト証明書とルートCA証明書の両方が更新されます。
通信	
SP API サービスを無効または再度有効にします	`system service-processor api-service modify{true`

3. コマンドを使用して、SP APIサービス設定を表示します `system service-processor api-service show`。

SP / BMCを使用したノードのリモート管理

SP / BMCを使用したONTAPノードのリモート管理

ノードをリモートから管理するには、 Service Processor （ SP ；サービスプロセッサ）または Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）と呼ばれるオンボードコントローラを使用します。このリモート管理コントローラは、現在のすべてのプラットフォームモデルに含まれています。コントローラは、ノードの動作状態に関係なく、継続して機能します。

プラットフォームのSPとBMCのサポートの詳細については、NetAppサポートサイトのを参照してください"サポートマトリックス"。

ONTAPサービスプロセッサを使用したリモートノード管理

サービスプロセッサ（SP）は、ノードに対するアクセス、監視、およびトラブルシューティングをリモートから実行できるリモート管理デバイスです。

SP の主な機能は次のとおりです。

- SP を使用すると、ノードコントローラの状態に関係なく、ノードにリモートからアクセスして、ノードの診断、シャットダウン、電源の再投入、リブートを実行できます。

  SPはスタンバイ電圧で動作します。スタンバイ電圧は、ノードの少なくとも1つの電源装置から電力が供給されていれば使用できます。

  SP にログインするには、管理ホストから Secure Shell クライアントアプリケーションを使用します。ログインすると、 SP CLI を使用して、リモートからノードの監視とトラブルシューティングを行うことができます。さらに、 SP を使用してシリアルコンソールにアクセスし、リモートから ONTAP コマンドを実行できます。

  SP にはシリアルコンソールからアクセスでき、また SP からシリアルコンソールにアクセスすることもできます。SP では、 SP CLI セッションと別のコンソールセッションを両方同時に開くことができます。

  たとえば、温度センサーで異常な高温または低温が検知されると、 ONTAP のトリガーによって、 SP がマザーボードを正常にシャットダウンします。シリアルコンソールが応答しなくなりますが、コンソールで Ctrl+G を押して SP CLI にアクセスすることができます。その後、SPからコマンドまたは `system power cycle`コマンドを使用して、ノードの電源をオンまたは再投入できます `system power on`。

- SP によって環境センサーが監視され、イベントがログに記録されるため、タイムリーで効果的なサービスアクションを実施できます。

  SP は、ノードの温度、電圧、電流、ファン速度などの環境センサーを監視します。環境センサーが異常な状態になると、 SP は異常な測定値をログに記録し、 ONTAP に問題を通知します。また SP は、ノードが AutoSupport メッセージを送信できるかどうかに関係なく、 AutoSupport メッセージを通じて必要に応じてアラートおよび「自身のシステム」通知を送信します。

  さらに、ブートの進行、 Field Replaceable Unit （ FRU ；フィールド交換可能ユニット）の交換、 ONTAP が生成するイベント、 SP のコマンド履歴といったイベントについてもログに記録します。AutoSupport メッセージを手動で起動し、指定したノードから収集された SP ログファイルを含める

ことができます。

SP は、停止したノードの代わりにこれらのメッセージを生成し、 AutoSupport メッセージに追加の診断情報を添付する以外には、 AutoSupport 機能にまったく影響を及ぼしません。AutoSupport の設定値やメッセージ内容は、 ONTAP から継承されます。

> SPは、通知を送信するときに、コマンドのパラメータ設定に `system node autosupport modify`依存しません `-transport`。SPはSMTP（簡易メール転送プロトコル）のみを使用し、メールホスト情報を含めるためにホストのAutoSupport設定を必要とします。

SNMP が有効になっている場合、 SP は SNMP トラップを生成して、すべての「独自のシステム」イベントに対するトラップホストを設定します。

- SPには、システムイベントログ（SEL）に最大4、000のイベントを格納できる不揮発性メモリバッファがあり、問題の診断に役立ちます。

  SEL には、各監査ログエントリが監査イベントとして格納されます。SP のオンボードフラッシュメモリに格納されています。SEL のイベントリストは、 SP によって、指定された受信者に AutoSupport メッセージを通じて自動的に送信されます。

  SEL には次の情報が含まれています。

  - SPによって検出されたハードウェアイベント。たとえば、電源装置、電圧、またはその他のコンポーネントに関するセンサーステータスなど
  - SPによって検出されたエラー（通信エラー、ファン障害、メモリまたはCPUのエラーなど）
  - ノードがSPに送信した重大なソフトウェアイベント。たとえば、パニック、通信障害、ブート障害、SPまたは `system power cycle`コマンドの実行結果として生じたユーザ起因の「`down system`」など `system reset`

- SP は、管理者によるコンソールログインまたはコンソール接続の有無にかかわらず、シリアルコンソールを監視します。

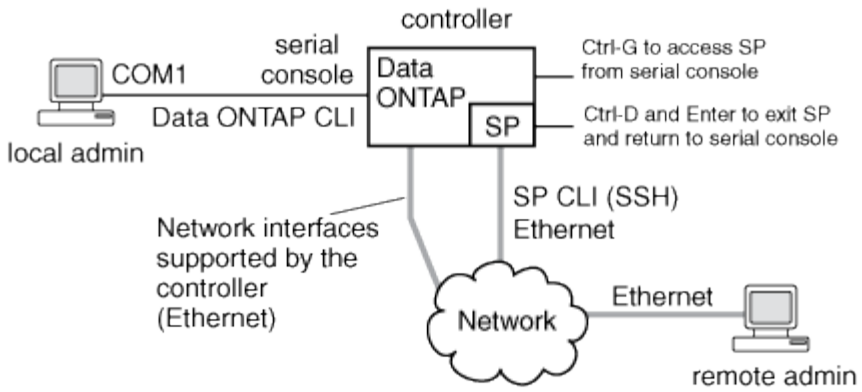
  コンソールにメッセージが送信されると、 SP はメッセージをコンソールログに格納します。ノードのいずれかの電源装置から SP に給電されていれば、コンソールログの機能は維持されます。SP はスタンバイ電源で動作するので、ノードの電源再投入時または電源オフ時にも使用可能です。

- SP が設定されている場合、ハードウェアアシストテイクオーバーが可能です。
- SP API サービスを使用すると、 ONTAP と SP がネットワーク経由で通信できます。

  このサービスは、 SP ファームウェアの更新にネットワークインターフェイスを使用する、ノードが別のノードの SP 機能やシステムコンソールにアクセスできるようにする、別のノードから SP ログをアップロードする、などのネットワークベースの機能をサポートすることで、 SP の ONTAP 管理を強化します。

  SP API サービスの設定を変更するには、サービスで使用するポートを変更し、サービスで内部の通信に使用する SSL 証明書と SSH 証明書を更新するか、サービス全体を無効にします。

次の図は、 ONTAP およびノードの SP へのアクセスを示しています。SP インターフェイスは、イーサネットポート（シャーシ背面にあるレンチマークの付いたポート）経由でアクセスされます。



ONTAPベースボード管理コントローラを使用してノードをリモートから管理する

特定のハードウェアプラットフォームでは、ベースボード管理コントローラ（BMC）の新しいオンボードコントローラをサポートするようにソフトウェアがカスタマイズされています。BMCには、デバイスをリモートで管理するために使用できるコマンドラインインターフェイス（CLI）コマンドが用意されています。

BMCはサービスプロセッサ（SP）と同様に機能し、同じコマンドの多くを使用します。BMCでは、次の操作を実行できます。

- BMCネットワークの設定を行います。
- ノードにリモートからアクセスし、ノードの診断、シャットダウン、電源の再投入、リブートなどのノード管理タスクを実行する。

SPとBMCにはいくつかの違いがあります。

- BMCは、電源装置要素、冷却要素、温度センサー、電圧センサー、および電流センサーの環境監視を完全に制御します。BMCは、IPMIを介してセンサー情報をONTAPに報告します。
- 一部のハイアベイラビリティ（HA）コマンドとストレージコマンドは異なります。
- BMCはAutoSupportメッセージを送信しません。

次の要件でONTAPを実行している場合は、自動ファームウェア更新も利用できます。

- BMCファームウェアリビジョン1.15以降がインストールされている必要があります。

  BMCファームウェアを1.12から1.15以降にアップグレードするには、手動で更新する必要があります。

- ファームウェアの更新が完了すると、BMCが自動的にリブートします。

  BMCのリブート中もノードの処理には影響しません。

ONTAP SP / BMCファームウェアの更新を管理します。

ONTAP には、 _baseline image_という SP ファームウェアイメージが含まれています。

新しいバージョンのSPファームウェアが利用可能になった場合は、そのファームウェアをダウンロードして、SPファームウェアをダウンロードしたバージョンに更新できます。ONTAPのバージョンをアップグレードする必要はありません。

このトピックは、SPとBMCの両方に適用されます。

ONTAPでは、次の方法でSPファームウェアの更新を管理できます。

- SP自動更新機能はデフォルトで有効になっており、次の場合にSPファームウェアを自動的に更新できます。
  - 新しいバージョンのONTAPにアップグレードする場合

    ONTAPにバンドルされているSPファームウェアのバージョンがノードで実行されているSPのバージョンよりも新しい場合、ONTAPのアップグレードプロセスには自動的にSPファームウェアの更新が含まれます。

    SPの自動更新が失敗した場合、ONTAPはこれを検出し、修正操作をトリガーしてSPの自動更新を最大3回試行します。3回の再試行がすべて失敗した場合は、"NetAppナレッジベース: ヘルスモニター SPAutoUpgradeFailedMajorAlert SPアップグレード失敗 - AutoSupportメッセージ" 。
  - NetApp Support Siteからダウンロードした SP ファームウェアのバージョンが、現在実行している SP ファームウェアのバージョンよりも新しい場合
  - ONTAPを以前のバージョンにダウングレードまたはリバートする場合

    SPファームウェアは、リバートまたはダウングレードしたONTAPのバージョンでサポートされている最新の互換バージョンに自動的に更新されます。SPファームウェアを手動で更新する必要はありません。

  コマンドを使用して、SP自動更新機能を無効にすることができます `system service-processor image modify`。ただし、この機能は有効にしておくことを推奨します。この機能を無効にすると、ONTAPイメージとSPファームウェアイメージの組み合わせが最適でない、または認定されていない可能性があります。

- ONTAPでは、SP更新を手動でトリガーし、コマンドを使用して更新の実行方法を指定でき `system service-processor image update`ます。

  次のオプションを指定できます。

  - 使用するSPファームウェアパッケージ(`-package`)

    パッケージファイル名を指定すると、ダウンロードしたパッケージにSPファームウェアを更新できます。advancedコマンドを使用すると、 `system image package show`ノードで使用可能なすべてのパッケージファイル（SPファームウェアパッケージのファイルを含む）が表示されます。
  - SPアップデートにベースラインSPファームウェアパッケージを使用するかどうか(`-baseline`)

    SPファームウェアを、現在実行しているバージョンのONTAPにバンドルされているベースラインバージョンに更新できます。

より高度な更新オプションまたはパラメータの一部を使用すると、BMCの構成設定が一時的にクリアされる場合があります。リブート後、ONTAPでBMC構成がリストアされるまでに最大10分かかることがあります。

- ONTAPでは、コマンドを使用して、ONTAPからトリガーされた最新のSPファームウェア更新のステータスを表示でき `system service-processor image update-progress show`ます。

SPへの既存の接続は、SPファームウェアの更新時に終了します。これは、SPファームウェアの更新が自動的に開始されるか手動で開始されるかに関係します。

関連情報

"NetAppのダウンロード：システムファームウェアと診断"

ファームウェアアップデートに使用する**ONTAP SP / BMC**およびネットワークインターフェイス

バージョン1.5、2.5、3.1、またはそれ以降を実行しているSPを搭載したONTAPからトリガーされるSPファームウェアの更新では、SPネットワークインターフェイス経由でのIPベースのファイル転送メカニズムの使用がサポートされます。

このトピックは、SPとBMCの両方に適用されます。

ネットワークインターフェイス経由のSPファームウェア更新は、シリアルインターフェイス経由の更新よりも高速です。これにより、SPファームウェアの更新中のメンテナンス時間が短縮されるだけでなく、ONTAPの処理が停止することもありません。この機能をサポートするSPバージョンは、ONTAPに含まれています。これらはNetAppサポートサイトからも入手でき、互換性のあるバージョンのONTAPを実行しているコントローラにインストールできます。

SPバージョン1.5、2.5、3.1、またはそれ以降を実行している場合、次のファームウェアアップグレード動作が適用されます。

- ONTAP によって自動でトリガーされる SP ファームウェア更新では、デフォルトでネットワークインターフェイスが使用されます。ただし、次のいずれかの条件に該当する場合、 SP 自動更新はシリアルインターフェイス経由に切り替わります。
  - SPネットワークインターフェイスが設定されていないか使用できません。
  - IPベースのファイル転送が失敗する。
  - SP APIサービスが無効になっています。

実行しているSPのバージョンに関係なく、SP CLIからトリガーされるSPファームウェアの更新では、常にSPネットワークインターフェイスが使用されます。

関連情報

"NetAppのダウンロード：システムファームウェアと診断"

クラスタユーザアカウントを使用した**ONTAP**サービスプロセッサへのアクセス

SPにアクセスしようとすると、クレデンシャルを入力するように求められます。アプリケーションタイプで作成されたクラスタユーザアカウント `service-processor`は、クラスタの任意のノード上のSP CLIにアクセスできます。SPユーザアカウント

はONTAPから管理され、パスワードによって認証されます。ONTAP 9 .9.1以降では、SPユーザアカウントにロールが必要です `admin`。

SPにアクセスするためのユーザアカウントは、SP CLIではなくONTAPから管理します。クラスタユーザアカウントは、コマンドのパラメータを `security login create`に、 `-authmethod`パラメータをに `service-processor`設定 `password`して作成したSPにアクセスできます `-application`。SPはパスワード認証のみをサポートしています。

SPユーザアカウントを作成するときは、パラメータを指定する必要があり `-role`ます。

- ONTAP 9 .9.1以降のリリースでは、パラメータに `-role`を指定する必要があり `admin`、アカウントを変更する場合はロールが必要 `admin`です。その他のロールは、セキュリティ上の理由から許可されなくなりました。
  - ONTAP 9 .9.1以降のリリースにアップグレードする場合は、を参照してください"サービスプロセッサにアクセスできるユーザアカウントの変更"。
  - ONTAP 9 .8以前のリリースに戻す場合は、を参照してください"サービスプロセッサにアクセスできるユーザアカウントの確認"。
- ONTAP 9 .8以前のリリースでは、すべてのロールがSPにアクセスできますが、 `admin`これが推奨されます。

デフォルトでは、「admin」という名前のクラスタユーザアカウントにはアプリケーションタイプが含まれて `service-processor`おり、SPへのアクセス権があります。

ONTAP では、システム用に予約されている名前（「 root 」や「 naroot 」など）を使用したユーザアカウントを作成できないようになっています。システムに予約されている名前を使用してクラスタまたはSPにアクセスすることはできません。

現在のSPユーザアカウントを表示するには、コマンドのパラメータを `security login show`使用し `-application service-processor`ます。

の詳細については `security login show`、を"ONTAPコマンド リファレンス"参照してください。

管理ホストからノードの**ONTAP SP / BMC**にアクセスする

管理ホストからノードの SP にログインして、ノードの管理タスクをリモートから実行できます。

開始する前に

次の条件を満たす必要があります。

- SP へのアクセスに使用する管理ホストでは SSHv2 がサポートされている必要がある。
- SP へのアクセス用にユーザアカウントがすでにセットアップされている必要があります。

  SPにアクセスするには、コマンドのパラメータを `security login create`に、 `-authmethod`パラメータを `password`に設定 `service-processor`してユーザアカウントを作成しておく必要があり `-application`ます。

このタスクは、SPとBMCの両方に適用されます。

SP が IPv4 または IPv6 アドレスを使用するように設定されていて、ホストからの SSH ログイン試行が 10 分以内に連続 5 回失敗した場合には、 SP は SSH ログイン要求を拒否し、ホストの IP アドレスとの通信を 15 分間中断します。通信は 15 分後に再開され、 SP へのログインを再度試行できるようになります。

ONTAP では、システム用に予約されている名前（「 root 」や「 naroot 」など）をクラスタまたは SP にアクセスする目的で作成または使用することはできません。

手順

1. 管理ホストから、 SP にログインします。

   ssh username@SP_IP_address

2. プロンプトが表示されたら、のパスワードを入力し `username`ます。

   SP プロンプトが表示され、 SP CLI にアクセスしていることが示されます。

管理ホストからの**SP**アクセスの例

次の例は、SPにアクセスするように設定されているユーザアカウントを使用してSPにログインする方法を示してい `joe`ます。

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

次の例は、 IPv6 グローバルアドレスまたは IPv6 ルータ通知アドレスを使用して、 IPv6 に対して SSH が設定されかつ SP が設定されているノードの SP にログインする方法を示しています。

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

システムコンソールからノードの**ONTAP SP / BMC**にアクセスする

システムコンソール（ *serial console*） から SP にアクセスして、タスクの監視やトラブルシューティングを実行できます。

タスクの内容

このタスクは、SPとBMCの両方に適用されます。

手順

1. システムコンソールからSP CLIにアクセスするには、プロンプトでCtrl+Gを押します。
2. プロンプトが表示されたら、 SP CLI にログインします。

   SP プロンプトが表示され、 SP CLI にアクセスしていることが示されます。

3. SP CLI を終了してシステムコンソールに戻るには、 Ctrl+D を押し、 Enter キーを押します。

システムコンソールから**SP CLI**へのアクセスの例

次の例に、 Ctrl+G を押してシステムコンソールから SP CLI にアクセスした結果を示します。 `help system power`SPプロンプトでコマンドを入力し、Ctrl+Dを押してからEnterキーを押してシステムコンソールに戻ります。

```
cluster1::>
```

（ SP CLI にアクセスするには Ctrl+G を押します。）

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

（システムコンソールに戻るには、 Ctrl+D と Enter キーを押します。）

```
cluster1::>
```

ONTAP SP CLIセッション、**SP**コンソールセッション、システムコンソールセッションの関連性について説明します。

SP CLI セッションを開いてノードをリモートから管理したり、別の SP コンソールセッションを開いてノードのコンソールにアクセスしたりすることができます。SP コンソールセッションは、同時システムコンソールセッションに表示される出力をミラーリングします。SP とシステムコンソールには独立したシェル環境があり、独立したログイン認証が行われます。

SP CLI セッション、 SP コンソールセッション、システムコンソールセッションの関係を理解しておくと、ノードをリモートから管理する際に役に立ちます。これらのセッションの関係を次に示します。

- SP CLI セッションには一度に 1 人の管理者しかログインできません。ただし SP では、 SP CLI セッショ

ンと別の SP コンソールセッションを同時に開くことができます。

SP CLIはSPプロンプトで示され(SP>`ます）。SP CLIセッションでは、SPコマンドを使用してSPコンソールセッションを開始できます `system console。同時に、 SSH を介して別の SP CLI セッションを開始することもできます。Ctrl+D キーを押して SP コンソールセッションを終了すると、自動的に SP CLI セッションに戻ります。SP CLI セッションがすでに存在する場合は、既存の SP CLI セッションを終了するかどうかを尋ねるメッセージが表示されます。「 y 」と入力すると、既存の SP CLI セッションが終了し、 SP コンソールから SP CLI に戻ることができます。このアクションは、SPイベントログに記録されます。

SSH経由で接続されたONTAP CLIセッションでは、別のノードからONTAPコマンドを実行して、ノードのシステムコンソールに切り替えることができます system node run-console。

- セキュリティ上の理由から、 SP CLI セッションとシステムコンソールセッションには独立したログイン認証機能があります。

  SP CLIから（SPコマンドを使用して）SPコンソールセッションを開始すると、 `system console`システムコンソールのクレデンシャルを入力するように求められます。システムコンソールセッションから（ Ctrl+G キーで） SP CLI にアクセスすると、 SP CLI のクレデンシャルを入力するように求められます。

- SP コンソールセッションとシステムコンソールセッションには独立したシェル環境があります。

  SP コンソールセッションは、同時システムコンソールセッションに表示される出力をミラーリングします。ただし、同時システムコンソールセッションでは、 SP コンソールセッションをミラーリングしません。

  SP コンソールセッションは、同時 SSH セッションの出力をミラーリングしません。

管理ホストの**IP**アドレスを追加して**ONTAP**サービスプロセッサにアクセス

デフォルトでは、 SP はすべての IP アドレスの管理ホストからの SSH 接続要求を受け付けます。指定した IP アドレスを持つ管理ホストのみからの SSH 接続要求を受け付けるように SP を設定できます。変更内容は、クラスタ内のすべてのノードの SP への SSH アクセスに適用されます。

手順

1. 指定したIPアドレスのみにSPアクセスを許可するには、 `system service-processor ssh add-allowed-addresses`コマンドでパラメータを指定 `-allowed-addresses`します。

   - パラメータの値は -allowed-addresses`の形式で指定する必要があります `address/netmask。複数の address/netmask`ペアはカンマで区切る必要があります（例：） `10.98.150.10/24, fd20:8b1e:b255:c09b::/64。

     パラメータをに `0.0.0.0/0, ::/0`設定する `-allowed-addresses`と、すべてのIPアドレスがSPにアクセスできるようになります（デフォルト）。

   - 指定したIPアドレスのみにSPアクセスを制限してデフォルトを変更すると、ONTAPは、指定したIPアドレスで「すべて許可」のデフォルト設定を置き換えることを確認するプロンプトを表示し(`0.0.0.0/0, ::/0`ます）。

   - `system service-processor ssh show`コマンドは、SPにアクセスできるIPアドレスを表示します。

2. 指定したIPアドレスによるSPへのアクセスをブロックするには、パラメータを指定してコマンドを `-

allowed-addresses`使用し `system service-processor ssh remove-allowed-addresses`ます。

すべての IP アドレスから SP へのアクセスをブロックすると、管理ホストから SP にアクセスできなくなります。

SPにアクセスできる**IP**アドレスの管理の例

次の例は、 SP への SSH アクセスのためのデフォルト設定を示しています。ここでは、指定した IP アドレスのみに SP アクセスを制限することで、デフォルトの設定を変更し、指定した IP アドレスをアクセスリストから削除し、すべての IP アドレスに対する SP アクセスをリストアします。

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

ONTAP SP / BMC CLIでのヘルプ情報の表示

オンラインヘルプには、SP / BMC CLIのコマンドとオプションが表示されます。

タスクの内容

このタスクは、SPとBMCの両方に適用されます。

手順

1. SP / BMCコマンドのヘルプ情報を表示するには、次のように入力します。

SPヘルプにアクセスする	**BMC**ヘルプにアクセスする
SPプロンプトでと入力し `help`ます。	BMCプロンプトでと入力し `system`ます。

次に、SP CLIオンライン ヘルプの例を示します。

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

次に、BMC CLIオンラインヘルプの例を示します。

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. SP / BMCコマンドのオプションのヘルプ情報を表示するには、SP / BMCコマンドの前または後ろにと入力します `help`。

   次に、SPコマンドのSP CLIオンラインヘルプの例を示し `events`ます。

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

   次に、BMCコマンドのBMC CLIオンラインヘルプの例を示し `system power`ます。

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

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

関連情報

- "イベント"
- "システム電源"

リモートノード管理用の**ONTAP**コマンド

SPにアクセスしてSP CLI コマンドを実行するか、 BMCにアクセスしてBMC CLI コマンドを実行することにより、ノード管理タスクをリモートで実行できます。よく実行されるいくつかのリモート ノード管理タスクについては、クラスタ内の別のノードからONTAPコマンドを使用することもできます。一部のSPおよびBMCコマンドはプラットフォーム固有であり、お使いのプラットフォームでは使用できない可能性があります。

特定のコマンド タイプは、 SPコマンド セットとBMCコマンド セットの両方で使用できます。それらの違いは、コマンドラインを入力するときに表示されます。

例

- その `help`SPのコマンド： `SP> help`
- その `help`BMCのコマンド： `BMC> help`

詳細はこちら `help`SPおよびBMCで使用できるコマンドオプション"ONTAP SP / BMC CLIでのヘルプ情報の表示"。

対応するONTAP BMC CLIの詳細については、"ONTAPベースボード管理コントローラでサポートされるCLIコマンド" 。

状況	使用する**SP**コマンド	使用する**BMC**コマンド	この**ONTAP**コマンドを使用します...
SP/ BMC/ ONTAPで利用可能なコマンドまたは指定されたコマンドのサブコマンドを表示します。	`help[command]`	`help[command]`	N/A
SP/ BMC/ ONTAP CLIの現在の権限レベルを表示します	`priv show`	`priv show`	N/A
SP/ BMC/ ONTAP CLIの指定されたモードにアクセスするための権限レベルを設定します	`priv set {admin`	`advanced`	`diag }`
`priv set {admin`	`advanced`	`diag`	`test }`
N/A	システムの日付と時刻を表示します。	`date`	`date`
`date`	SP/ BMC/ ONTAPによって記録されたイベントを表示します	`events {all`	`info`
`newest number`	`oldest number`	`search keyword }`	`events {all`
`info`	`newest`	`oldest`	`search }`
N/A	SP/ BMC/ ONTAPのステータスとネットワーク構成情報を表示します	`sp status [-v`	`-d ]` * その `-v`オプションは、SP統計を詳細形式で表示します。 * その `-d`オプションは、SPデバッグ ログをディスプレイに追加します。

状況	使用するSPコマンド	使用するBMCコマンド	このONTAPコマンドを使用します…

`bmc status`
 	
`[-v`
	`-d ]`
	
	* その `-v`オプションは、SP統計を詳細形式で表示します。
	* その `-d`オプションは、SPデバッグ ログをディスプレイに追加します。
		`system service-processor show`	SP/ BMC/ ONTAP の起動時間と、過去 1 分、5 分、15 分間の実行キュー内のジョブの平均数を表示します。

`sp uptime`	`bmc uptime`	N/A	システムコンソールログを表示する

`system log`	`system log`
	
	`[-a]`
		`system log`
		
		(システムコンソールのログを出力します)
			SP/ BMC/ ONTAPログ アーカイブまたはアーカイブ内のファイルを表示します

`sp log history show`
 	
`[-archive {latest`
	`{all`	`archive-name }][-dump {all`	`file-name }]`

`bmc log history show`
 	
`[-archive {latest`
	`{all`	`archive-name }][-dump {all`	`file-name }]`

N/A	ノードのコントローラの電源ステータスを表示する	`system power status`	`system power status`
`system node power show`	バッテリ情報を表示します。	`system battery show`	`system battery show`

N/A	ACP情報またはエキスパンダセンサーのステータスを表示する	`system acp`
		
		`[show`
			`sensors show ]`

N/A	N/A	すべてのシステムFRUとそのIDを一覧表示する	`system fru list`
`system fru list`	N/A	指定したFRUの製品情報を表示します。	`system fru show fru_id`

状況	使用するSPコマンド	使用するBMCコマンド	このONTAPコマンドを使用します…
`system fru show` [`show <id>`]	N/A	FRUのデータ履歴ログを表示する	`system fru log show` （advanced権限レベル）

`system fru log show`	N/A	状態や現在の値など、環境センサーのステータスを表示する	`system sensors`
			
			または
			
			`system sensors show`

`system sensors` {`show`	`filter <sensor_string>` }	`system node environment sensors show`	指定したセンサーのステータスと詳細を表示する
`system sensors get sensor_name` は、または `system sensors show`コマンドを使用して `system sensors`取得できます `sensor_name`。	`system sensors` [`get`]	N/A	SP/ BMC/ ONTAPファームウェアのバージョン情報を表示する
`version`	`version`	`system service-processor image show`	SP/ BMC/ ONTAPコマンド履歴を表示する
`sp log audit` （advanced権限レベル）	`bmc log audit` （advanced権限レベル）	N/A	SP/ BMC/ ONTAPのデバッグ情報を表示する
`sp log debug` （advanced権限レベル）	`bmc log debug` （advanced権限レベル）	N/A	SP/ BMC/ ONTAPメッセージファイルを表示する
`sp log messages` （advanced権限レベル）	`bmc log messages` （advanced権限レベル）	N/A	watchdogリセットイベントでシステムの詳細情報を収集する設定を表示するか、watchdogリセットイベント中に収集されたシステムの詳細情報を表示するか、収集されたシステム詳細情報をクリアする

状況	使用するSPコマンド	使用するBMCコマンド	このONTAPコマンドを使用します…
system forensics [show	log dump	log clear]	N/A
N/A	システムコンソールにログインする	system console	system console
system node run-console	システムコンソールセッションを終了するには、Ctrl+Dキーを押します。	ノードをオンまたはオフにするか、電源の再投入を行う（電源をオフにして再度オンにする）	system power on
system power on	system node power on （advanced権限レベル）	system power off	system power off
N/A	system power cycle	system power cycle	N/A

状況	使用するSPコマンド	使用するBMCコマンド	このONTAPコマンドを使用します…
スタンバイ電源はオンのままで、SPを中断することなく稼働させます。電源再投入の場合は、電源は一時的に停止したあと、再度オンになります。 これらのコマンドを使用してノードの電源をオフにするか再投入すると、ノードが誤ってシャットダウンされる（*dirty shutdown*）ことがあります。この方法は、ONTAPコマンドを使用した正常なシャットダウンの代わりにはなりません。`system node halt`	コアダンプを作成してノードをリセットする	`system core[-f]` オプションを指定する `-f` と、コアダンプが強制的に作成され、ノードがリセットされます。	`system core`

状況	使用するSPコマンド	使用するBMCコマンド	このONTAPコマンドを使用します…
`system node coredump trigger` （advanced権限レベル）	これらのコマンドの機能は、ノードでNon-maskable Interrupt（NMI）ボタンを押した場合と同じです。その結果、ノードがダーティーシャットダウンされ、ノードを停止するときにコアファイルが強制的にダンプされます。これらのコマンドは、ノード上のONTAPがハングした場合やなどのコマンドに応答しない場合に役立ち `system node shutdown`ます。生成されたコアダンプファイルは、コマンドの出力に表示され `system node coredump show`ます。SPは、ノードへの給電が遮断されないかぎり、動作可能な状態を維持します。	オプションでBIOSファームウェアイメージ（primary、backup、current）を指定してノードをリブートし、ノードのブートデバイスイメージの破損などの問題からリカバリする	`system reset` {`primary`
`backup`	`current` }	`system reset` { `current`	`primary`
`backup` }	`system node reset`と `-firmware` {`primary`	`backup`	`current` } パラメータ （advanced権限レベル）
この処理を実行すると、ノードがダーティーシャットダウンされます。 BIOSファームウェアイメージが指定されていない場合は、現在のイメージが再起動に使用されます。SPは、ノードへの給電が遮断されないかぎり、動作可能な状態を維持します。	現在のバッテリファームウェアイメージを指定したファームウェアイメージと比較する	`system battery verify[image_URL]` （advanced権限レベル） が指定されていない場合 `image_URL`、比較にはデフォルトのバッテリファームウェアイメージが使用されます。	`system battery verify[image_URL]` （advanced権限レベル） が指定されていない場合 `image_URL`、比較にはデフォルトのバッテリファームウェアイメージが使用されます。

状況	使用するSPコマンド	使用するBMCコマンド	このONTAPコマンドを使用します…
N/A	指定した場所のイメージからバッテリファームウェアを更新します。	`system battery flash [image_URL]` （advanced権限レベル） このコマンドは、何らかの理由でバッテリファームウェアの自動アップグレードプロセスが失敗した場合に使用します。	N/A

N/A	指定された場所にあるイメージを使用して、 SP/ BMC/ ONTAPファームウェアを更新します。	`sp update`
		
		`image_URL`
		
		`image_URL`200文字を超えてはなりません。
			`bmc update`
			
			`image_URL`
			
			`image_URL`200文字を超えてはなりません。

`system service-processor image update`	SP/ BMC/ ONTAPを再起動します	`sp reboot`	`bmc reboot`
`system service-processor reboot-sp`	NVRAMフラッシュコンテンツを消去する	`system nvram flash clear` （advanced権限レベル） このコマンドは、コントローラの電源がオフのときは開始できません(`system power off`)。	N/A
N/A	SP/ BMC/ ONTAP CLIを終了します	`exit`	`exit`

関連情報

- "ONTAPコマンド リファレンス"

しきい値ベースのSPセンサーの読み取り値とステータスを使用したONTAPノードの健全性監視

しきい値ベースのセンサーは、さまざまなシステムコンポーネントを定期的に読み取ります。SPは、しきい値ベースのセンサーの読み取り値を、コンポーネントで許容される動作条件を定義する事前設定されたしきい値制限と比較します。

SP は、センサーの読み取り値に基づいてセンサーの状態を表示し、コンポーネントの状態の監視に役立ちま

す。

しきい値ベースのセンサーには、システム温度、電圧、電流、ファン速度のセンサーなどがあります。しきい値ベースのセンサーのリストは、プラットフォームによって異なります。

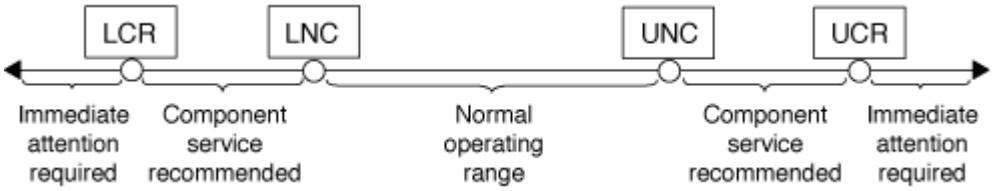
しきい値ベースのセンサーには次のしきい値があり、SPコマンドの出力に表示されます。 `system sensors`

- 異常 - 下限（ LCR ）
- 異常 - 下限（ LNC ）
- 異常 - 上限（ UNC ）
- 重大 - 上限（ UCR ）

センサー読み取り値が LNC と LCR の間、または UNC と UCR の間の場合は、コンポーネントが問題の兆候を示しており、その結果、システムに障害が発生する可能性があることを示します。そのため、コンポーネントの保守をすぐに計画する必要があります。

センサーの読み取り値が LCR 以下、または UCR 以上の場合は、コンポーネントが誤動作しており、システム障害が発生しつつあることを意味します。したがって、コンポーネントに対して緊急な対応が必要です。

次の図に、しきい値と対応する重大度の範囲を示します。



しきい値ベースのセンサーの読み取り値は、コマンド出力の列で `system sensors`確認できます `Current`。コマンドは `system sensors get sensor_name`、指定したセンサーに関するその他の詳細を表示します。読み取り値が異常および重大のしきい値を超えると、センサーは重大度が上昇していることを報告します。読み取り値がしきい値を超えると、しきい値の超過に応じて、コマンド出力に表示されるセンサーのステータスが `system sensors`から `nc`（非クリティカル）または `cr`（クリティカル）に変わり `ok`、SELイベントログにイベントメッセージが記録されます。

しきい値ベースのセンサーには、 4 つのしきい値レベルが全部揃っていないものもあります。これらのセンサーのしきい値がない場合、 `system sensors`コマンド出力にはしきい値が表示さ `na`れます。これは、特定のセンサーに該当するしきい値または重大度が設定されていないことを示し、SPはそのしきい値についてセンサーを監視しません。

system sensorsコマンド出力の例を示します

次の例は、コマンドでSP CLIに表示される情報の一部を示してい `system sensors`ます。

```
SP node1> system sensors

Sensor Name       | Current    | Unit        | Status| LCR        | LNC
| UNC        | UCR
------------------+------------+-------------+-------+------------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
CPU1_Temp_Margin | -56.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
In_Flow_Temp      | 32.000     | degrees C   | ok    | 0.000      | 10.000
| 42.000     | 52.000
Out_Flow_Temp     | 38.000     | degrees C   | ok    | 0.000      | 10.000
| 59.000     | 68.000
CPU1_Error        | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Therm_Trip   | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Hot          | 0x0        | discrete    | 0x0180| na         | na
| na         | na
IO_Mid1_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
IO_Mid2_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
CPU_VTT           | 1.106      | Volts       | ok    | 1.028      | 1.048
| 1.154      | 1.174
CPU0_VCC          | 1.154      | Volts       | ok    | 0.834      | 0.844
| 1.348      | 1.368
3.3V              | 3.323      | Volts       | ok    | 3.053      | 3.116
| 3.466      | 3.546
5V                | 5.002      | Volts       | ok    | 4.368      | 4.465
| 5.490      | 5.636
STBY_1.8V         | 1.794      | Volts       | ok    | 1.678      | 1.707
| 1.892      | 1.911
…
```

しきい値ベースのセンサーの**system sensors sensor_name**コマンド出力の例

次の例は、しきい値ベースのセンサー5VについてSP CLIにコマンドを入力した結果を示して `system sensors get` `sensor_name`います。

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID               : 5V (0x13)
 Entity ID              : 7.97
 Sensor Type (Analog)   : Voltage
 Sensor Reading         : 5.002 (+/- 0) Volts
 Status                 : ok
 Lower Non-Recoverable  : na
 Lower Critical         : 4.246
 Lower Non-Critical     : 4.490
 Upper Non-Critical     : 5.490
 Upper Critical         : 5.758
 Upper Non-Recoverable  : na
 Assertion Events       :
 Assertions Enabled     : lnc- lcr- ucr+
 Deassertions Enabled   : lnc- lcr- ucr+
```

system sensorコマンド出力の**ONTAP SP**センサーステータス値

ディスクリートセンサーにはしきい値がありません。SP CLIコマンド出力の列の `system sensors`下に表示されるこれらの読み取り値は `Current、実際の意味を持たないため、SPでは無視されます。コマンド出力の列には system sensors、`Status`ディスクリートセンサーのステータス値が16進形式で表示されます。

ディスクリートセンサーの例としては、ファン、電源ユニット（ PSU ）エラー、システムエラーのセンサーがあります。ディスクリートセンサーの具体的なリストは、プラットフォームによって異なります。

SP CLIのコマンドを使用すると、ほとんどのディスクリートセンサーのステータス値を解釈できます `system sensors get sensor_name`。次の例は、ディスクリートセンサーCPU0_ErrorおよびIO_Slot1_Presentに対してを実行した結果を示してい `system sensors get `sensor_name`ます。

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID               : CPU0_Error (0x67)
 Entity ID              : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted        : Digital State
                          [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID               : IO_Slot1_Present (0x74)
 Entity ID              : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted        : Availability State
                          [Device Present]
```

コマンドで `system sensors get` `sensor_name`はほとんどのディスクリートセンサーのステータス情報が表示されますが、System_FW_Status、System_Watchdog、PSU1_Input_Type、およびPSU2_Input_Typeディスクリートセンサーのステータス情報は提供されません。これらのセンサーのステータス情報は、次の情報を使用して解釈できます。

System_FW_Status の場合

System_FW_Statusセンサーの状態は、の形式で表示されます `0xAABB`。と `BB`の情報を組み合わせて、センサーの状態を判断できます `AA`。

`AA`次のいずれかの値を指定できます。

値	センサの状態
01	システムファームウェアのエラーです
02	システムファームウェアがハングした
04	システムファームウェア実行中です

`BB`次のいずれかの値を指定できます。

値	センサの状態
00	システムソフトウェアが正常にシャットダウンされました
01	メモリを初期化しています
02	NVMEM を初期化しています（ NVMEM がある場合）
04	メモリコントローラのハブ（ MCH ）値をリストアしています（ NVMEM がある場合）
05	ユーザがセットアップを開始しました

値	センサの状態
13	オペレーティングシステムまたは LOADER を起動しています
1F	BIOS を起動しています
20	LOADER が実行されています
21	LOADER がプライマリ BIOS ファームウェアをプログラミングしています。システムの電源を切らないでください
22	LOADER が代替 BIOS ファームウェアをプログラミングしています。システムの電源を切らないでください
2F	ONTAP が実行されています
60	SP によってシステムの電源が切断されました
61	SP によってシステムの電源がオンになりました
62	SP によってシステムがリセットされました
63	SP watchdog 電源再投入
64	SP watchdogコールドリセット

たとえば、 System_FW_Status センサーのステータス 0x042F は、「システムファームウェアが進行中（ 04 ）で、 ONTAP が実行中（ 2F ）」という意味です。

System_Watchdog

System_Watchdog センサーの状態は次のいずれかです。

- * 0x0080*

  このセンサーの状態は変更されていません

値	センサの状態
0x0081	タイマー割り込み
0x0180	タイマー期限切れ

値	センサの状態
0x0280	ハードリセット
0x0480	電源オフ
0x0880	電源再投入

たとえば、System_Watchdogセンサーのステータス0x0880は、ウォッチドッグタイムアウトが発生し、システムの電源が再投入されたことを意味します。

PSU1_Input_Typeおよび**PSU2_Input_Type**

直流（ DC ）電源の場合、 PSU1_Input_Type および PSU2_Input_Type センサーは適用されません。交流（ AC ）電源の場合、センサーのステータスは次のいずれかの値になります。

値	センサの状態
0x01 xx	220V PSUタイプ
0x02 xx	110V PSUタイプ

たとえば、 PSU1_Input_Type センサーのステータス 0x0280 は、 PSU タイプが 110V であるとセンサーが報告していることを意味します。

サービスプロセッサ管理用の**ONTAP**コマンド

ONTAPには、SPネットワーク設定、SPファームウェアイメージ、SPへのSSHアクセス、一般的なSP管理など、SPを管理するためのコマンドが用意されています。

SPネットワーク設定の管理用コマンド

状況	実行する **ONTAP** コマンド
指定したサブネットのIPv4またはIPv6アドレスファミリーを使用するように、SP用のSP自動ネットワーク設定を有効にする	`system service-processor network auto-configuration enable`
指定したサブネットのIPv4またはIPv6アドレスファミリーを使用するSPの自動ネットワーク設定を無効にするSP	`system service-processor network auto-configuration disable`
SPの自動ネットワーク設定を表示する	`system service-processor network auto-configuration show`

状況	実行する **ONTAP** コマンド
ノードのSPネットワークを手動で設定します。これには、次の項目が含まれます。 • IPアドレスファミリー（IPv4またはIPv6） • 指定したIPアドレスファミリーのネットワークインターフェイスを有効にするかどうか • IPv4を使用している場合、DHCPサーバのネットワーク設定と指定したネットワークアドレスのどちらを使用するか • SPのパブリックIPアドレス • SPのネットマスク（IPv4を使用している場合） • SPのサブネットマスクのネットワークプレフィックス長（IPv6を使用している場合） • SPのゲートウェイIPアドレス	`system service-processor network modify`
次のようなSPネットワーク設定を表示します。 • 設定されているアドレスファミリー（IPv4またはIPv6）および有効かどうか • リモート管理デバイスのタイプ • 現在のSPステータスとリンクステータス • ネットワーク設定（IPアドレス、MACアドレス、ネットマスク、サブネットマスクのプレフィックス長、ルータが割り当てたIPアドレス、リンクローカルIPアドレス、ゲートウェイIPアドレスなど） • SPが最後に更新された時刻 • SPの自動設定に使用されるサブネットの名前 • ルータによって割り当てられたIPv6 IPアドレスが有効かどうか • SPネットワークのセットアップステータス • SPネットワークのセットアップに失敗した理由	`system service-processor network show` SPネットワークの詳細をすべて表示するには、パラメータが必要です `-instance`。
次のようなSP APIサービス設定を変更します。 • SP APIサービスで使用されるポートの変更 • SP APIサービスの有効化と無効化	`system service-processor api-service modify` （advanced権限レベル）

状況	実行する **ONTAP** コマンド
SP APIサービス設定を表示する	`system service-processor api-service show` （advanced権限レベル）
SP APIサービスで内部通信に使用するSSL証明書とSSH証明書を更新する	• ONTAP 9 .5以降の場合： `system service-processor api-service renew-internal-certificates` • ONTAP 9 .4以前の場合： `system service-processor api-service renew-certificates` （advanced権限レベル）

SPファームウェアイメージの管理用コマンド

状況	実行する **ONTAP** コマンド
現在インストールされているSPファームウェアイメージの次のような詳細を表示します。 • リモート管理デバイスのタイプ • SPが起動されるイメージ（プライマリまたはバックアップ）、そのステータス、およびファームウェアバージョン • ファームウェアの自動更新が有効かどうかと、最新の更新ステータス	`system service-processor image show` パラメータは、 `-is-current`インストールされているファームウェアのバージョンが最新である場合ではなく、SPが現在ブートされているイメージ（プライマリまたはバックアップ）を示します。
SPの自動ファームウェア更新を有効または無効にする	`system service-processor image modify` デフォルトでは、SPファームウェアは、ONTAPの更新時、または新しいバージョンのSPファームウェアを手動でダウンロードしたときに、自動的に更新されます。自動更新を無効にすると、ONTAPイメージとSPファームウェアイメージの組み合わせが最適でなくなる、または無効になる可能性があるため、無効にしないことを推奨します。

状況	実行する **ONTAP** コマンド
ノードにSPファームウェアイメージを手動でダウンロードする	`system node image get` コマンドを実行する前に `system node image`、権限レベルをadvancedに設定する必要があり(`set -privilege advanced`ます）。続行するかどうかを尋ねられたら、「* y *」と入力します。 SPファームウェアイメージはONTAPに同梱されています。ONTAPに同梱されているものとは異なるSPファームウェアバージョンを使用する場合を除き、SPファームウェアを手動でダウンロードする必要はありません。
ONTAPからトリガーされた最新のSPファームウェア更新のステータス（次の情報を含む）を表示する • 最新のSPファームウェアアップデートの開始時刻と終了時刻 • 更新が進行中かどうかと進行状況	`system service-processor image update-progress show`

SPへの**SSH**アクセスの管理用コマンド

状況	実行する **ONTAP** コマンド
指定したIPアドレスのみにSPアクセスを許可する	`system service-processor ssh add-allowed-addresses`
指定したIPアドレスによるSPへのアクセスをブロックする	`system service-processor ssh remove-allowed-addresses`
SPにアクセスできるIPアドレスを表示する	`system service-processor ssh show`

一般的な**SP**管理用コマンド

状況	実行する **ONTAP** コマンド
次のような一般的なSP情報を表示します。 • リモート管理デバイスのタイプ • 現在のSPステータス • SPネットワークが設定されているかどうか • パブリックIPアドレスやMACアドレスなどのネットワーク情報 • SPファームウェアのバージョンとIntelligent Platform Management Interface（IPMI）のバージョン • SPファームウェアの自動更新が有効かどうか	`system service-processor show`SPの情報をすべて表示するには、パラメータが必要です `-instance。
ノードのSPをリブートします。	`system service-processor reboot-sp`
指定したノードから収集されたSPログファイルを含むAutoSupportメッセージを生成して送信する	`system node autosupport invoke-splog`
クラスタ内で収集されたSPログファイルの割り当てマップを表示する（収集元の各ノードに存在するSPログファイルのシーケンス番号を含む）	`system service-processor log show-allocations`

関連情報

"ONTAPコマンド リファレンス"

BMC管理用の**ONTAP**コマンド

ここでは、 Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）に対してサポートされる ONTAP コマンドを示します。

BMC では、 Service Processor （ SP ；サービスプロセッサ）と同じコマンドをいくつか使用します。BMC では次の SP コマンドがサポートされます。

状況	使用するコマンド
BMC の情報を表示します	**`system service-processor show`**
BMC のネットワーク設定を表示または変更します	**`system service-processor network show/modify`**
BMC をリセットします	**`system service-processor reboot-sp`**
現在インストールされている BMC ファームウェアイメージの詳細を表示または変更します	**`system service-processor image show/modify`**

状況	使用するコマンド
BMC ファームウェアを更新します	**system service-processor image update**
最新の BMC ファームウェア更新のステータスを表示します	**system service-processor image update-progress show**
BMC の自動ネットワーク設定を有効にして、指定したサブネットの IPv4 または IPv6 アドレスを使用するように設定します	**system service-processor network auto-configuration enable**
BMC 用に指定したサブネットで、 IPv4 アドレスまたは IPv6 アドレスの自動ネットワーク設定を無効にします	**system service-processor network auto-configuration disable**
BMCの自動ネットワーク設定を表示する	**system service-processor network auto-configuration show**

BMC ファームウェアでサポートされていないコマンドを実行すると、次のエラーメッセージが返されます。

```
::> Error: Command not supported on this platform.
```

関連情報

- "system service-processor"

ONTAPベースボード管理コントローラでサポートされる**CLI**コマンド

BMC には SSH を使用してログインできます。BMC コマンドラインでは次のコマンドがサポートされます。

コマンド	機能
システム	すべてのコマンドのリストを表示します。
システムコンソール	システムのコンソールに接続します。セッションを終了するには、を使用し `Ctrl+D`ます。
システムコア	システムコアをダンプしてリセットします。
システムの電源を再投入します	システムの電源をオフにしてからオンにします。
システムの電源がオフになりました	システムの電源をオフにします。
システムの電源が入っている	システムの電源をオンにします。

コマンド	機能
システム電源ステータス	システムの電源ステータスを出力します。
システムリセット	システムをリセットします。
システムログ	システムコンソールログを出力します。
system fru show [id]	すべてまたは選択した Field Replaceable Unit （ FRU ；フィールド交換可能ユニット）の情報をダンプします。

ONTAPクラスタ時間の管理（クラスタ管理者のみ）

クラスタ時間が不正確だと問題が発生する可能性があります。ONTAPではクラスタのタイム ゾーン、日付、時刻を手動で設定できますが、クラスタ時間を同期する場合はネットワーク タイム プロトコル（NTP）サーバを設定する必要があります。

ONTAP 9 .5以降では、対称認証を使用してNTPサーバを設定できます。

NTPは常に有効です。ただし、クラスタを外部の時間ソースと同期するには、設定が必要です。ONTAPでは、次の方法でクラスタのNTP設定を管理できます。

- 最大10台の外部NTPサーバをクラスタに関連付ける(`cluster time-service ntp server create`ことができます）。
  - タイムサービスの冗長性と品質を高めるには、少なくとも3台の外部NTPサーバをクラスタに関連付ける必要があります。
  - NTPサーバは、IPv4またはIPv6アドレス、または完全修飾ホスト名を使用して指定できます。
  - 使用するNTPバージョン（v3またはv4）を手動で指定できます。

    デフォルトでは、ONTAPは指定された外部NTPサーバでサポートされているNTPバージョンを自動的に選択します。

  指定したNTPバージョンがNTPサーバでサポートされていない場合は、時間を交換できません。

  - advanced権限レベルでは、クラスタに関連付けられている外部NTPサーバを、クラスタ時間を修正および調整するためのプライマリ時間ソースとして指定できます。
- クラスタに関連付けられているNTPサーバを表示でき(`cluster time-service ntp server show`ます）。
- クラスタのNTP設定を変更でき(`cluster time-service ntp server modify`ます）。
- クラスタと外部NTPサーバの関連付けを解除でき(`cluster time-service ntp server delete`ます）。
- advanced権限レベルでは、クラスタに関連付けられているすべての外部NTPサーバをクリアすることで設定をリセットでき(`cluster time-service ntp server reset`ます。

クラスタに参加するノードは、自動的にクラスタのNTP設定を採用します。

ONTAPでは、NTPを使用できるだけでなく、クラスタ時間を手動で管理することもできます。この機能は、

誤った時間を修正する必要がある場合（リブート後にノードの時間が大幅にずれた場合など）に役立ちます。その場合は、NTPが外部のタイムサーバと同期できるようになるまで、クラスタのおおよその時間を指定できます。手動で設定した時間は、クラスタ上のすべてのノードに反映されます。

クラスタ時間を手動で管理するには、次の方法があります。

- クラスタのタイムゾーン、日付、時刻を設定または変更でき(`cluster date modify`ます）。
- クラスタの現在のタイムゾーン、日付、時刻の設定を表示でき(`cluster date show`ます）。

> 手動でのクラスタの日付や時刻の変更は、ジョブスケジュールには反映されません。ジョブは、ジョブが作成された時点または最後に実行された時点のクラスタの時刻に基づいて実行されます。そのため、クラスタの日付や時刻を手動で変更した場合は、コマンドと `job history show`コマンドを使用して、スケジュール済みのすべてのジョブが必要に応じてキューに格納されているか完了していることを確認する必要があります `job show`。

クラスタ時間の管理用コマンド

クラスタのNTPサーバを管理するには、コマンドを使用し `cluster time-service ntp server`ます。クラスタ時間を手動で管理するには、コマンドを使用し `cluster date`ます。

ONTAP 9 .5以降では、対称認証を使用してNTPサーバを設定できます。

次のコマンドを使用して、クラスタのNTPサーバを管理できます。

状況	使用するコマンド
クラスタを外部NTPサーバと対称認証を使用せずに関連付ける	`cluster time-service ntp server create -server server_name`
ONTAP 9 .5以降で対称認証を使用してクラスタを外部NTPサーバと関連付けます。	`cluster time-service ntp server create -server server_ip_address -key-id key_id` > は、 `key_id`「cluster time-service ntp key」で設定された既存の共有キーを参照する必要があります。
既存のNTPサーバの対称認証を有効にする必要なキーIDを追加することで、既存のNTPサーバを変更して認証を有効にすることができます。 ONTAP 9 .5以降で使用可能	`cluster time-service ntp server modify -server server_name -key-id key_id`
対称認証を無効にする	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`

状況	使用するコマンド
共有NTPキーを設定する	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共有キーはIDで参照されます。ID、そのタイプ、および値がノードとNTPサーバの両方で同じである必要があります。
クラスタに関連付けられているNTPサーバに関する情報を表示する	`cluster time-service ntp server show`
クラスタに関連付けられている外部NTPサーバの設定を変更する	`cluster time-service ntp server modify`
クラスタとNTPサーバの関連付けを解除する	`cluster time-service ntp server delete`
すべての外部NTPサーバのクラスタとの関連付けを消去して設定をリセットする	`cluster time-service ntp server reset` このコマンドにはadvanced権限レベルが必要です。

次のコマンドによって、手動でクラスタ時間を管理できます。

状況	使用するコマンド
タイムゾーン、日付、時刻を設定または変更する	`cluster date modify`
クラスタのタイムゾーン、日付、および時刻の設定を表示する	`cluster date show`

関連情報

- "cluster date show"
- "cluster date modify"
- "クラスタタイムサービスNTP"
- "ジョブの表示"

バナーと**MOTD**の管理

ONTAPのログインバナーと**Message-of-The-Day**のテキストを確認する

ONTAPでは、ログインバナーまたはMessage Of The Day（MOTD）を設定して、クラスタまたはStorage Virtual Machine（SVM）のSystem ManagerおよびCLIユーザに管理

情報を提供できます。

バナーは、ユーザにパスワードなどの認証を要求する前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。たとえば、バナーを使用して、システムへのログインを試行したユーザに次のような警告メッセージを表示することができます。

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

MOTD は、ユーザの認証後、クラスタシェルプロンプトが表示される前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。たとえば、 MOTD を使用して、認証されたユーザに次のような情報メッセージを表示することができます。

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

バナーまたはMOTDの内容は、コマンドまたは `security login motd modify`コマンドを使用して次の方法で作成または変更できます `security login banner modify`。

- CLI の対話型モードまたは非対話型モードを使用して、バナーまたは MOTD に使用するテキストを指定できます。

  対話型モードでは、または `-uri`パラメータを指定せずにコマンドを実行すると起動されます。このモードで `-message`は、メッセージに改行（行末とも呼ばれます）を使用できます。

  パラメータを使用してメッセージ文字列を指定する非対話型モードで `-message`は、改行はサポートされません。

- バナーまたは MOTD に使用する内容を FTP または HTTP からアップロードできます。
- 動的な内容を表示するように MOTD を設定できます。

  MOTD には、たとえば次のような情報を動的に表示することができます。

  - クラスタ名、ノード名、または SVM 名
  - クラスタの日付と時刻
  - ログインしているユーザの名前
  - ユーザによるクラスタのノードへの前回のログイン

- ログインしたデバイスの名前または IP アドレス
- オペレーティングシステムの名前
- ソフトウェアリリースバージョン
- 有効なクラスタバージョン文字列

バナーでは動的な内容はサポートされていません。動的に生成される内容をMOTDに表示するためのエスケープシーケンスの詳細については、およびを参照してください。 `security login motd modify`"ONTAPコマンド リファレンス"

バナーと MOTD はクラスタレベルまたは SVM レベルで管理できます。

- バナーには次の特徴があります。
  - クラスタ用に設定したバナーは、バナーメッセージが定義されていない SVM に対しても表示されます。
  - SVM ごとに SVM レベルのバナーを設定できます。

    このバナーが設定された SVM では、クラスタレベルのバナーが設定されていても、 SVM レベルのバナーだけが表示されます。
- MOTD には次の特徴があります。
  - クラスタに設定したMOTDは、デフォルトですべてのSVMに対しても有効になります。
  - さらに、SVMごとにSVMレベルのMOTDを設定できます。

    この場合、 SVM にログインしたユーザには、クラスタレベルと SVM レベルの 2 つの MOTD が表示されます。
  - クラスタレベルの MOTD を有効にするか無効にするかは、クラスタ管理者が SVM 単位で設定できます。

    クラスタ管理者が SVM でクラスタレベルの MOTD を無効にした場合、その SVM にログインしたユーザにはクラスタレベルの MOTD は表示されません。

ONTAPのログインバナーを作成する

バナーを作成して、クラスタまたはSVMへのアクセスを試みたユーザにメッセージを表示できます。バナーは、ユーザに認証を要求する前に、コンソールセッション（クラスタアクセスのみ）またはSSHセッション（クラスタアクセスまたはSVMアクセス）に表示されます。

手順

1. コマンドを使用し `security login banner modify`て、クラスタまたはSVM用のバナーを作成します。

状況	そしたら...。
1行のメッセージを指定する	`<text>`パラメータを使用し `-message`てテキストを指定します。

状況	そしたら...。
メッセージに改行(行末とも呼ばれる)を含める	または `-uri`パラメータを指定せずにコマンドを実行する `-message`と、対話型モードでバナーを編集できます。
バナーに使用するコンテンツを場所からアップロードする	パラメータを使用し `-uri`て、コンテンツのFTPまたはHTTPの場所を指定します。

バナーの最大サイズは、改行も含めて 2 、 048 バイトまでです。

パラメータを使用して作成されたバナーは `-uri`静的です。ソースコンテンツのその後の変更を反映して自動的に更新されることはありません。

クラスタ用に作成したバナーは、既存のバナーがないすべてのSVMに対しても表示されます。以降にSVM用のバナーを作成すると、そのSVMに対してはクラスタレベルのバナーではなくそのバナーが表示されます。パラメータに二重引用符で囲まれ(`"-"`たハイフンを指定）を指定する `-message`と、クラスタレベルのバナーを使用するようにSVMがリセットされます。

2. コマンドを使用して、作成したバナーが表示されることを確認します `security login banner show`。

   パラメータに空の文字列を指定する `-message(`""`と、内容のないバナーが表示されます。

   パラメータをに `"-"`指定する `-message`と、バナーが設定されていないすべてのSVM（管理またはデータ）が表示されます。

バナーの作成例

次の例では、非対話型モードを使用して「 cluster1 」クラスタ用のバナーを作成しています。

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

次の例では、対話型モードを使用してSVM用のバナーを作成して `svm1`います。

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0         1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

次の例は、作成されたバナーを表示します。

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

関連情報

- バナーの管理
- "セキュリティログインバナーの変更"
- "security login banner showのコマンドです"

ONTAPクラスタレベルおよび**SVM**レベルで表示されるバナーテキストを管理します。

バナーはクラスタレベルまたは SVM レベルで管理できます。クラスタ用に設定したバナーは、バナーメッセージが定義されていない SVM に対しても表示されます。以降に SVM 用のバナーを作成すると、その SVM に対しては、クラスタ用のバナーではなくそ

のバナーが表示されます。

選択肢

- クラスタレベルのバナーの管理タスクを次に示します。

状況	そしたら...。
すべてのログインセッションに対して表示するバナーを作成する	クラスタレベルのバナーを設定します。 `security login banner modify -vserver <cluster_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	すべてのログイン（クラスタと SVM の両方）に対するバナーを削除する
バナーを空の文字列 (``) に設定します。 `security login banner modify -vserver * -message`	SVM管理者が作成したバナーを上書きする
SVMのバナーメッセージを変更します。 `security login banner modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }`

- SVMレベルのバナーの管理タスクを次に示します。

  SVMのコンテキストでは、を指定する `-vserver <svm_name>`必要はありません。

状況	そしたら...。
クラスタ管理者が指定したバナーの代わりに SVM 用の別のバナーを表示する	SVM用のバナーを作成します。 `security login banner modify -vserver <svm_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	クラスタ管理者が指定したバナーも含め、いずれのバナーも SVM に対して表示されないようにする
SVMのSVMバナーを空の文字列に設定します。 `security login banner modify -vserver <svm_name> -message`	現在 SVM レベルのバナーを使用している SVM でクラスタレベルのバナーを使用している場合

関連情報

- "セキュリティログインバナーの変更"

ONTAPユーザ向けのmessage-of-the-dayテキストの作成

Message Of The Day（MOTD）を作成して、認証されたCLIユーザに情報を伝達できます。MOTD は、ユーザの認証後、クラスタシェルプロンプトが表示される前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。

手順

1. コマンドを使用し `security login motd modify`て、クラスタまたはSVMのMOTDを作成します。

状況	そしたら...。
1行のメッセージを指定する	`text`パラメータを使用し `-message`てテキストを指定します。
改行を含める(行末とも呼ばれる)	または `-uri`パラメータを指定せずにコマンドを実行する `-message`と、対話型モードでMOTDを編集できます。
MOTDに使用するコンテンツを場所からアップロードする	パラメータを使用し `-uri`て、コンテンツのFTPまたはHTTPの場所を指定します。

   MOTDの最大サイズは、改行を含めて2、048バイトです。

   `Security login motd modify`動的に生成される内容をMOTDに表示するためのエスケープシーケンスについて説明します。

   パラメータを使用して作成されたMOTD `-uri`は静的です。ソースコンテンツのその後の変更を反映して自動的に更新されることはありません。

   クラスタ用に作成した MOTD は、デフォルトでは、各 SVM に対して個別に作成した SVM レベルの MOTD と一緒に、すべての SVM ログインに対しても表示されます。SVMのパラメータをに `false`設定する `-is-cluster-message-enabled`と、そのSVMに対するクラスタレベルのMOTDは表示されません。

2. コマンドを使用して、作成されたMOTDが表示されることを確認します `security login motd show`。

   指定する `-message`空の文字列 （`） を持つパラメータは、構成されていない、またはコンテンツのない MOTD を表示します。

   動的に生成されるコンテンツをMOTDに表示するためのパラメータとの詳細については、"ONTAPコマンド リファレンス"を参照してください `security login motd modify`。

MOTDの作成例

次の例では、非対話型モードを使用して、 `cluster1`クラスタ：

```
cluster1::> security login motd modify -message "Greetings!"
```

次の例では、対話型モードを使用して、 `svm1`エスケープ シーケンスを使用して動的に生成されたコンテンツを表示する SVM:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

次の例は、作成したMOTDを表示します。

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

の詳細については `security login motd show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPクラスタレベルおよび**SVM**レベルで表示される**Message-of-The-Day**テキストを管理します。

Message Of The Day（MOTD）はクラスタレベルまたはSVMレベルで管理できます。クラスタに設定したMOTDは、デフォルトですべてのSVMに対しても有効になります。さらに、SVMごとにSVMレベルのMOTDを設定できます。クラスタレベルのMOTDは、クラスタ管理者が各SVMに対して有効または無効にできます。

MOTDのコンテンツを動的に生成するために使用できるの詳細については"エスケープシーケンス"、ONTAPの

コマンドリファレンスを参照してください。

選択肢

- クラスタレベルでMOTDを管理します。

状況	そしたら...。
既存のMOTDがない場合にすべてのログインに対するMOTDを作成する	クラスタレベルのMOTDを設定します。 `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	SVMレベルのMOTDが設定されていない場合にすべてのログインに対するMOTDを変更する
クラスタレベルのMOTDを変更します。 `security login motd modify -vserver <cluster_name> { [-message "<text>"] }	[-uri <ftp_or_http_addr>] }`
SVMレベルのMOTDが設定されていない場合にすべてのログインに対するMOTDを削除する	クラスタレベルのMOTDを空の文字列に設定し(`""`ます）。 `security login motd modify -vserver <cluster_name> -message ""`
すべてのSVMで、SVMレベルのMOTDを使用するのではなく、クラスタレベルのMOTDを表示する	クラスタレベルのMOTDを設定してから、SVMレベルのすべてのMOTDを空の文字列に設定し、クラスタレベルのMOTDを有効にします。 a. `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` .. `security login motd modify { -vserver !"<cluster_name>" } -message "" -is -cluster-message-enabled true`	クラスタレベルのMOTDを使用せずに、選択したSVMについてのみMOTDを表示する
クラスタレベルのMOTDを空の文字列に設定し、選択したSVMに対するSVMレベルのMOTDを設定します。 a. `security login motd modify -vserver <cluster_name> -message ""` b. `security login motd modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }` + この手順は、必要に応じてSVMごとに繰り返すことができます。

状況	そしたら...。
すべてのSVM（データと管理）に対して同じSVMレベルのMOTDを使用する	同じMOTDを使用するようにクラスタとすべてのSVMを設定します。 `security login motd modify -vserver * { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` [NOTE] ==== CLIの対話型モードでは、クラスタと各SVMについてMOTDを個別に入力するように求められます。プロンプトが表示されたら、各インスタンスに同じMOTDを貼り付けることができます。 ====	クラスタレベルのMOTDをすべてのSVMで必要に応じて表示できるようにし、クラスタログイン時に表示されないようにする
クラスタレベルのMOTDを設定し、クラスタに対する表示を無効にします。 `security login motd modify -vserver <cluster_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] } -is-cluster-message -enabled false`
一部のSVMだけでクラスタレベルとSVMレベルの両方のMOTDが設定されている場合は、クラスタレベルとSVMレベルのすべてのMOTDを削除する	MOTDに空の文字列を使用するようにクラスタとすべてのSVMを設定します。 `security login motd modify -vserver * -message ""`
他のSVMで空の文字列が使用されている場合、およびクラスタレベルで別のMOTDが使用されている場合にのみ、文字列が空でないSVMのMOTDを変更する	拡張クエリを使用して選択したMOTDを変更します。 `security login motd modify { -vserver !"<cluster_name>" -message !"" } { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	単一行または複数行のメッセージ内の任意の場所に特定のテキスト（たとえば、「January」の後に「2015」が続く）を含むすべての MOTD を表示します（テキストが複数の行に分割されている場合でも）。
クエリを使用してMOTDを表示します。 `security login motd show -message *"January"*"2015"*`	複数の連続する改行（EOL）を含むMOTDを対話型モードで作成する

- SVMレベルのMOTDを管理します。

  SVMのコンテキストでは、を指定する `-vserver <svm_name>`必要はありません。

状況	そしたら...。
すでにSVMレベルのMOTDが設定されている場合は、別のSVMレベルのMOTDを使用する	SVMレベルのMOTDを変更します。 `security login motd modify -vserver <svm_name> {[-message "<text>"]
[-uri <ftp_or_http_addr>] }`	すでにSVMレベルのMOTDが設定されている場合は、SVMでクラスタレベルのMOTDのみを使用する
SVMレベルのMOTDを空の文字列に設定し、そのSVMに対してクラスタレベルのMOTDを有効にするようにクラスタ管理者に依頼します。 a. `security login motd modify -vserver <svm_name> -message ""` b. （クラスタ管理者） `security login motd modify -vserver <svm_name> -is -cluster-message-enabled true`	現在クラスタレベルとSVMレベルの両方のMOTDが表示されているSVMに対して、SVMにどのMOTDも表示されないようにする

関連情報

- "security login motd modify のように変更します"
- "security login motd showのコマンドを使用します"

ONTAPジョブおよびジョブスケジュールを管理します。

ジョブはジョブキューに配置され、リソースが使用可能になるとバックグラウンドで実行されます。ジョブが大量のクラスタリソースを消費している場合は、そのジョブを停止するか、クラスタに対する要求が少なくなるまで一時停止できます。ジョブを監視して再開することもできます。

ジョブのカテゴリ

管理可能なジョブには、サーバ関連、クラスタ関連、プライベートの3つのカテゴリがあります。

ジョブは、次のいずれかのカテゴリに分類されます。

- * サーバ関連ジョブ *

  これらのジョブは、実行する特定のノードに対して管理フレームワークによってキューに登録されます。

- * クラスタ関連ジョブ *

  これらのジョブは、実行するクラスタ内の任意のノードに対して管理フレームワークによってキューに登

録されます。

- * プライベートジョブ *

  これらのジョブはノードに固有であり、Replicated Database（RDB；複製データベース）やその他のクラスタメカニズムは使用しません。プライベートジョブを管理するコマンドには、advanced権限レベル以上が必要です。

ジョブの管理用コマンド

あるジョブを呼び出すコマンドを入力すると、通常、ジョブがキューに登録されたというメッセージが表示され、CLIのコマンド プロンプトに戻ります。ただし、一部のコマンドではジョブの進捗状況が表示され、ジョブが完了するまでCLIのコマンド プロンプトに戻りません。このような場合は、Ctrl+Cキーを押してジョブをバックグラウンドに移動できます。

状況	使用するコマンド
すべてのジョブに関する情報を表示する	`job show`
ジョブに関する情報をノード単位で表示する	`job show bynode`
クラスタ関連ジョブに関する情報を表示する	`job show-cluster`
完了したジョブに関する情報を表示する	`job show-completed`
ジョブ履歴に関する情報を表示する	`job history show` クラスタ内の各ノードには、最大 25 、 000 個のジョブレコードが格納されます。そのため、完全なジョブ履歴を表示しようとすると時間がかかることがあります。待ち時間が長くならないようにするには、ジョブをノード、Storage Virtual Machine（SVM）、またはレコードID別に表示します。
プライベートジョブのリストを表示します。	`job private show`（advanced権限レベル）
完了したプライベートジョブに関する情報を表示する	`job private show-completed`（advanced権限レベル）
ジョブマネージャの初期化状態に関する情報を表示する	`job initstate show`（advanced権限レベル）
ジョブの進捗状況の監視	`job watch-progress`
プライベートジョブの進捗状況を監視する	`job private watch-progress`（advanced権限レベル）

状況	使用するコマンド
ジョブを一時停止する	`job pause`
プライベートジョブを一時停止する	`job private pause`（advanced権限レベル）
一時停止したジョブを再開する	`job resume`
一時停止したプライベートジョブを再開する	`job private resume`（advanced権限レベル）
ジョブを停止する	`job stop`
プライベートジョブを停止する	`job private stop`（advanced権限レベル）
ジョブの削除	`job delete`
プライベートジョブを削除する	`job private delete`（advanced権限レベル）
クラスタ関連ジョブと、そのジョブを所有している使用できないノードとの関連付けを解除し、別のノードがそのジョブの所有権を取得できるようにする	`job unclaim`（advanced権限レベル）

完了したジョブの結果は、コマンドを使用して確認できます `event log show`。の詳細については `event log show`、を"ONTAPコマンド リファレンス"参照してください。

ジョブスケジュールの管理用コマンド

多くのタスク（ボリュームSnapshotなど）は、指定したスケジュールで実行するように設定できます。特定の時間に実行されるスケジュールは、_cron_schedulesと呼ばれます（UNIXのスケジュールに似ています）。`cron`一定間隔で実行されるスケジュールは、 _interval_schedules と呼ばれます。ジョブスケジュールを管理するには、コマンドを使用し `job schedule`ます。

手動でのクラスタの日付や時刻の変更は、ジョブスケジュールには反映されません。ジョブは、ジョブが作成された時点または最後に実行された時点のクラスタの時刻に基づいて実行されます。そのため、クラスタの日付や時刻を手動で変更した場合は、コマンドと `job history show`コマンドを使用して、スケジュール済みのすべてのジョブが必要に応じてキューに格納されているか完了していることを確認する必要があり `job show`ます。

クラスタがMetroCluster構成に含まれている場合は、両方のクラスタのジョブスケジュールが同一である必要があります。そのため、ジョブスケジュールを作成、変更、または削除する場合は、リモートクラスタでも同じ処理を実行する必要があります。

状況	使用するコマンド
すべてのスケジュールに関する情報を表示する	`job schedule show`

状況	使用するコマンド
ジョブのリストをスケジュール別に表示する	`job schedule show-jobs`
cronスケジュールに関する情報を表示する	`job schedule cron show`
インターバル スケジュールに関する情報を表示する	`job schedule interval show`
cronスケジュールを作成する	`job schedule cron create` ONTAP 9.10.1以降では、ジョブ スケジュールにSVMを含めることができます。
インターバル スケジュールを作成する	`job schedule interval create` 、 `-hours`、 `-minutes`、またはの `-seconds`いずれかのパラメータを少なくとも1つ指定する必要があります `-days`。
cronスケジュールを変更する	`job schedule cron modify`
インターバルスケジュールを変更する	`job schedule interval modify`
スケジュールを削除する	`job schedule delete`
cronスケジュールを削除する	`job schedule cron delete`
インターバルスケジュールを削除する	`job schedule interval delete`

関連情報

- "ジョブ"

クラスタ構成のバックアップとリストア（クラスタ管理者のみ）

ONTAP構成バックアップファイルの詳細

構成バックアップファイルはアーカイブファイル（.7z）で、クラスタおよびクラスタ内のノードが適切に動作するために必要な、設定可能なすべてのオプションの情報が含まれています。

これらのファイルには、各ノードのローカル設定に加えて、クラスタ全体でレプリケートされる設定が格納されます。クラスタの構成をバックアップおよびリストアするには、構成バックアップファイルを使用します。

構成バックアップファイルには、次の2種類があります。

- * ノード構成バックアップファイル *

クラスタ内の正常な各ノードには、ノード構成バックアップファイルが含まれています。このファイルには、ノードがクラスタ内で正常に動作するために必要な設定情報とメタデータがすべて含まれています。

- * クラスタ構成バックアップファイル *

  これらのファイルには、クラスタ内のすべてのノード構成バックアップファイルのアーカイブと、レプリケートされたクラスタ構成情報（レプリケートされたデータベース（RDBファイル））が含まれます。クラスタ構成バックアップファイルを使用すると、クラスタ全体またはクラスタ内の任意のノードの構成をリストアできます。クラスタ構成バックアップスケジュールでは、これらのファイルが自動的に作成され、クラスタ内の複数のノードに格納されます。

構成バックアップファイルには構成情報のみが含まれています。ユーザデータは含まれません。ユーザデータのリストアについては、を参照してください"データ保護"。

ONTAPクラスタおよびノードの構成バックアップファイルのバックアップのスケジュール設定について

3種類のスケジュールで、クラスタとノードの構成バックアップファイルが自動的に作成され、クラスタ内のノード間でレプリケートされます。

構成バックアップファイルは、次のスケジュールに従って自動的に作成されます。

- 8時間ごと
- 毎日
- 毎週

それぞれの時間に、クラスタ内の正常な各ノードにノード構成バックアップファイルが作成されます。これらのノード構成バックアップファイルはすべて、レプリケートされたクラスタ構成と一緒に単一のクラスタ構成バックアップファイルに収集され、クラスタ内の1つ以上のノードに保存されます。

構成バックアップスケジュールの管理用**ONTAP**コマンド

構成バックアップスケジュールは、コマンドを使用して管理でき `system configuration backup settings`ます。

これらのコマンドはadvanced権限レベルで使用できます。

状況	使用するコマンド
構成バックアップスケジュールの設定を変更します。 • クラスタ内のデフォルトの場所に加えて、構成バックアップ ファイルがアップロードされるリモート URL (HTTP、HTTPS、FTP、または FTPS) を指定します。 • リモートURLへのログインに使用するユーザ名を指定します。 • 構成バックアップスケジュールごとに保持するバックアップ数を設定する	`system configuration backup settings modify` リモートURLでHTTPSを使用する場合は、オプションを使用し `-validate-certification`てデジタル証明書の検証を有効または無効にします。証明書の検証はデフォルトでは無効になっています。 構成バックアップファイルのアップロード先のWebサーバで、HTTPの場合はPUT処理、HTTPSの場合はPOST処理が有効になっている必要があります。詳細については、Webサーバのマニュアルを参照してください。
リモートURLへのログインに使用するパスワードを設定する	`system configuration backup settings set-password`
構成バックアップスケジュールの設定を表示する	`system configuration backup settings show` パラメータを設定する `-instance`と、各スケジュールで保持するバックアップのユーザ名と数が表示されます。

ノード構成バックアップファイルの管理用**ONTAP**コマンド

クラスタとノードの構成バックアップファイルを管理するには、コマンドを使用し `system configuration backup`ます。

これらのコマンドはadvanced権限レベルで使用できます。

状況	使用するコマンド
新しいノードまたはクラスタの構成バックアップファイルを作成する	`system configuration backup create`
クラスタ内のノードから別のノードに構成バックアップファイルをコピーする	`system configuration backup copy`

状況	使用するコマンド
クラスター内のノードからリモート URL (FTP 、HTTP、HTTPS、または FTPS) に構成バックアップ ファイルをアップロードします。	`system configuration backup upload` リモートURLでHTTPSを使用する場合は、オプションを使用し `-validate-certification`てデジタル証明書の検証を有効または無効にします。証明書の検証はデフォルトでは無効になっています。 構成バックアップ ファイルのアップロード先のWebサーバで、HTTPの場合はPUT処理、HTTPSの場合はPOST処理が有効になっている必要があります。一部の Web サーバーでは追加のモジュールをインストールする必要がある場合があります。詳細については、Webサーバのマニュアルを参照してください。サポートされるURL形式はONTAPリリースによって異なります。システム設定コマンドの詳細については、 "ONTAPコマンド リファレンス"。
リモートURLからクラスタ内のノードに構成バックアップファイルをダウンロードし、指定されている場合はデジタル証明書を検証する	`system configuration backup download` リモートURLでHTTPSを使用する場合は、オプションを使用し `-validate-certification`てデジタル証明書の検証を有効または無効にします。証明書の検証はデフォルトでは無効になっています。
クラスタ内のノードで構成バックアップファイルの名前を変更する	`system configuration backup rename`
クラスタ内の1つ以上のノードのノードおよびクラスタ構成バックアップファイルを表示する	`system configuration backup show`
ノード上の構成バックアップファイルを削除する	`system configuration backup delete` このコマンドは、指定したノードにある構成バックアップファイルのみを削除します。構成バックアップファイルがクラスタ内の他のノードにも存在する場合、ファイルはそれらのノードに残ります。

関連情報

- "システム構成のバックアップ"

ONTAPノード構成バックアップファイルを検索してノードをリストア

ノード構成をリカバリするには、リモート URL またはクラスタ内のノードにある構成バックアップファイルを使用します。

タスクの内容

ノード構成をリストアするには、クラスタまたはノード構成バックアップファイルのいずれかを使用します。

ステップ

1. 構成のリストアに必要なノードに構成バックアップファイルを利用できるようにします。

構成バックアップファイルの場所	そしたら...。
リモートURL	リカバリするノードにコマンドをダウンロードするには、advanced権限レベルで使用し `system configuration backup download`ます。
クラスタ内のノード	a. リカバリするノードの構成を含むクラスタで利用可能な構成バックアップファイルのリストを表示するには、advanced権限レベルでコマンドを使用し `system configuration backup show`ます。 b. 特定した構成バックアップファイルがリカバリノードに存在しない場合は、コマンドを使用し `system configuration backup copy`てリカバリノードにコピーします。

以前にクラスタを作成し直したことがある場合は、クラスタの再作成後に作成した構成バックアップファイルを選択します。クラスタの再作成の前に作成した構成バックアップファイルを使用する必要がある場合は、ノードをリカバリしたあとで、クラスタを再度作成する必要があります。

関連情報

- "system configuration backup copy"

ONTAPノード構成バックアップファイルを使用したノードのリストア

ノード構成をリストアするには、特定してリカバリノードに利用可能にした構成バックアップファイルを使用します。

タスクの内容

このタスクは、災害によってノードのローカル構成ファイルが失われた場合にのみ実行します。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. ノードが正常な場合は、別のノードのadvanced権限レベルで、パラメータと `-eligibility`パラメータを指

定してコマンドを `-node`実行し、ノード `cluster modify`の参加資格を無効にしてクラスタから分離します。

ノードが正常でない場合は、この手順を省略する必要があります。

この例では、node2を変更してクラスタへの参加資格を無効にし、構成をリストアできるようにします。

```
cluster1::*> cluster modify -node node2 -eligibility false
```

の詳細については `cluster modify`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドをadvanced権限レベルで使用して `system configuration recovery node restore`、ノードの構成を構成バックアップファイルからリストアします。

   名前を含むノードのIDが失われた場合は、パラメータを使用して構成バックアップファイルにノード名を指定する必要があります `-nodename-in-backup`。

   この例では、ノードに保存されているいずれかの構成バックアップファイルを使用してノードの構成をリストアしています。

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z

Warning: This command overwrites local configuration files with
         files contained in the specified backup file. Use this
         command only to recover from a disaster that resulted
         in the loss of the local configuration files.
         The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

   構成がリストアされ、ノードがリブートします。

4. ノードをクラスタの対象外にした場合は、コマンドを使用し `system configuration recovery cluster sync`てノードを対象としてマークし、クラスタと同期します。
5. SAN環境を使用している場合は、コマンドを使用し `system node reboot`てノードをリブートし、SANクォーラムを再確立します。

終了後

以前にクラスタを作成し直したことがある場合や、クラスタの再作成前に作成された構成バックアップファイルを使用してノード構成をリストアする場合は、もう一度クラスタを作成し直す必要があります。

ONTAPクラスタ構成バックアップファイルを検索してクラスタをリストア

クラスタをリカバリするには、クラスタ内のノードまたはクラスタ構成バックアップファイルのいずれかの構成を使用します。

手順

1. クラスタのリカバリに使用する構成の種類を選択します。

   - クラスタ内のノード

     クラスタが複数のノードで構成されていて、いずれかのノードにクラスタ構成が設定されている場合は、そのノードに保存されている構成を使用してクラスタをリカバリできます。

     ほとんどの場合、クラスタ構成のリストアには、最新のトランザクションIDを持つレプリケーションリングを含むノードが最適です。advanced権限レベルでコマンドを使用する `cluster ring show`と、クラスタ内の各ノードで使用可能なレプリケートリングのリストを表示できます。

   - クラスタ構成バックアップファイル

     正しいクラスタ構成のノードを特定できない場合、またはクラスタがシングルノードで構成されている場合は、クラスタ構成バックアップファイルを使用してクラスタをリカバリできます。

   クラスタを構成バックアップ ファイルからリカバリする場合、バックアップ後に行われた構成の変更はすべて失われます。リカバリ後に構成バックアップ ファイルと現在の構成との矛盾をすべて解決する必要があります。参照"NetAppナレッジベース: ONTAP構成バックアップ解決ガイド"トラブルシューティングのガイダンス。

2. クラスタ構成バックアップファイルを使用するように選択した場合は、クラスタのリカバリに使用するノードでそのファイルを使用できるようにします。

構成バックアップファイルの場所	そしたら...。
リモートURL	リカバリするノードにコマンドをダウンロードするには、advanced権限レベルで使用し `system configuration backup download`ます。
クラスタ内のノード	a. advanced権限レベルでコマンドを使用して、`system configuration backup show`クラスタが適切な構成であったときに作成されたクラスタ構成バックアップファイルを検索します。 b. クラスタのリカバリに使用するノード上にクラスタ構成バックアップファイルがない場合は、コマンドを使用し `system configuration backup copy`てリカバリするノードにコピーします。

関連情報

- "cluster ring show"
- "system configuration backup copy"

ONTAPクラスタ構成バックアップファイルを使用したクラスタのリストア

クラスタ障害後に既存の構成からクラスタ構成をリストアするには、選択したクラスタ構成をリカバリするノードで使用できるようにしてクラスタを再作成し、追加する各ノードを新しいクラスタに再追加します。

タスクの内容

このタスクは、クラスタの構成が失われた災害からリカバリする場合にのみ実行します。

> 構成バックアップファイルからクラスタを再作成する場合は、テクニカルサポートに連絡して、構成バックアップファイルとクラスタ内の構成との不一致を解決する必要があります。
>
> クラスタを構成バックアップ ファイルからリカバリする場合、バックアップ後に行われた構成の変更はすべて失われます。リカバリ後に構成バックアップ ファイルと現在の構成との矛盾をすべて解決する必要があります。参照"NetAppナレッジベース: ONTAP構成バックアップ解決ガイド"トラブルシューティングのガイダンス。

手順

1. 各HAペアのストレージフェイルオーバーを無効にします。

   storage failover modify -node *node_name* -enabled false

   ストレージフェイルオーバーを無効にする必要があるのは、HAペアごとに1回だけです。ノードのストレージフェイルオーバーを無効にすると、ノードのパートナーでもストレージフェイルオーバーが無効になります。

2. リカバリするノード以外の各ノードを停止します。

   system node halt -node *node_name* -reason "text"

   ```
   cluster1::*> system node halt -node node0 -reason "recovering cluster"

   Warning: Are you sure you want to halt the node? {y|n}: y
   ```

3. 権限レベルをadvancedに設定します。

   set -privilege advanced

4. リカバリノードで、コマンドを使用して `**system configuration recovery cluster recreate**`クラスタを再作成します。

   この例では、リカバリノードに保存されている構成情報を使用してクラスタを再作成します。

   ```
   cluster1::*> configuration recovery cluster recreate -from node

   Warning: This command will destroy your existing cluster. It will
            rebuild a new single-node cluster consisting of this node
            and its current configuration. This feature should only be
            used to recover from a disaster. Do not perform any other
            recovery operations while this operation is in progress.
   Do you want to continue? {y|n}: y
   ```

   リカバリノードに新しいクラスタが作成されます。

5. 構成バックアップファイルからクラスタを再作成する場合は、クラスタのリカバリが進行中であることを確認します。

   system configuration recovery cluster show

   正常なノードからクラスタを再作成する場合は、クラスタのリカバリ状態を確認する必要はありません。

   ```
   cluster1::*> system configuration recovery cluster show
    Recovery Status: in-progress
    Is Recovery Status Persisted: false
   ```

6. 再作成したクラスタに再追加が必要な各ノードをブートします。

   ノードは一度に1つずつリブートする必要があります。

7. 再作成したクラスタに追加する必要がある各ノードについて、次の手順を実行します。

   a. 再作成したクラスタの正常なノードから、ターゲットノードを再追加します。

      system configuration recovery cluster rejoin -node *node_name*

      この例では ' ターゲット・ノードを再作成されたクラスタに再結合します

      ```
      cluster1::*> system configuration recovery cluster rejoin -node node2

      Warning: This command will rejoin node "node2" into the local
               cluster, potentially overwriting critical cluster
               configuration files. This command should only be used
               to recover from a disaster. Do not perform any other
               recovery operations while this operation is in progress.
               This command will cause node "node2" to reboot.
      Do you want to continue? {y|n}: y
      ```

      ターゲットノードがリブートし、クラスタに追加されます。

   b. ターゲットノードが正常であり、クラスタ内の残りのノードとクォーラムを形成していることを確認します。

      cluster show -eligibility true

      別のノードを再追加する前に、ターゲットノードを再作成したクラスタに再追加する必要があります。

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. 構成バックアップファイルからクラスタを再作成した場合は、リカバリステータスをcompleteに設定します。

   system configuration recovery cluster modify -recovery-status complete

9. admin権限レベルに戻ります。

   set -privilege admin

10. クラスタが2つのノードだけで構成されている場合は、コマンドを使用し`**cluster ha modify**`てクラスタHAを再度有効にします。
11. コマンドを使用し`**storage failover modify**`て、各HAペアのストレージフェイルオーバーを再度有効にします。

終了後

クラスタにSnapMirrorピア関係が設定されている場合は、それらの関係を再作成する必要もあります。詳細については、を参照してください "データ保護"。

関連情報

- "ONTAPコマンド リファレンス"
- "storage failover modify"

ノードを**ONTAP**クラスタと同期して、クラスタ全体のクォーラムを確保する

クラスタ全体のクォーラムが存在するものの、1つ以上のノードがクラスタと同期していない場合は、ノードを同期してノード上のレプリケートされたデータベース（RDB）をリストアし、クォーラムに加える必要があります。

ステップ

1. 正常なノードから、advanced権限レベルでコマンドを使用して `system configuration recovery cluster sync`、同期されていないノードをクラスタ構成と同期します。

   次の例では、残りのクラスタとノード（ _node2 _ ）を同期します。

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

結果

RDBがノードにレプリケートされ、そのノードはクラスタへの参加資格を取得します。

ONTAPクラスタのノードコアダンプの管理（クラスタ管理者のみ）

ノードでパニックが発生すると、コアダンプが発生してシステムによってコアダンプファイルが作成され、テクニカルサポートが問題のトラブルシューティングに使用できます。コアダンプ属性を設定または表示できます。コアダンプファイルは、保存、表示、セグメント化、アップロード、削除することもできます。

コアダンプは、次の方法で管理できます。

- コアダンプの設定と設定の表示
- コアダンプの基本情報、ステータス、および属性の表示

  コアダンプファイルおよびレポートは、ノードのディレクトリに格納され `/mroot/etc/crash/`ます。コマンドまたはWebブラウザを使用して、ディレクトリの内容を表示できます `system node coredump`。

- コアダンプの内容の保存と、指定した場所またはテクニカルサポートへの保存済みファイルのアップロード

  ONTAPでは、テイクオーバー、アグリゲートの再配置、またはギブバックの実行中にコアダンプファイルの保存を開始することはできません。

- 不要になったコアダンプファイルの削除

コアダンプの管理用コマンド

コアダンプの設定を管理するにはコマンド、コアダンプファイルを管理するにはコマンド、 `system node coredump reports`アプリケーションコアレポートを管理するには `system node coredump`コマンドを使用し `system node coredump config`ます。

このトピックで説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

状況	使用するコマンド
コアダンプの設定	`system node coredump config modify`
コアダンプの設定を表示する	`system node coredump config show`
コアダンプに関する基本情報を表示する	`system node coredump show`
ノードをリブートするときにコアダンプを手動でトリガーする	`system node reboot`パラメータと `-skip-lif-migration-before-reboot`パラメータの両方を使用した場合 `-dump` link：https://docs。ONTAP lif com/us-en/lif-cli//system-node-reboot.html#parameters^]パラメータは、リブート前のNetApp[`skip-lif-migration-before-reboot`の移行をスキップするように指定しています。
ノードをシャットダウンしたときにコアダンプを手動でトリガーする	`system node halt`パラメータと `-skip-lif-migration-before-shutdown`パラメータの両方を使用した場合 `-dump` link：https://docs。NetApp .com /us-en/lif-cli/system-node-halt.html#parameters^]パラメータは、シャットダウン前のONTAP[`skip-lif-migration-before-shutdown`の移行をスキップするように指定します。
指定したコアダンプを保存する	`system node coredump save`
指定したノード上の保存されていないコアダンプをすべて保存する	`system node coredump save-all`
指定したコアダンプファイルを含むAutoSupportメッセージを生成して送信する	`system node autosupport invoke-core-upload` オプションのパラメータは、`-uri`AutoSupportメッセージのMAT送信先を指定します。
コアダンプに関するステータス情報を表示する	`system node coredump status`

状況	使用するコマンド
指定したコアダンプを削除する	`system node coredump delete`
ノード上の保存されていないコアダンプまたは保存されているすべてのコアファイルを削除する	`system node coredump delete-all`
アプリケーションコアダンプレポートを表示します。	`system node coredump reports show`
アプリケーションコアダンプレポートを削除する	`system node coredump reports delete`

関連情報

"ONTAPコマンド リファレンス"

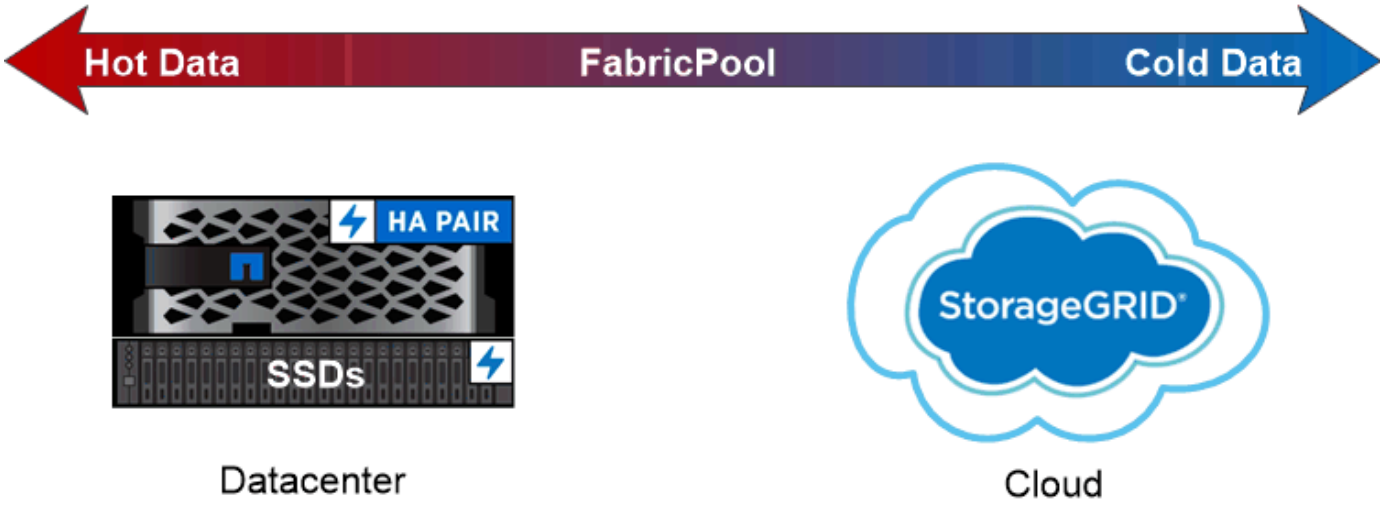
ディスクと階層の管理

ディスクと**ONTAP**ローカル階層

_Local Tiers_は_aggregates_とも呼ばれ、ノードで管理されるディスクの論理コンテナです。ローカル階層を使用すると、パフォーマンス要件が異なるワークロードを分離したり、アクセスパターンが異なるデータを階層化したり、規制要件に準拠するためにデータを分離したりできます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。

- レイテンシを最小限に抑え、パフォーマンスを最大限に高める必要があるビジネスクリティカルなアプリケーションの場合は、SSDのみで構成されるローカル階層を作成します。
- アクセスパターンに応じてデータを階層化する場合は、_hybrid local tier _を作成し、作業データセットにはフラッシュを導入して高性能なキャッシュを利用しながら、アクセス頻度が低いデータには低コストのHDDやオブジェクトストレージを使用することができます。
  - は、"Flash Pool _"SSDとHDDの両方で構成されます。
  - は"_ FabricPool _"、オブジェクトストアが接続されたオールSSDローカル階層で構成されます。
- 規制要件に準拠するためにアクティブなデータからアーカイブデータを分離する必要がある場合は、大容量HDDまたはパフォーマンスHDDと大容量HDDで構成されるローカル階層を使用できます。



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.

MetroCluster構成でのローカル階層の使用

MetroCluster構成を使用している場合は、ドキュメントの初期設定手順、およびローカル階層とディスク管理に関するガイドラインに従って"MetroCluster"ください。

関連情報

- "ローカル階層の管理"
- "ディスクの管理"
- "RAID構成の管理"
- "Flash Pool階層の管理"
- "FabricPoolクラウド階層の管理"

ローカル階層の管理

ONTAPローカル階層の管理の詳細

System ManagerまたはONTAP CLIを使用して、ローカル階層の追加、使用状況の管理、およびデータ（ディスク）の追加を行うことができます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

次のタスクを実行できます。

- "ローカル階層を追加（作成）します"

ローカル階層を追加するには、特定のワークフローに従います。ローカル階層に必要なディスクまたはディスク パーティションの数を確認し、どの方法を使用してローカル階層を作成するかを決めます。ONTAPによって割り当てられる構成でローカル階層を自動的に追加することも、手動で構成を指定することもできます。

- "ローカル階層の使用の管理"

  既存のローカル階層について、名前の変更やメディア コストの設定を行ったり、ドライブとRAIDグループの情報を確認したりできます。ローカル階層のRAID構成を変更し、Storage VM（SVM）にローカル階層を割り当てることができます。ローカル階層のRAID構成を変更し、Storage VM（SVM）にローカル階層を割り当てることができます。ローカル階層に配置されているボリュームを特定し、それらがローカル階層で使用しているスペースを確認できます。ボリュームが使用できるスペースの量を制御できます。HAペアでローカル階層の所有権を切り替えることができます。ローカル階層を削除することもできます。

- "ローカル階層へのデータ（ディスク）の追加"

  さまざまな方法を使用して、特定のワークフローに従って容量を追加します。ローカル階層にディスクを追加し、ノードまたはシェルフにドライブを追加できます。必要に応じて、スペア パーティションのミスアライメントを修正できます。

ローカル階層を追加（作成）します

ONTAPローカル階層を追加するワークフロー

ローカル階層を作成すると、システム上のボリュームにストレージが提供されます。

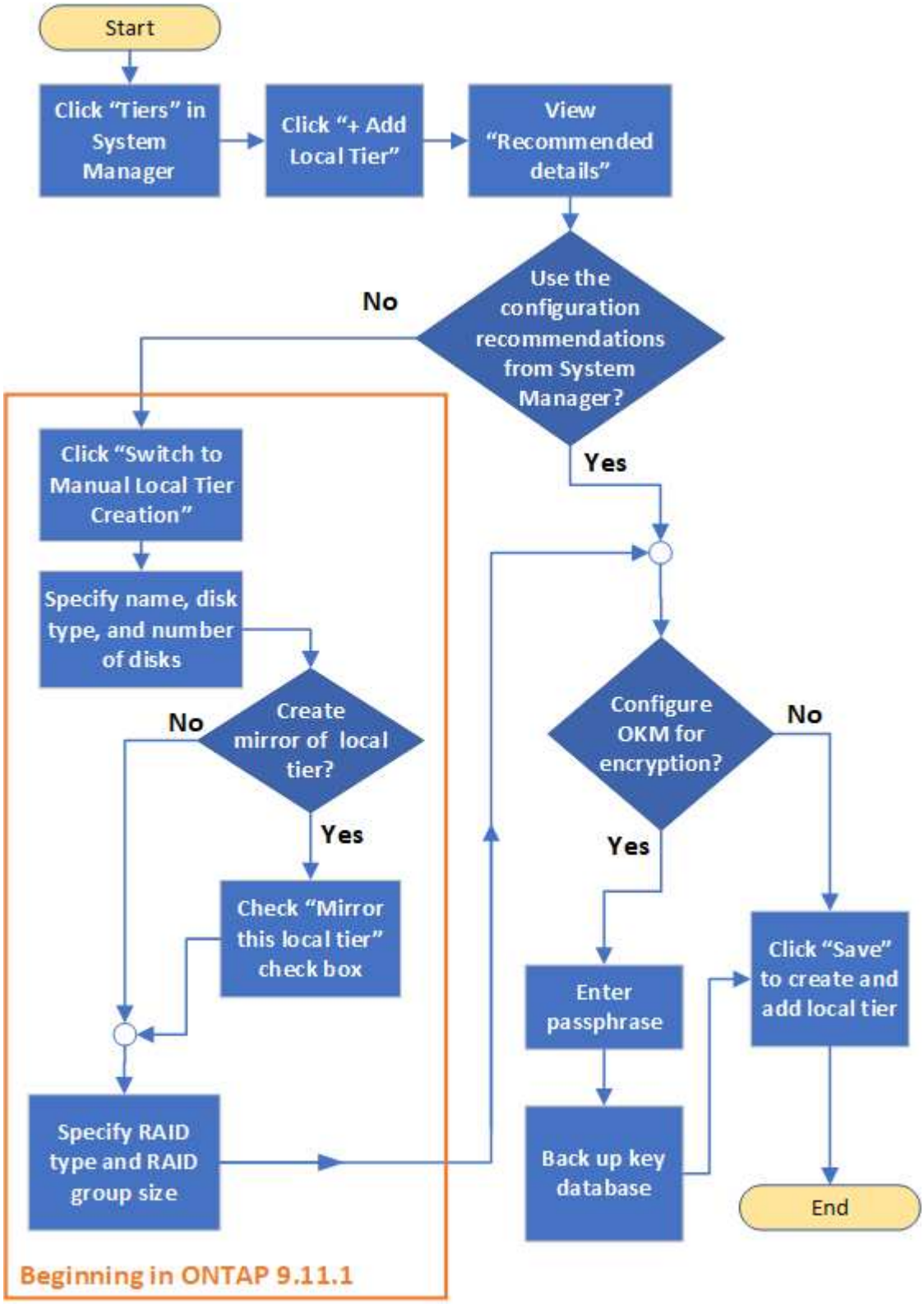
> ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

ローカル階層を作成するワークフローは、使用するインターフェイス（System ManagerまたはCLI）に固有です。

System Manager

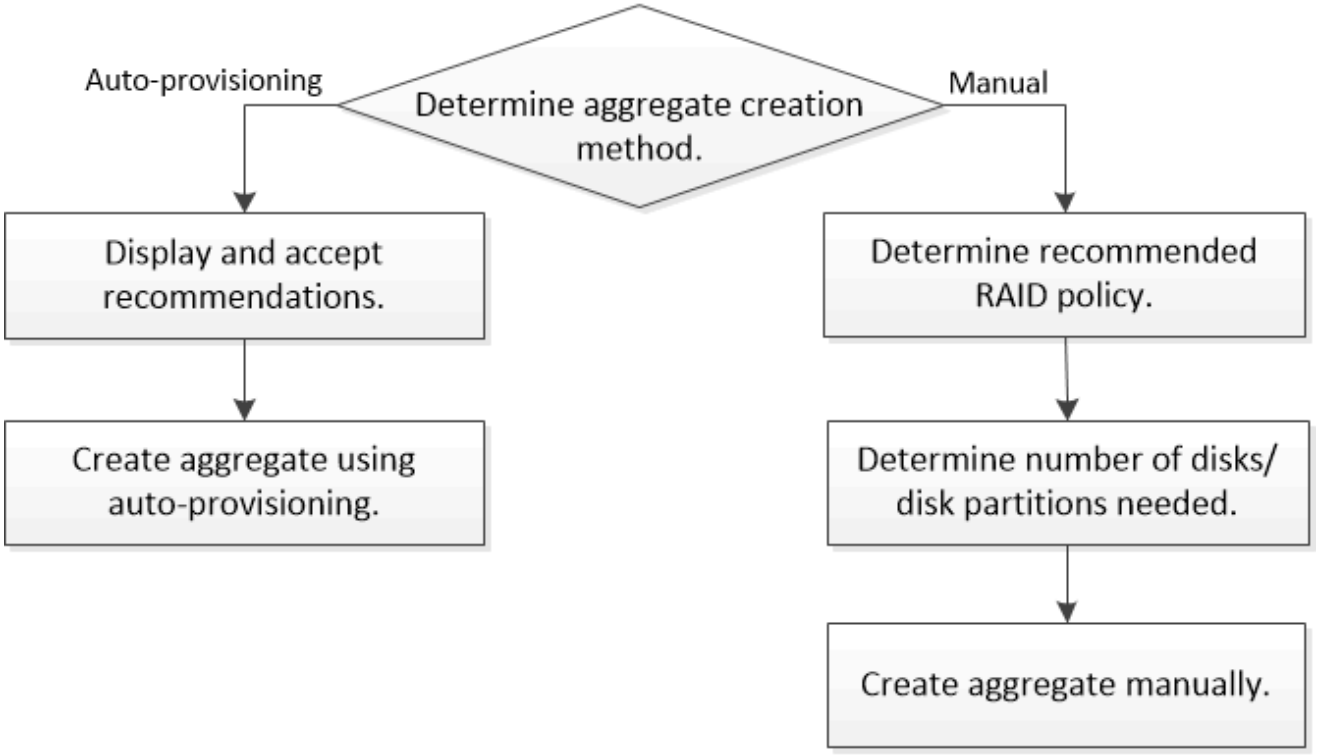
ローカル階層の設定に関する推奨されるベストプラクティスに基づいて、System Managerでローカル階層が作成されます。

ONTAP 9 .11.1以降では、自動プロセスで推奨される設定とは別の設定を使用してローカル階層を手動で追加することもできます。



CLI

ONTAP は、ローカル階層を作成するときに推奨構成を提供できます (自動プロビジョニング)。ベストプラクティスに基づく推奨構成が環境に適している場合は、それらの構成を受け入れてローカル階層を作成できます。それ以外の場合は、ローカル階層を手動で作成できます。



ONTAPローカル階層に必要なディスクまたはディスクパーティションの数を確認する

ローカル階層に、システム要件とビジネス要件を満たす十分な数のディスクまたはディスクパーティションが必要です。また、データ損失の可能性を最小限に抑えるために、推奨される数のホットスペアディスクまたはホットスペアディスクパーティションを用意しておく必要があります。

ルート/データパーティショニングは、特定の構成ではデフォルトで有効になります。ルートデータパーティショニングが有効になっているシステムでは、ディスクパーティションを使用してローカル階層を作成します。ルート / データパーティショニングが有効になっていないシステムでは、パーティショニングされていないディスクを使用します。

RAIDポリシーに必要な最小数と最小容量要件を満たすのに十分な数のディスクまたはディスクパーティションが必要です。

ONTAPでは、ドライブの使用可能スペースがドライブの物理容量よりも少なくなります。特定のドライブの使用可能スペースと、各RAIDポリシーに必要なディスクまたはディスクパーティションの最小数はで確認できます "Hardware Universe"。

特定のディスクの使用可能スペースを確認する

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

System Manager

- System Managerを使用して、ディスクの使用可能スペースを確認します。*

ディスクの使用可能なサイズを表示するには、次の手順を実行します。

手順

1. 「*ストレージ」>「階層」に移動します
2. ローカル階層の名前の横にあるをクリックします ⋮ 。
3. [ディスク情報]タブを選択します。

CLI

- CLIを使用して、ディスクの使用可能スペースを確認してください。*

ディスクの使用可能なサイズを表示するには、次の手順を実行します。

ステップ

1. スペアディスク情報を表示します。

```
storage aggregate show-spare-disks
```

RAIDグループを作成し、容量の要件を満たすために必要なディスクまたはディスクパーティションの数に加えて、ローカル階層に推奨されるホットスペアディスクまたはホットスペアディスクパーティションの最小数を確保しておく必要があります。

- オールフラッシュローカル階層には、少なくとも1つのホットスペアディスクまたはディスクパーティションが必要です。

> ⓘ AFF C190はデフォルトでスペアドライブなしに設定されています。この例外は完全にサポートされています。

- フラッシュ以外の同種のローカル階層には、少なくとも2つのホットスペアディスクまたはディスクパーティションが必要です。
- SSDストレージプールの場合は、HAペアごとに少なくとも1つのホットスペアディスクが必要です。
- Flash Poolローカル階層の場合は、HAペアごとに少なくとも2本のスペアディスクが必要です。Flash Poolローカル階層でサポートされるRAIDポリシーの詳細については、を参照して "Hardware Universe"ください。
- Maintenance Centerを使用できるようにし、同時に複数のディスク障害が発生した場合の問題を回避するには、マルチディスクキャリアに少なくとも4つのホットスペアを用意する必要があります。

関連情報

- "NetApp Hardware Universe"
- "NetAppテクニカルレポート3838：『ストレージサブシステム構成ガイド』"
- "storage aggregate show"

ONTAPにはローカル階層を自動的に追加するためのベストプラクティスが推奨されますが、推奨される構成が環境でサポートされるかどうかを確認する必要があります。サポートされていない場合は、使用するRAIDポリシーとディスク構成を決定し、ローカル階層を手動で作成する必要があります。

ローカル階層を自動で作成する場合、クラスタ内の使用可能なスペア ディスクがONTAPで分析され、それらのスペア ディスクを使用してローカル階層を追加する方法がベストプラクティスに基づく推奨事項として生成されます。ONTAPに表示される推奨構成を確認し、それらの推奨構成を受け入れるか、手動でローカル階層を追加できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

ONTAPの推奨事項を受け入れる前に

ディスクが次のいずれかの状態である場合は、ONTAPによる推奨事項を受け入れる前にそれらに対処する必要があります。

- ディスクが不足している
- スペア ディスクの数が安定しない
- ディスクが割り当てられていない
- スペアが初期化されていない
- ディスクがメンテナンス テスト中である

手動方式を使用する必要がある場合

多くの場合、環境に最適なローカル階層のレイアウトが推奨されます。ただし、ご使用の環境で次の設定が行われている場合は、手動でローカル階層を作成する必要があります。

ONTAP 9 .11.1以降では、System Managerを使用してローカル階層を手動で追加できます。

- サードパーティ製アレイLUNを使用するローカル階層
- Cloud Volumes ONTAPまたはONTAP Selectを使用した仮想ディスク
- MetroClusterシステム
- SyncMirror
- MSATAディスク
- Flash Pool階層
- 複数のタイプまたはサイズのディスクがノードに接続されている場合

ローカル階層を作成する方法を選択してください

使用する方法を選択します。

- "ローカル階層を自動的に追加（作成）する"
- "ローカル階層を手動で追加（作成）する"

関連情報

- "ONTAPコマンド リファレンス"
- "ストレージアグリゲートの自動プロビジョニング"

ONTAPローカル階層の自動追加

ONTAPで提供されるローカル階層の自動追加に関するベストプラクティスが環境に適している場合は、その推奨事項を承認してONTAPにローカル階層を追加させることができます。

> ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

ディスクをローカル階層で使用するには、ディスクがノードに所有されている必要があります。ディスク所有権の自動割り当てを使用するようにクラスタが設定されていない場合は、が必要です"所有権を手動で割り当てる"。

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

System Manager

手順

1. System Manager で、 * Storage > Tiers * をクリックします。
2. [階層]*ページで、をクリックし + Add Local Tier て新しいローカル階層を作成します。

   Add Local Tier *ページには、ノード上に作成できるローカル階層と使用可能なストレージが推奨数で表示されます。

3. 推奨構成の詳細を表示するには、* Recommended details *をクリックします。

   ONTAP 9 8以降では、次の情報が表示されます。

   - ローカル階層名（ONTAP 9.10.1で始まるローカル階層名を編集できます）
   - * ノード名 *
   - 使用可能なサイズ
   - ストレージの種類

     ONTAP 9 .10.1以降では、次の追加情報が表示されます。

   - ディスク：ディスクの数、サイズ、タイプが表示されます
   - レイアウト：RAIDグループのレイアウトを示します。ディスクがパリティかデータか、どのスロットが未使用かなどが含まれます。
   - スペアディスク：ノード名、スペアディスクの数とサイズ、ストレージの種類が表示されます。
4. 次のいずれかの手順を実行します。

実行する操作	操作
System Managerからの推奨事項を承認します。	に進みます暗号化用にオンボードキーマネージャを設定する手順。
ローカル階層を手動で設定し、System Managerの推奨事項を使用して「**_ not_**」を設定します。	次の"ローカル階層を手動で追加する"手順に進みます。 • ONTAP 9 .10.1以前の場合は、次の手順に従ってCLIを使用します。 • ONTAP 9 .11.1以降では、次の手順に従ってSystem Managerを使用します。

5. （オプション）：オンボードキーマネージャがインストールされている場合は、暗号化用に設定できます。Configure Onboard Key Manager for encryption *チェックボックスをオンにします。
   a. パスフレーズを入力します。
   b. 確認のためにもう一度パスフレーズを入力します。
   c. あとでシステムのリカバリが必要になったときのためにパスフレーズを保存します。

d. あとで使用できるようにキー データベースをバックアップします。

6. 保存*をクリックしてローカル階層を作成し、ストレージ解決策 に追加します。

CLI

コマンドを実行し `storage aggregate auto-provision`て、ローカル階層のレイアウトに関する推奨事項を生成します。ONTAPの推奨事項を確認して承認したあとに、ローカル階層を作成できます。

タスクの内容

コマンドで生成されるデフォルトの概要に、 `storage aggregate auto-provision`作成が推奨されるローカル階層のリスト（名前や使用可能なサイズなど）が表示されます。リストを表示し、プロンプトが表示されたら推奨されるローカル階層を作成するかどうかを確認できます。

オプションを使用すると、次のレポートを表示することもできます `-verbose`。

- 作成する新しいローカル階層のノードごとの概要、検出されたスペア、およびローカル階層の作成後の残りのスペアディスクとパーティション
- 作成する新しいデータローカル階層（使用するディスクとパーティションの数を含む）
- 作成する新しいデータローカル階層でのスペアディスクとパーティションの使用方法を示すRAIDグループのレイアウト
- ローカル階層の作成後の残りのスペアディスクとパーティションに関する詳細

自動プロビジョニング方法に精通していて、環境の準備が整っている場合は、オプションを使用すると、 `-skip-confirmation`表示と確認を行わずに推奨されるローカル階層を作成できます。 `storage aggregate auto-provision`コマンドは、CLIセッション設定の影響を受けません `-confirmations`。

の詳細については `storage aggregate auto-provision`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. 必要な表示オプションを指定してコマンドを実行し `storage aggregate auto-provision`ます。
   - オプションなし：標準の概要を表示します
   - `-verbose`オプション：詳細な概要を表示
   - `-skip-confirmation`オプション：表示や確認を行わずに推奨されるローカル階層を作成する
2. 次のいずれかの手順を実行します。

実行する操作	操作

ONTAP からの推奨事項を受け入れます。	推奨されるローカル階層の表示を確認し、プロンプトに応答して推奨されるローカル階層を作成します。
	
	`myA400-44556677::> storage aggregate auto-provision`
	`Node New Data Aggregate Usable Size`
	`---`
	`--- ---`
	`myA400-364 myA400_364_SSD_1 3.29TB`
	`myA400-363 myA400_363_SSD_1 1.46TB`
	`---`
	`--- ---`
	`Total: 2 new data aggregates 4.75TB`
	
	`Do you want to create recommended aggregates? {y`

n}: y Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress. myA400-44556677::> ----	ローカル階層を手動で設定し、ONTAP からの推奨事項を使用する*_ not_*。

関連情報

- "ONTAPコマンド リファレンス"

ONTAPローカル階層の手動追加

ONTAPの推奨ベストプラクティスに基づいてローカル階層を追加しない場合は、プロセスを手動で実行できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

ディスクをローカル階層で使用するには、ディスクがノードに所有されている必要があります。ディスク所有権の自動割り当てを使用するようにクラスタが設定されていない場合は、が必要です"所有権を手動で割り当てる"。

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

System Manager

ONTAP 9 .11.1以降では、System Managerで推奨される設定を使用してローカル階層を作成しない場合は、必要な設定を指定できます。

手順

1. System Manager で、 * Storage > Tiers * をクリックします。
2. [階層]*ページで、をクリックし + Add Local Tier て新しいローカル階層を作成します。

   Add Local Tier *ページには、ノード上に作成できるローカル階層と使用可能なストレージが推奨数で表示されます。

3. System Managerでローカル階層に対するストレージの推奨が表示されたら、「スペアディスク」セクションの「ローカル階層の手動作成に切り替え」をクリックします。

   [Add Local Tier]ページには、ローカル階層の設定に使用するフィールドが表示されます。

4. ローカル階層の追加*ページの最初のセクションで、次の手順を実行します。
   a. ローカル階層の名前を入力します。
   b. （オプション）：ローカル階層をミラーリングする場合は、[このローカル階層をミラーリングする*]チェックボックスをオンにします。
   c. ディスクタイプを選択します。
   d. ディスク数を選択します。
5. [**RAID Configuration**]セクションで、次の手順を実行します。
   a. RAIDタイプを選択します。
   b. Select the RAID group size.
   c. [RAID allocation]をクリックして、グループ内のディスクの割り当て状況を確認します。
6. （オプション）：オンボードキーマネージャがインストールされている場合は、ページの「* Encryption *」セクションで暗号化を設定できます。Configure Onboard Key Manager for encryption *チェックボックスをオンにします。
   a. パスフレーズを入力します。
   b. 確認のためにもう一度パスフレーズを入力します。
   c. あとでシステムのリカバリが必要になったときのためにパスフレーズを保存します。
   d. あとで使用できるようにキー データベースをバックアップします。
7. 保存*をクリックしてローカル階層を作成し、ストレージ解決策 に追加します。

CLI

ローカル階層を手動で作成する前に、ディスク構成オプションを確認し、作成をシミュレートする必要があります。

その後、コマンドを実行して結果を確認できます `storage aggregate create`。

開始する前に

ローカル階層で必要なディスク数とホットスペアディスクの数を決めておく必要があります。

タスクの内容

ルート/データ/データパーティショニングが有効になっていて、構成に含まれるソリッドステートドライブ（SSD）が24本以下の場合は、データパーティションを別 々 のノードに割り当てることを推奨します。

ルート/データパーティショニングとルート/データ/データパーティショニングが有効になっているシステムでローカル階層を作成する手順は、パーティショニングされていないディスクを使用するシステムでローカル階層を作成する手順と同じです。システムでルート/データパーティショニングが有効になっている場合は、ディスクパーティションの数をオプションに指定する必要があります `-diskcount`。ルート/データ/データパーティショニングの場合、オプションは `-diskcount`使用するディスクの数を指定します。

FlexGroupで使用する複数のローカル階層を作成する場合は、できるだけ近いサイズにする必要があります。

およびローカル階層の作成オプションと要件の詳細について `storage aggregate create`は、を"ONTAP コマンド リファレンス"参照してください。

手順

1. スペアディスクパーティションのリストを表示して、ローカル階層を作成するための十分な数のパーティションがあることを確認します。

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   データパーティションはに表示され `Local Data Usable`ます。ルートパーティションをスペアとして使用することはできません。

2. ローカル階層の作成をシミュレートします。

   ```
   storage aggregate create -aggregate aggregate_name -node node_name
   -raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
   ```

3. シミュレートしたコマンドから警告が表示された場合は、コマンドを調整してシミュレーションを繰り返します。
4. ローカル階層を作成します。

   ```
   storage aggregate create -aggregate aggr_name -node node_name -raidtype
   raid_dp -diskcount number_of_disks_or_partitions
   ```

5. ローカル階層を表示して、作成されたことを確認します。

   ```
   storage aggregate show-status aggregate_name
   ```

関連情報

- "storage aggregate show"

SyncMirrorを有効にして**ONTAP**ローカル階層を追加する

ローカル層を手動で作成して、ローカル層のデータを同期的にミラーリングするとき

に、 SyncMirrorを有効にできます。

詳細はこちら"ミラーリングされたローカル層とミラーリングされていないローカル層" 。

開始する前に

- クラスターは内部ストレージのみで初期化する必要があります。
- 両方のノードでクラスターのセットアップが完了している必要があります。

タスクの内容

この手順により、各クラスター ノードに同じサイズのミラー化されたデータ ローカル層が作成され、各ローカル層のディスク数は 44 になります。

手順

1. ストレージの自動割り当てを無効にする:

   ```
   storage disk option modify -node * -autoassign off
   ```

2. 自動割り当てが無効になっていることを確認します。

   ```
   storage disk option show
   ```

3. 外部棚を取り付けます。
4. プール 1 を指定して各ノードに外部ドライブを割り当てます。

   ```
   storage disk assign -disk <disk ID> -owner <node name> -pool 1
   ```

5. 各ノードのルート ローカル層をミラーリングします。

   ```
   storage aggregate mirror -aggregate <node1 root-aggr>

   storage aggregate mirror -aggregate <node2 root-aggr>
   ```

   プール 1 内のドライブは、プレックス 0 内のドライブと一致するように自動的にパーティション分割されます。

6. ノード 1 で、ディスク数 44 を使用してミラー化されたデータ ローカル層を作成します。これにより、プール 0 から 22 個のパーティションとプール 1 から 22 個のパーティションが選択されます。

   ```
   storage aggregate create -node <node1 name> -aggregate <node1 aggr-name>
   -diskcount 44 -mirror true
   ```

7. ノード 2 で、ディスク数 44 を使用してミラー化されたデータ ローカル層を作成します。これにより、プール 0 から 22 個のパーティションとプール 1 から 22 個のパーティションが選択されます。

   ```
   storage aggregate create -node <node2 name> -aggregate <node2 aggr-name>
   -diskcount 44 -mirror true
   ```

8. 同じサイズのローカル層が正常に作成されたことを確認します。

   ```
   storage aggregate show
   ```

関連情報

- "storage disk assign"
- "ストレージディスクオプションの変更"
- "ストレージディスクオプションの表示"

ローカル階層の使用の管理

ONTAPローカル階層の名前を変更します。

ローカル階層の名前は変更できます。実行する方法は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

System Manager

- System Managerを使用してローカル階層の名前を変更する*

ONTAP 9.10.1以降では、ローカル階層の名前を変更できます。

手順

1. System Manager で、 * Storage > Tiers * をクリックします。
2. ローカル階層の名前の横にあるをクリックします ⋮ 。
3. [名前の変更 *] を選択します。
4. ローカル階層の新しい名前を指定します。

CLI

- CLIを使用してローカル階層の名前を変更する*

ステップ

1. CLIを使用して、ローカル階層の名前を変更します。

   `storage aggregate rename -aggregate` *`aggr-name`* `-newname` *`aggr-new-name`*

   次の例では、「aggr5」という名前のアグリゲートの名前を「sales-aggr」に変更します。

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

関連情報

- "ストレージアグリゲートの名前変更"

ONTAPローカル階層のメディアコストの設定

ONTAP 9.11.1以降では、System Managerを使用してローカル階層のメディアコストを設定できます。

手順

1. System Managerで、**[**ストレージ**]>[**階層**]***をクリックし、必要なローカル階層のタイルで[メディアコストの設定]*をクリックします。
2. 「* active and inactive Tiers *」を選択して比較を有効にします。
3. 通貨タイプと金額を入力します。

メディアコストを入力または変更すると、すべてのメディアタイプで変更が行われます。

ONTAPドライブを手動で高速化

システムにONTAP 9.4以降を新規にインストールし、システムをONTAP 9.4以降で再初期化した場合、_fast zeroing_is used to zero drivs.

高速初期化では、ドライブが数秒で初期化されます。この処理はプロビジョニング前に自動的に実行されるため、スペアドライブを追加したときにシステムの初期化、ローカル階層の作成、またはローカル階層の拡張にかかる時間が大幅に短縮されます。

高速初期化_はSSDとHDDの両方でサポートされます。

> 高速初期化_は、ONTAP 9.3以前からアップグレードされたシステムではサポートされません。ONTAP 9 .4以降を新規にインストールするか、システムを再初期化する必要があります。ONTAP 9.3以前では、ONTAPによってドライブも自動的に初期化されますが、処理に時間がかかります。

ドライブを手動で初期化する必要がある場合は、次のいずれかの方法を使用できます。ONTAP 9.4以降では、ドライブの手動での初期化もわずか数秒で完了します。

CLIコマンド

ドライブを高速に初期化するには、**CLI**コマンドを使用します。

タスクの内容

このコマンドを使用するには管理者権限が必要です。

手順

1. CLIコマンドを入力します。

```
storage disk zerospares
```

ブート メニュー オプション

*ブートメニューから高速初期化ドライブ*のオプションを選択します

タスクの内容

- 高速初期化の拡張機能では、ONTAP 9より前のリリースからアップグレードされたシステムはサポートされません。4.

手順

1. ブートメニューから、次のいずれかのオプションを選択します。
    - （4）設定を消去してすべてのディスクを初期化
    - （9a）すべてのディスクのパーティショニングを解除し、ディスクの所有権情報を削除
    - （9b）設定を消去し、ディスク全体を含むノードを初期化

関連情報

- "storage disk zerospares"

ONTAPディスク所有権を手動で割り当てる

ディスクをローカル階層で使用するには、ディスクがノードに所有されている必要があります。

タスクの内容

- DS460Cシェルフだけのない初期化前のHAペアで所有権を手動で割り当てる場合は、オプション1を使用します。
- DS460CシェルフしかないHAペアを初期化する場合は、オプション2を使用してルートドライブの所有権を手動で割り当てます。

オプション**1**：ほとんどの**HA**ペア

DS460Cシェルフだけのないペアで初期化を実行していない場合は、次の手順に従って手動で所有権を割り当てます。

タスクの内容

- 所有権を割り当てるディスクは、所有権を割り当てるノードに物理的にケーブル接続されたシェルフに含まれている必要があります。
- ローカル階層（アグリゲート）内のディスクを使用する場合：
  - ディスクをローカル階層（アグリゲート）で使用するには、そのディスクがノードに所有されていなければなりません。
  - ローカル階層（アグリゲート）で使用中のディスクの所有権を再割り当てすることはできません。

手順

1. CLIを使用して、所有権が未設定のディスクをすべて表示します。

   ```
   storage disk show -container-type unassigned
   ```

2. それぞれのディスクを割り当てます。

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。すでに別のノードで所有されているスペアディスクを再割り当てする場合は、「-force」オプションを使用する必要があります。

初期化するHAペアで、DS460Cシェルフしかない場合は、次の手順に従ってルートドライブの所有権を手動で割り当てます。

タスクの内容

- DS460Cシェルフのみを含むHAペアを初期化する場合は、ハーフドロワーのポリシーに準拠するようにルートドライブを手動で割り当てる必要があります。

  HAペアの初期化（ブートアップ）後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して残りのドライブ（ルートドライブ以外）と今後追加されるドライブ（障害ディスクの交換、「low spares」メッセージへの応答、容量の追加など）に所有権が割り当てられます。

  "ハーフドロワーポリシーの詳細"です。

- DS460Cシェルフに8TBを超えるNL-SASドライブを搭載する場合、RAIDにはHAペアごとに最低10本のドライブ（各ノードに5本）が必要です。

手順

1. DS460Cシェルフがフル装備されていない場合は、次の手順を実行します。フル装備されていない場合は、次の手順に進みます。

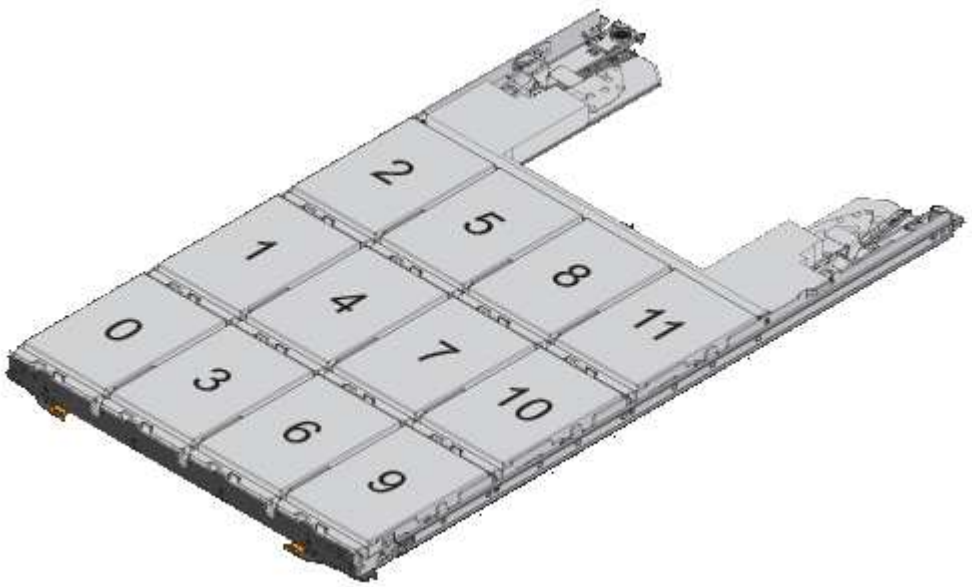
   a. まず、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。

      各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

   b. 残りのドライブについては、各ドロワーに均等に配置します。

      ドロワーの列への取り付けを前面から背面へ進めます。列がドライブで埋まりきらない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

      次の図は、DS460Cドロワー内のドライブ ベイの番号と場所を表しています。



2. ノード管理LIFまたはクラスタ管理LIFを使用してクラスタシェルにログインします。
3. 次の手順を使用して、ハーフドロワーポリシーに準拠するように各ドロワーのルートドライブを手動で割り当てます。

   ハーフドロワーポリシーでは、ドロワーのドライブの左半分（ベイ0$_{5}$）をノードAに、右半分（ベイ6$_{11}$）をノードBに割り当てます。

   a. 所有権が未設定のディスクをすべて表示します。
      `storage disk show -container-type unassigned`
   b. ルートディスクを割り当てます。
      `storage disk assign -disk disk_name -owner owner_name`

      ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。

の詳細については `storage disk`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "storage disk assign"
- "storage disk show"

ONTAPローカル階層のドライブと**RAID**グループの情報を確認する

一部のローカル階層の管理作業では、ローカル階層を構成するドライブのタイプ、サイズ、チェックサム、およびステータス、他のローカル階層と共有するかどうか、およびRAIDグループのサイズと構成を把握しておく必要があります。

ステップ

1. ローカル階層のドライブをRAIDグループ別に表示します。

   `storage aggregate show-status` *`aggr_name`*

   ローカル階層内の各RAIDグループのドライブが表示されます。

   ドライブ（データ、パリティ、ダブルパリティ）のRAIDタイプは列で確認できます `Position`。列にと表示されている `shared`場合 `Position`、ドライブは共有されます。HDDの場合はパーティショニングされたディスクです。SSDの場合はストレージプールの一部です。

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

関連情報

- "ストレージアグリゲートのステータス表示"

Storage VM（SVM）へのONTAPローカル階層の割り当て

Storage Virtual Machine（Storage VMまたはSVM、旧Vserver）に1つ以上のローカル階層を割り当てた場合、そのStorage VM（SVM）のボリュームはそれらのローカル階層にのみ含めることができます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

Storage VMとそのStorage VMに割り当てるローカル階層を用意しておく必要があります。

タスクの内容

Storage VMにローカル階層を割り当てると、Storage VM同士の分離に役立ちます。これはマルチテナンシー環境で特に重要になります。

手順

1. SVMにすでに割り当てられているローカル階層のリストを確認します。

   ```
   vserver show -fields aggr-list
   ```

   SVMに現在割り当てられているローカル階層が表示されます。ローカル階層が割り当てられていない場合は –、が表示されます。

2. 要件に応じて、割り当てられているローカル階層を追加または削除します。

状況	使用するコマンド
追加のローカル階層を割り当てる	`vserver add-aggregates`
ローカル階層の割り当て解除	`vserver remove-aggregates`

   表示されているローカル階層がSVMに割り当てられているか、SVMから削除されています。SVMに割り当てられていないアグリゲートを使用するボリュームがすでにSVMにある場合は、警告メッセージが表示されますが、コマンドは正常に完了します。SVMにすでに割り当てられているローカル階層とコマンドで指定していないローカル階層には影響はありません。

例

次の例では、ローカル階層aggr1とaggr2がSVM svm1に割り当てられます。

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

ONTAPローカル階層に配置するボリュームを確認する

ローカル階層で処理（ローカル階層の再配置やオフライン化など）を実行する前に、ローカル階層に配置されているボリュームを確認しなければならない場合があります。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

手順

1. ローカル階層にあるボリュームを表示するには、次のように入力します。

   ```
   volume show -aggregate aggregate_name
   ```

   指定したローカル階層にあるすべてのボリュームが表示されます。

ローカル階層のスペースを最も使用しているFlexVolボリューム、特にボリューム内のどの機能が最も使用しているかを確認できます。

コマンドは、 `volume show-footprint`ボリュームの占有量（ボリュームを含むローカル階層内でのスペース使用量）に関する情報を表示します。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

`volume show-footprint`コマンドは、ローカル階層内の各ボリューム（オフラインボリュームを含む）のスペース使用量の詳細を表示します。このコマンドは、コマンドと `aggregate show-space`コマンドの出力のギャップを埋めます `volume show-space`。割合はすべて、ローカル階層のサイズに対する割合として計算されます。

testvolという名前のボリュームに対するコマンドの出力例を次に示します `volume show-footprint`。

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                                     Used    Used%
      --------------------------------    ----------    -----
      Volume Data Footprint                    120.6MB       4%
      Volume Guarantee                          1.88GB      71%
      Flexible Volume Metadata                 11.38MB       0%
      Delayed Frees                             1.36MB       0%
      Total Footprint                           2.01GB      76%
```

次の表に、コマンドの出力の主な行と、その機能によるスペース使用量を削減する方法を示し `volume show-footprint`ます。

行 / 機能名	説明 / 行の内容	削減方法もあります
`Volume Data Footprint`	アクティブファイルシステムでボリュームのデータに使用されている包含ローカル階層のスペースとボリュームのSnapshotで使用されているスペースの合計。この行にはリザーブスペースは含まれません。	• ボリュームからデータを削除します。 • ボリュームからSnapshotを削除しています。

`Volume Guarantee`	ボリュームによって今後の書き込み用にリザーブされているローカル階層のスペースの量。リザーブされるスペースの量は、ボリュームのギャランティタイプによって異なります。	ボリュームのギャランティタイプをに変更しています `none`。
`Flexible Volume Metadata`	ボリュームのメタデータファイルに使用されているローカル階層のスペースの総容量。	直接制御する方法はありません。
`Delayed Frees`	ONTAPがパフォーマンスのために使用していた、すぐには解放できないブロック。SnapMirrorデスティネーションの場合、この行の値はに `0`なり、表示されません。	直接制御する方法はありません。
`File Operation Metadata`	ファイル処理メタデータ用にリザーブされているスペースの総容量。	直接制御する方法はありません。
`Total Footprint`	ボリュームがローカル階層で使用するスペースの総容量。すべての行の合計です。	ボリュームの使用スペースを削減するために使用されるいずれかの方法。

関連情報

"NetAppテクニカルレポート3483：『NetApp SANまたはIP SAN構成のエンタープライズ環境におけるシンプロビジョニング』"

ONTAPローカル階層のスペース使用量を確認する

1つ以上のローカル階層内のすべてのボリュームによるスペース使用量を表示して、空きスペースを増やすための対処を行うことができます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

WAFLは、合計ディスクスペースの割合をローカル階層レベルのメタデータとパフォーマンス用にリザーブします。ローカル階層でボリュームの保持に使用されているスペースはWAFLリザーブから解放され、変更することはできません。

30TB未満のローカル階層では、WAFLによって合計ディスクスペースの10%がローカル階層レベルのメタデータとパフォーマンス用にリザーブされます。

ONTAP 9.12.1以降では、30TB以上のローカル階層では、ローカル階層レベルのメタデータとパフォーマンス用にリザーブされるディスクスペースが削減され、ローカル階層の使用可能スペースが5%増加します。このスペース削減効果は、プラットフォームとONTAPのバージョンによって異なります。

ONTAPによってローカル階層に**30TB**以上リザーブされているディスクスペース	プラットフォームに適用	**ONTAP**ノハアシヨン
5%	All AFFおよびFASプラットフォーム	ONTAP 9.14.1以降
5%	AFFプラットフォームとFAS500fプラットフォーム	ONTAP 9.12.1以降
10%	すべてのプラットフォーム	ONTAP 9.11.1以降

コマンドを使用して、1つ以上のローカル階層内のすべてのボリュームによるスペース使用量を確認できます `aggregate show-space`。この情報から、格納されているローカル階層のスペースを最も消費しているボリュームを確認して、空きスペースを増やすための対処を行うことができます。

ローカル階層の使用済みスペースは、ローカル階層に含まれるFlexVolで使用されるスペースに直接影響されます。ボリュームのスペースを増やすための対処方法も、ローカル階層のスペースに影響します。

ONTAP 9.15.1以降では、2つの新しいメタデータカウンタを使用できます。いくつかの既存のカウンタへの変更とともに、割り当てられたユーザデータの量をより明確に表示できます。詳細については、を参照してください "ボリュームまたはローカル階層のスペース使用量を確認する" 。

コマンド出力に表示される行は次のとおり `aggregate show-space`です。

- ボリュームフットプリント

  ローカル階層内のすべてのボリュームフットプリントの合計。これには、格納先ローカル階層内のすべてのボリュームのすべてのデータおよびメタデータによって使用またはリザーブされているすべてのスペースが含まれます。

- 集計メタデータ

  ローカル階層で必要なファイルシステムメタデータ（割り当てビットマップやinodeファイルなど）の合計。

- * Snapshot リザーブ *

  ローカル階層のSnapshot用にリザーブされているスペースの量（ボリュームサイズに基づいて決まります）。このスペースは使用済みとみなされ、ボリュームまたはローカル階層のデータやメタデータには使用できません。

- * Snapshotリザーブを使用できません*

  ローカル階層のSnapshotリザーブ用に当初割り当てられていたスペースです。ローカル階層に関連付けられているボリュームで使用されているため、ローカル階層のSnapshotには使用できません。ローカル階層のSnapshotリザーブがゼロでないローカル階層に対してのみ実行できます。

- 合計使用量

  ボリューム、メタデータ、またはSnapshotによってローカル階層で使用またはリザーブされているすべてのスペースの合計。

- 合計使用物理容量

  将来使用するためにリザーブされているのではなく、現在データに使用されているスペースの量。ローカル階層のSnapshotで使用されているスペースが含まれます。

次の例は、Snapshotリザーブが5%のローカル階層に対するコマンドの出力を示して `aggregate show-space` います。スナップショット予約が0の場合、行は表示されません。

```
cluster1::> storage aggregate show-space

                        Aggregate : wqa_gx106_aggr1

      Feature                                   Used      Used%
      --------------------------------    ----------     ------
      Volume Footprints                      101.0MB         0%
      Aggregate Metadata                       300KB         0%
      Snapshot Reserve                        5.98GB         5%

      Total Used                              6.07GB         5%
      Total Physical Used                    34.82KB         0%
```

関連情報

- "ナレッジベースの記事：スペース使用量"
- "ONTAP 9にアップグレードすることで、ストレージ容量の5%を解放できます。12.1"
- "ストレージアグリゲートショースペース"

HAペア内の**ONTAP**ローカル階層の所有権を切り替えます。

ローカル階層からのサービスを中断することなく、HAペアのノード間でローカル階層の所有権を変更できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

HAペアの両方のノードのディスクまたはアレイLUNが相互に物理的に接続されています。各ディスクまたはアレイLUNはどちらか一方のノードで所有されます。

テイクオーバーの発生時には、ローカル階層内のすべてのディスクまたはアレイLUNの所有権が一時的に一方のノードからもう一方のノードに切り替わります。ただし、ローカル階層の再配置処理によって所有権が永続的に変更されることもあります（負荷分散の場合など）。所有権が変更されても、データコピープロセスやディスクまたはアレイLUNの物理的な移動は行われません。

タスクの内容

- ローカル階層の再配置処理では、ボリューム数の制限がプログラムで検証されるため、手動でチェックする必要はありません。

ボリューム数がサポートされる上限を超えると、ローカル階層の再配置処理が失敗し、関連するエラーメッセージが表示されます。

- ソースノードまたはデスティネーションノードでシステムレベルの処理を実行中のときは、ローカル階層の再配置を開始しないでください。同様に、ローカル階層の再配置の実行中にそれらの処理を開始しないでください。

  これらの処理には、次のようなものがあります。

  - テイクオーバー
  - ギブバック
  - シャットダウン
  - 別のローカル階層の再配置処理です
  - ディスク所有権の変更
  - ローカル階層またはボリューム構成の処理
  - ストレージコントローラの交換
  - ONTAP のアップグレード
  - ONTAPのリバート
- MetroCluster 構成を使用する場合は、ディザスタリカバリ処理（*switchover*、*healing*、または_switchback _）の実行中にローカル階層の再配置を開始しないでください。
- MetroCluster構成を使用している場合に、スイッチオーバーされたローカル階層でローカル階層の再配置を開始すると、DRパートナーのボリューム数の上限を超えて処理が失敗することがあります。
- 破損しているかメンテナンス中のローカル階層では、ローカル階層の再配置を開始しないでください。
- ローカル階層の再配置を開始する前に、ソースノードとデスティネーションノードにコアダンプを保存する必要があります。

手順

1. ノードのローカル階層を表示して移動するローカル階層を確認し、オンラインで良好な状態にあることを確認します。

   `storage aggregate show -node source-node`

   次のコマンドは、クラスタ内の4つのノード上の6つのローカル階層を表示します。すべてのローカル階層がオンラインです。ノード1とノード3がHAペアを形成し、ノード2とノード4がHAペアを形成しています。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. コマンドを実行してローカル階層の再配置を開始します。

   `storage aggregate relocation start -aggregate-list` *aggregate-1*, *aggregate-2*… `-node` *source-node* `-destination` *destination-node*

   ローカル階層aggr_1およびaggr_2をノード1からノード3に移動するコマンドの例を次に示します。ノード3はノード1のHAパートナーです。ローカル階層はHAペア内でのみ移動できます。

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. コマンドを使用して、ローカル階層の再配置の進捗を監視し `storage aggregate relocation show`ます。

   `storage aggregate relocation show -node` *source-node*

   次のコマンドは、ノード3に移動中のローカル階層の進捗状況を表示します。

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

再配置が完了すると、このコマンドの出力には、各ローカル階層の再配置ステータスが「`done'」と表示されます。

関連情報

- "storage aggregate relocation show"
- "storage aggregate relocation start"
- "storage aggregate show"

ONTAPローカル階層を削除します。

ローカル階層にボリュームがない場合は、ローカル階層を削除できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

`storage aggregate delete`コマンドは、ストレージローカル階層を削除します。ローカル階層にボリュームがある場合、コマンドは失敗します。ローカル階層にオブジェクトストアが接続されている場合は、ローカルが削除されるだけでなく、オブジェクトストア内のオブジェクトも削除されます。このコマンドでオブジェクトストア設定が変更されることはありません。

次の例は、「aggr1」という名前のローカル階層を削除します。

```
> storage aggregate delete -aggregate aggr1
```

関連情報

- "ストレージ集約の削除"

ローカル階層の再配置用の**ONTAP**コマンド

ONTAPには、HAペアでローカル階層の所有権を切り替えるための固有のコマンドが用意されています。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

状況	使用するコマンド
ローカル階層の再配置プロセスを開始します	`storage aggregate relocation start`
ローカル階層の再配置プロセスを監視	`storage aggregate relocation show`

関連情報

- "storage aggregate relocation show"
- "storage aggregate relocation start"

ローカル階層の管理用**ONTAP**コマンド

ローカル階層を管理するには、コマンドを使用し `storage aggregate`ます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

状況	使用するコマンド
すべてのFlash Poolローカル階層のキャッシュサイズを表示する	`storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total >0`
ローカル階層のディスクの情報とステータスを表示する	`storage aggregate show-status`
ノード別のスペア ディスクを表示する	`storage aggregate show-spare-disks`
クラスタ内のルートローカル階層を表示します。	`storage aggregate show -has-mroot true`
ローカル階層の基本情報とステータスを表示する	`storage aggregate show`
ローカル階層で使用されているストレージのタイプを表示します。	`storage aggregate show -fields storage-type`
ローカル階層をオンラインにする	`storage aggregate online`
ローカル階層を削除します。	`storage aggregate delete`

状況	使用するコマンド
ローカル階層を制限状態にします。	`storage aggregate restrict`
ローカル階層の名前を変更します。	`storage aggregate rename`
ローカル階層をオフラインにする	`storage aggregate offline`
ローカル階層のRAIDタイプを変更する	`storage aggregate modify -raidtype`

関連情報

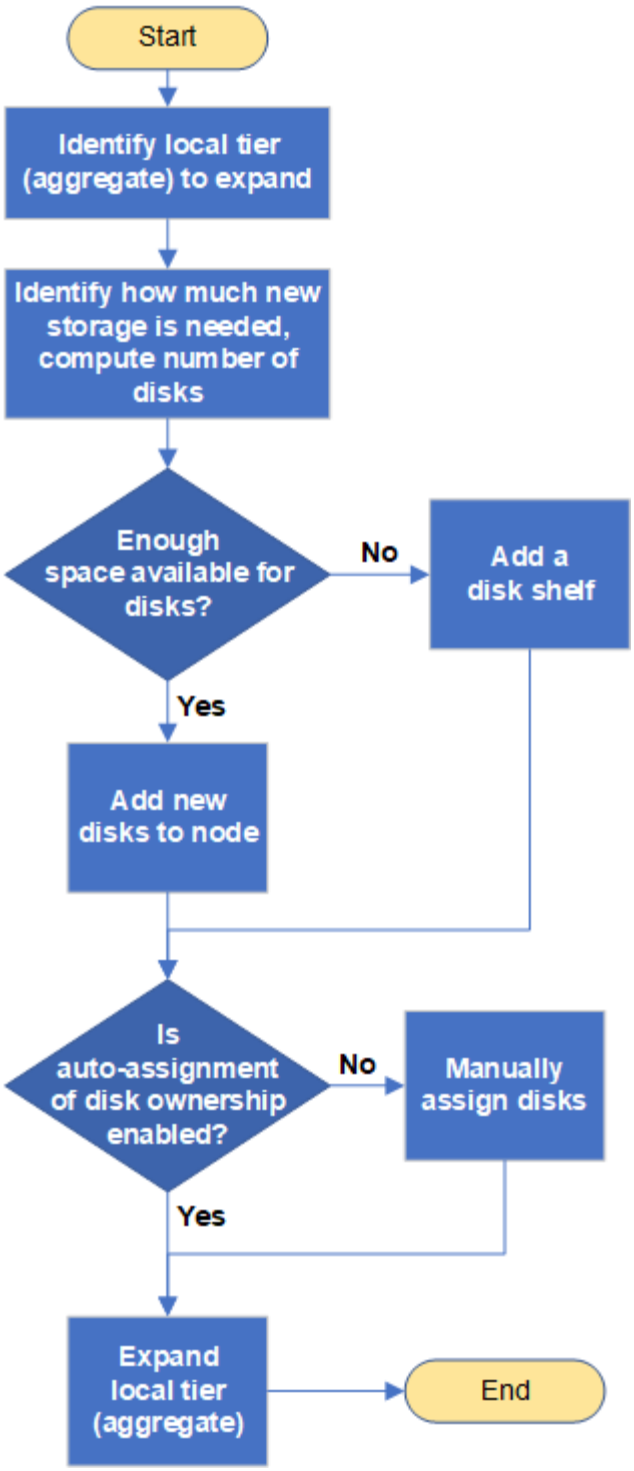
- "ストレージ集約の削除"
- "storage aggregate modify"
- "ストレージアグリゲートがオフライン"
- "ストレージアグリゲートオンライン"
- "ストレージアグリゲートの名前変更"
- "ストレージ集約制限"
- "storage aggregate show"

ローカル階層へのデータ（ディスク）の追加

ONTAPローカル階層に容量を追加するワークフロー

ローカル階層に容量を追加するには、まずどのローカル階層に追加するかを特定し、必要な新しいストレージ容量を決定し、新しいディスクを取り付けてディスク所有権を割り当て、必要に応じて新しいRAIDグループを作成する必要があります。

容量は、System ManagerまたはONTAP CLIを使用して追加できます。



ONTAPローカル階層内のスペースの作成方法

ローカル階層の空きスペースが不足すると、データの損失からボリュームギャランティの無効化まで、さまざまな問題が発生する可能性があります。ローカル階層のスペースを増やす方法は複数あります。

どの方法にもさまざまな影響があります。アクションを実行する前に、ドキュメントの該当するセクションをお読みください。

ローカル階層のスペースを確保するための一般的ないくつかの方法について、影響が小さいものから順に次に

示します。

- ローカル階層にディスクを追加します。
- 使用可能なスペースがある別のローカル階層に一部のボリュームを移動してください。
- ローカル階層内のボリュームギャランティが設定されたボリュームのサイズを縮小します。
- ボリュームのギャランティタイプが「none」の場合は、不要なボリュームSnapshotを削除します。
- 不要なボリュームを削除する。
- 重複排除や圧縮などのスペース削減機能を有効にします。
- 大量のメタデータを使用している機能を（一時的に）無効にする。

ONTAPローカル階層への容量の追加

ローカル階層にディスクを追加して、関連付けられているボリュームに提供できるストレージを増やすことができます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

System Manager（ONTAP 9.8以降）

ONTAP 9.12.1以降では、System Managerを使用してローカル階層のコミット済み容量を表示し、ローカル階層に追加の容量が必要かどうかを判断できます。を参照して "System Managerで容量を監視する"

手順

1. [ストレージ]>[階層]*を選択します。
2. 容量を追加するローカル階層の名前の横にあるを選択します。
3. [容量の追加]*を選択します。

追加できるスペアディスクがない場合、 * 容量の追加 * オプションは表示されず、ローカル階層の容量を増やすことはできません。

4. インストールされているONTAPのバージョンに応じて、次の手順を実行します。

インストールされているONTAP のバージョン	実行する手順
ONTAP 9.11.1以降	a. ディスクのタイプと数を選択します。 b. 新しいRAIDグループにディスクを追加する場合は、チェックボックスをオンにします。RAID割り当てが表示されます。 c. [保存（ Save ）] を選択します。
ONTAP 9.10.1、9.9、または9.8	a. ノードに複数のストレージ階層が含まれている場合は、ローカル階層に追加するディスクの数を選択します。それ以外の場合は、ノードに含まれるストレージ階層が1つだけの場合、追加される容量が自動的に推定されます。 b. 「 * 追加」を選択します。

5. （オプション）プロセスが完了するまでに時間がかかります。バックグラウンドでプロセスを実行する場合は、 [バックグラウンドで実行（ Run in Background ）] を選択します。
6. 処理が完了したら、ローカル階層の情報で容量の増加を確認できます。詳細については、「 * Storage 」 > 「 Tiers * 」を参照してください。

System Manager（ONTAP 9.7以前）

手順

1. （ONTAP 9.7のみ）*（クラシックバージョンに戻る）*を選択します。
2. [ハードウェアおよび診断]>[アグリゲート]*を選択します。
3. データディスクを追加するローカル階層を選択し、*[操作]>[容量の追加]*を選択します。

ローカル階層内の他のディスクと同じサイズのディスクを追加する必要があります。

4. （ONTAP 9.7のみ）*[新しいエクスペリエンスに切り替える]*を選択します。

5. [ストレージ]>[階層]*を選択して、新しいローカル階層のサイズを確認します。

CLI

開始する前に

ストレージの追加先のローカル階層のRAIDグループサイズを確認しておく必要があります。

タスクの内容

パーティショニングされたディスクをローカル階層に追加する手順は、パーティショニングされていないディスクを追加する手順と似ています。

ローカル階層を拡張する場合は、パーティションとパーティショニングされていないディスクのどちらをローカル階層に追加するかを確認しておく必要があります。パーティショニングされていないドライブを既存のローカル階層に追加すると、既存のRAIDグループのサイズが新しいRAIDグループに継承され、必要なパリティディスクの数に影響する可能性があります。パーティショニングされたディスクで構成されるRAIDグループにパーティショニングされていないディスクを追加すると、新しいディスクがパーティショニングされ、未使用のスペアパーティションが残ります。

パーティションをプロビジョニングするときは、両方のパーティションを含むスペアドライブがノードに存在しないようにする必要があります。この状況でノードのコントローラが停止すると、問題に関する有用な情報（コアファイル）をテクニカルサポートに提供できなくなる可能性があります。

手順

1. ローカル階層を所有するシステムで使用可能なスペアストレージを表示します。

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   パラメータを使用すると、パーティショニングされたドライブのみ、またはパーティショニングされていないドライブのみを表示できます `-is-disk-shared`。

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                      BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. ローカル階層の現在のRAIDグループを表示します。

```
storage aggregate show-status <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. アグリゲートへのストレージの追加をシミュレートします。

```
storage aggregate add-disks -aggregate <aggr_name> -diskcount
<number_of_disks_or_partitions> -simulate true
```

実際にストレージをプロビジョニングしなくてもストレージの追加結果を確認できます。シミュレートしたコマンドから警告が表示された場合は、コマンドを調整してシミュレーションを繰り返すことができます。

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                        Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. アグリゲートにストレージを追加します。

```
storage aggregate add-disks -aggregate <aggr_name> -raidgroup new
-diskcount <number_of_disks_or_partitions>
```

Flash Poolローカル階層の作成時に、チェックサムがローカル階層と異なるディスクを追加する場合や、チェックサムが混在するローカル階層にディスクを追加する場合は、パラメータを使用する必要があります `-checksumstyle`。

Flash Poolローカル階層にディスクを追加する場合は、パラメータを使用してディスクタイプを指定する必要があります `-disktype`。

パラメータを使用して、追加するディスクのサイズを指定でき `-disksize`ます。指定したサイズに近いディスクのみがローカル階層への追加対象として選択されます。

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. ストレージが正常に追加されたことを確認します。

```
storage aggregate show-status -aggregate <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                                    Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                        0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. ルートパーティションとデータパーティションの両方を含む少なくとも1本のスペアドライブがノードに残っていることを確認します。

```
storage aggregate show-spare-disks -original-owner <node_name>
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                Local
Local
                                                                 Data
Root Physical
 Disk                        Type      RPM Checksum          Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                      BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

関連情報

- "storage aggregate add-disks"
- "ストレージアグリゲートのスペアディスク表示"
- "ストレージアグリゲートのステータス表示"

ONTAPノードまたはシェルフにドライブを追加する

ホットスペアの数を増やしたり、ローカル階層にスペースを追加したりするには、ノードまたはシェルフにドライブを追加します。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

追加するドライブがプラットフォームでサポートされている必要があります。を使用して確認できます"NetApp Hardware Universe"。

1回の手順で少なくとも6本のドライブを追加する必要があります。ドライブを1本追加するとパフォーマンスが低下する可能性があります。

NetApp Hardware Universeの手順

1. [* **Products**]ドロップダウンメニューで、ハードウェア構成を選択します。
2. プラットフォームを選択します。
3. 実行しているONTAPのバージョンを選択し、**Show Results**を選択します。
4. 図の下で、[*別のビューを表示するにはここをクリック]を選択します。設定に一致するビューを選択します。

の画像"]

ドライブの取り付け手順

1. で、新しいドライブファームウェア、シェルフファームウェア、Disk Qualification Packageファイルを確認します"NetAppサポートサイト"。

   ノードまたはシェルフに最新バージョンがインストールされていない場合は、新しいドライブを取り付ける前に更新してください。

   新しいドライブのファームウェアが最新バージョンでない場合は、自動的に更新されます（システムは停止されません）。

2. 自分自身を適切にアースします。
3. プラットフォームの前面からベゼルをそっと取り外します。
4. 新しいドライブ用のスロットを特定します。

   ドライブを追加するスロットは、プラットフォームのモデルとONTAPのバージョンによって異なります。場合によっては、特定のスロットに順番にドライブを追加する必要があります。たとえば、AFF A800では、特定の間隔で空きスロットを残してドライブを追加します。一方、AFF A220では、シェルフの外側から順番に空きスロットに新しいドライブを追加していきます。

   の構成に適したスロットを特定するには、「**Before You Begin** 」の手順を参照して"NetApp Hardware Universe"ください。

5. 新しいドライブを挿入します。
   a. カムハンドルが開いた状態で、両手で新しいドライブを挿入します。
   b. ドライブが止まるまで押します。
   c. ドライブがミッドプレーンに完全に収まり、カチッという音がして固定されるまで、カムハンドルを閉じます。カムハンドルは、ドライブの前面に揃うようにゆっくりと閉じてください。
6. ドライブのアクティビティLED（緑）が点灯していることを確認します。

   ドライブのアクティビティLEDが点灯している場合は、ドライブに電力が供給されています。ドライブのアクティビティLEDが点滅しているときは、ドライブに電力が供給されていて、I/Oが実行中です。ドライ

ブファームウェアが自動的に更新されている場合は、LEDが点滅します。

7. 別のドライブを追加するには、手順4~6を繰り返します。

   ノードに割り当てるまで新しいドライブは認識されません。新しいドライブを手動で割り当てることができます。また、ドライブの自動割り当てルールを適用しているノードの場合は、ONTAPによって新しいドライブが自動的に割り当てられるまで待つこともできます。

8. 新しいドライブがすべて認識されたら、ドライブが追加され、所有権が正しく指定されていることを確認します。

インストールの確認手順

1. ディスクのリストを表示します。

   ```
   storage aggregate show-spare-disks
   ```

   新しいドライブが正しいノードに所有されていることを確認してください。

2. 必要に応じて（**ONTAP 9.3**以前の場合のみ）新しく追加したドライブを初期化します。

   ```
   storage disk zerospares
   ```

   別のローカル階層に追加する前に、ONTAPローカル階層で使用されていたドライブを初期化する必要があります。ONTAP 9.3以前では、ノード内の初期化されていないドライブのサイズによっては、初期化が完了するまでに数時間かかることがあります。この時点でドライブを初期化しておくと、ローカル階層のサイズをすぐに拡張する必要がある場合に時間を短縮できます。これはONTAP 9.4以降の問題 ではありません。ドライブは高速初期化を使用して初期化されますが、これには数秒しかかかりません。

結果

新しいドライブの準備が完了しました。ローカル階層に追加したり、ホットスペアのリストに追加したり、新しいローカル階層の作成時に追加したりできます。

関連情報

- "ストレージアグリゲートのスペアディスク表示"
- "storage disk zerospares"

ミスアライメント状態の**ONTAP**スペアパーティションを修正する

パーティショニングされたディスクをローカル階層に追加する場合は、すべてのノードで使用可能なルートパーティションとデータパーティションの両方を含むディスクをスペアとして残しておく必要があります。スペアディスクがない状態でノードが停止すると、ONTAPはスペアデータパーティションにコアをダンプできません。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

同じノードが所有する同じタイプのディスク上に、スペアデータパーティションとスペアルートパーティショ

ンの両方が必要です。

手順

1. CLIを使用して、ノードのスペアパーティションを表示します。

   `storage aggregate show-spare-disks -original-owner node_name`

   どのディスクにスペアデータパーティション（spare_data）があり、どのディスクにスペアルートパーティション（spare_root）があるかを確認します。スペアパーティションの列または `Local Root Usable`列にゼロ以外の値が表示されます `Local Data Usable`。

2. スペアデータパーティションを含むディスクを、スペアルートパーティションを含むディスクと交換します。

   `storage disk replace -disk spare_data -replacement spare_root -action start`

   データはどちらの方向にもコピーできますが、ルートパーティションのコピーにかかる時間は短くなります。

3. ディスク交換の進捗を監視します。

   `storage aggregate show-status -aggregate aggr_name`

4. 交換処理が完了したら、もう一度スペアを表示して、スペアディスクがあることを確認します。

   `storage aggregate show-spare-disks -original-owner node_name`

   「Local Data Usable」との両方に、使用可能なスペースがあるスペアディスクが表示されます `Local Root Usable`。

例

ノードc1-01のスペアパーティションを表示して、スペアパーティションがアライメントされていないことを確認します。

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                                Local    Local
                                 Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- ------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block         0B 73.89GB  828.0GB
```

ディスク交換ジョブを開始します。

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

交換処理が完了するのを待っている間に、処理の進捗状況を表示します。

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                      Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

交換処理が完了したら、スペアディスクがあることを確認します。

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type    RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

関連情報

- "storage aggregate show"
- "storage disk replace"

ディスクの管理

ONTAPのホットスペアディスクの機能

ホットスペアディスクは、ストレージシステムに割り当てられて使用可能なディスクで

すが、RAIDグループでは使用されておらず、データは格納されていません。

RAIDグループ内でディスク障害が発生すると、ホットスペアディスクが自動的にRAIDグループに割り当てられ、障害が発生したディスクと交換されます。障害ディスクのデータは、RAIDパリティディスクからホットスペア交換ディスクにバックグラウンドで再構築されます。再構築処理がファイルに記録され `/etc/message`、AutoSupportメッセージが送信されます。

使用可能なホットスペアディスクが障害ディスクと同じサイズでない場合は、次に大きいサイズのディスクが選択され、交換するディスクのサイズに合わせて縮小されます。

マルチディスクキャリアノディスクノスペアニカンスルヨウケン

ストレージの冗長性を最適化し、最適なディスクレイアウトを実現するためにONTAPがディスクコピーに費やす時間を最小限に抑えるには、マルチディスクキャリアのディスクに対して適切な数のスペアを用意することが重要です。

マルチディスクキャリアのディスクに対しては、常に2つ以上のホットスペアを用意しておく必要があります。Maintenance Center を使用できるようにし、同時に複数のディスク障害が発生した場合の問題を回避するには、 4 つ以上のホットスペアを用意して安定した運用を確保し、障害が発生したディスクを迅速に交換するようにします。

ONTAPでは、同時に2つのディスクで障害が発生した場合に利用できるホット スペアが2つしかないと、障害が発生したディスクとそのキャリア メイトの両方のコンテンツをスペア ディスクにスワップできないことがあります。このシナリオは膠着状態と呼ばれます。この状況が発生すると、EMSメッセージとAutoSupportメッセージで通知されます。交換用キャリアが使用可能になったら、EMSメッセージの手順に従います。詳細については、"NetAppナレッジベース: RAID レイアウトを自動修正できません - AutoSupportメッセージ"

スペア不足に対する警告を使用した**ONTAP**スペアディスクの管理

デフォルトでは、ストレージシステム内の各ドライブの属性に一致するホットスペアドライブが1本もない場合、警告がコンソールとログに出力されます。

システムがベストプラクティスに準拠するようにこれらの警告メッセージのしきい値を変更できます。

タスクの内容

推奨される最小数のスペア・ディスクを常に持つようにするには'min_sspare_count' RAIDオプションを2'に設定する必要があります

ステップ

1. オプションを「2`」に設定します。

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

関連情報

- "storage raid-options modify"

ONTAPルート/データパーティショニングの追加の管理オプション

ルート データ パーティショニング オプションは、ブート メニューから使用でき、ルート データ パーティショニング用に構成されたディスクに追加の管理機能を提供します。

ブートメニューオプション9では、次の管理機能を使用できます。

- すべてのディスクのパーティションを解除し、ディスクの所有権情報を削除します。

  このオプションは、ルート/データパーティショニング用に設定されたシステムを別の設定で再初期化する必要がある場合に役立ちます。

- パーティショニングされたディスクを含むノードをクリーンアップして初期化します。

  このオプションは、次の場合に役立ちます。

  - ルート/データパーティショニング用に設定されていないシステムをルート/データパーティショニング用に設定する
  - ルート/データパーティショニング用に正しく設定されていないシステムを修正する必要がある
  - 以前のバージョンのルート/データパーティショニング用に設定されたSSDのみが接続されたAFFプラットフォームまたはFASプラットフォームを使用しており、ルート/データパーティショニングを新しいバージョンにアップグレードしてストレージ効率を向上させる場合

- 構成を消去し、ディスク全体を含むノードを初期化します。

  このオプションは、次の処理が必要な場合に役立ちます。

  - 既存のパーティションのパーティショニングを解除する
  - ローカルディスクの所有権を削除する
  - RAID-DPを使用してディスク全体を含むシステムを再初期化する

ONTAP Disk Qualification Packageを更新するタイミングについて

Disk Qualification Package（DQP）は、新しく認定されたドライブに対する完全なサポートを追加するパッケージです。ドライブファームウェアを更新したり、新しいタイプやサイズのドライブをクラスタに追加したりする前に、DQPを更新する必要があります。また、四半期ごとや半年ごとなど、DQPを定期的に更新することを推奨します。

次の状況では、DQPをダウンロードしてインストールする必要があります。

- 新しいタイプやサイズのドライブをノードに追加したとき

  たとえば、1TBのドライブをすでに使用している場合に2TBのドライブを追加するには、DQPの最新情報を確認する必要があります。

- ディスクファームウェアを更新したとき
- 新しいディスクファームウェアまたはDQPファイルが利用可能になったとき
- ONTAPの新しいバージョンにアップグレードするとき。

  ONTAPアップグレードの一環としてDQPが更新されることはありません。

関連情報

"NetAppのダウンロード：Disk Qualification Package"

"NetAppのダウンロード：ディスクドライブファームウェア"

ディスクとパーティションの所有権

ONTAPディスクとパーティションの所有権を管理します。

ディスクとパーティションの所有権を管理できます。

次のタスクを実行できます。

- "ディスクとパーティションの所有権を表示します。"**

  ディスク所有権を表示して、ストレージを制御しているノードを特定できます。共有ディスクを使用するシステムのパーティション所有権も表示できます。

- "ディスク所有権の自動割り当てに関する設定の変更"**

  デフォルト以外のポリシーを選択してディスク所有権を自動的に割り当てることも、ディスク所有権の自動割り当てを無効にすることもできます。

- "パーティショニングされていないディスクの所有権を手動で割り当てる"**

  ディスク所有権の自動割り当てを使用するようにクラスタが設定されていない場合は、所有権を手動で割り当てる必要があります。

- "パーティショニングされたディスクの所有権を手動で割り当てる"**

  コンテナディスクまたはパーティションの所有権は、パーティショニングされていないディスクの場合と同様に、手動で設定することも、自動割り当てを使用して設定することもできます。

- "障害ディスクの取り外し"**

  完全に障害が発生したディスクは、ONTAPでは使用可能なディスクとみなされなくなり、ディスクをシェルフからただちに取り外すことができます。

- "ディスクから所有権を削除する"**

  ONTAPは、ディスク所有権情報をディスクに書き込みます。スペアディスクまたはそのシェルフをノードから取り外す前に、所有権情報を削除して、別のノードに適切に統合できるようにする必要があります。

ONTAPディスク所有権の自動割り当てについて

未割り当てディスクの自動割り当てはデフォルトで有効になっています。ディスク所有権の自動割り当ては、HAペアの初期化後10分、および通常のシステム動作中は5分おきに実行されます。

HA ペアに新しいディスクを追加する場合、たとえば、障害が発生したディスクを交換する場合、「スペア不足」メッセージに応答する場合、または容量を追加する場合、デフォルトの自動割り当てポリシーにより、ディスクの所有権がスペアとしてノードに割り当てられます。

デフォルトの自動割り当てポリシーは、プラットフォーム固有の特性（HAペアに搭載されているシェルフのみの場合）に基づいており、次のいずれかの方法（ポリシー）を使用してディスク所有権が割り当てられま

す。

割り当て方法	ノードの割り当てに影響します	割り当て方法にデフォルト設定されているプラットフォーム構成
ベイ	偶数番号のベイはノードAに、奇数番号のベイはノードBに割り当てられます。	1台の共有シェルフを使用するHAペア構成内のエントリレベル システム。
シェルフ	シェルフ内のすべてのディスクがノードAに割り当てられます。	1つのスタックに複数のシェルフが含まれるHAペア構成、およびノードごとに1つのスタックに複数のシェルフが含まれるMetroCluster構成内の、エントリレベル システム。
スプリット シェルフ このポリシーは、該当するプラットフォームおよびシェルフ構成のコマンドのパラメータ `storage disk option`の「default」値に該当し `-autoassign-policy`ます。	シェルフ左側のディスクはノードAに、右側のディスクはノードBに割り当てられます。工場からの出荷時、HAペアのシェルフには、シェルフの端から中央に向かって部分的にディスクが搭載されています。	ほとんどのAFFプラットフォームと一部のMetroCluster構成。
スタック	スタック内のすべてのディスクがノードAに割り当てられます。	エントリレベルのスタンドアロン システムおよびその他のすべての構成。
ハーフドロワー このポリシーは、該当するプラットフォームおよびシェルフ構成のコマンドのパラメータ `storage disk option`の「default」値に該当し `-autoassign-policy`ます。	DS460Cドロワーの左半分（ドライブベイ0_{5}）のすべてのドライブがノードAに割り当てられ、ドロワーの右半分（ドライブベイ$_{6}$11）のすべてのドライブがノードBに割り当てられます。 DS460CシェルフのみのHAペアを初期化する場合、ディスク所有権の自動割り当てはサポートされません。ハーフドロワーのポリシーに従って、ルートパーティションが設定されたルート/コンテナドライブを含むドライブに所有権を手動で割り当てる必要があります。	DS460Cシェルフのみを使用したHAペア（HAペアの初期化（ブートアップ）後） HAペアのブート後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して、残りのドライブ（ルートパーティションを含むルートドライブ/コンテナドライブを除く）と今後追加されるすべてのドライブに所有権が割り当てられます。 HAペアに他のシェルフモデルに加えてDS460Cシェルフがある場合は、ハーフドロワーポリシーは使用されません。使用されるデフォルトポリシーは、プラットフォーム固有の特性によって決まります。

自動割り当ての設定と変更：

- コマンドを使用すると、現在の自動割り当て設定（オン/オフ）を表示できます `storage disk option show`。
- 自動割り当てを無効にするには、コマンドを使用し `storage disk option modify`ます。
- デフォルトの自動割り当てポリシーが環境に適していない場合は、コマンドのパラメータを `storage disk option modify`使用して、ベイ、シェルフ、またはスタックの割り当て方法を指定（変更）できます `-autoassign-policy`。

  方法をご確認ください"ディスク所有権の自動割り当てに関する設定の変更"。

> ハーフドロワーおよびスプリットシェルフのデフォルトの自動割り当てポリシーは、ベイ、シェルフ、スタックのポリシーなどのユーザが設定できないため、一意です。

Advanced Drive Partitioning (ADP)システムで、収容数が半分のシェルフに対して自動割り当てを機能させるには、ドライブのタイプに基づいて正しいシェルフベイにドライブを取り付ける必要があります。

- DS460Cシェルフ以外のシェルフの場合は、左端と右端に均等にドライブを取り付けます。たとえば、DS224Cシェルフのベイ0$_{5に6本のドライブを、ベイ18}$23に6本のドライブを搭載したとします。
- DS460Cシェルフの場合は、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。残りのドライブについては、ドロワーの前から後ろまで列を埋めて、各ドロワーに均等に配置します。行を埋めるための十分なドライブがない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

  各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

> 収容数が半分のシェルフの正しいシェルフベイにドライブが取り付けられていない場合は、コンテナドライブに障害が発生して交換したときに、ONTAPで所有権が自動割り当てされません。この場合、新しいコンテナドライブの割り当てを手動で行う必要があります。コンテナドライブに所有権を割り当てると、必要なドライブのパーティショニングとパーティショニングの割り当てがONTAPによって自動的に処理されます。

自動割り当てが機能しない場合は、コマンドを使用してディスク所有権を手動で割り当てる必要があり `storage disk assign`ます。

- 自動割り当てを無効にすると、新しいディスクがノードに手動で割り当てられるまでスペアとして使用できなくなります。
- 異なる所有権が必要なスタックまたはシェルフが複数ある場合にディスクを自動割り当てするには、各スタックまたはシェルフで所有権の自動割り当てが機能するように、各スタックまたはシェルフで1つのディスクを手動で割り当てておく必要があります。
- 自動割り当てが有効になっている場合に、アクティブポリシーで指定されていないノードにドライブを手動で1本割り当てると、自動割り当てが停止し、EMSメッセージが表示されます。

方法をご確認ください"パーティショニングされていないディスクのディスク所有権を手動で割り当てる"。

方法をご確認ください"パーティショニングされたディスクのディスク所有権を手動で割り当てる"。

関連情報

- "storage disk assign"

- "ストレージディスクオプションの変更"
- "ストレージディスクオプションの表示"

ONTAPディスクとパーティションの所有権を表示します。

ディスク所有権を表示して、ストレージを制御しているノードを特定できます。共有ディスクを使用するシステムのパーティション所有権も表示できます。

手順

1. 物理ディスクの所有権を表示します。

   ```
   storage disk show -ownership
   ```

   ```
   cluster::> storage disk show -ownership
   Disk     Aggregate Home     Owner    DR Home  Home ID     Owner ID   DR
   Home ID  Reserver    Pool
   -------- --------- -------- -------- -------- ---------- -----------
   ----------- ----------- ------
   1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
   2014941509  Pool0
   1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
   2014941509  Pool0
   1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
   2014941219  Pool0
   1.0.3    -         node1    node1    -        2014941219 2014941219  -
   2014941219  Pool0
   ```

2. 共有ディスクを使用するシステムの場合は、パーティション所有権を表示できます。

   ```
   storage disk show -partition-ownership
   ```

```
cluster::> storage disk show -partition-ownership
                                 Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

関連情報

- "storage disk show"

ONTAPディスク所有権の自動割り当てに関する設定の変更

コマンドを使用して、ディスク所有権を自動的に割り当てるデフォルト以外のポリシーを選択したり、ディスク所有権の自動割り当てを無効にしたりできます `storage disk option modify`。

詳細はこちらをご覧ください "ディスク所有権の自動割り当て"。

タスクの内容

DS460Cシェルフのみを使用するHAペアの場合、デフォルトの自動割り当てポリシーはハーフドロワーです。デフォルト以外のポリシー（ベイ、シェルフ、スタック）に変更することはできません。

手順

1. ディスクの自動割り当てを変更します。
   a. デフォルト以外のポリシーを選択するには、次のように入力します。

      `storage disk option modify -autoassign-policy` *`autoassign_policy`* `-node` *`node_name`*

      - `*autoassign_policy*`所有権の自動割り当てをスタックレベルまたはループレベルで実行するように設定するには、としてを使用し `stack`ます。
      - 所有権の自動割り当てをシェルフレベルで実行するように設定するには、として `*autoassign_policy*`を使用し `shelf`ます。
      - 所有権の自動割り当てをベイレベルで実行するように設定するには、として `*autoassign_policy*`を使用し `bay`ます。

   b. ディスク所有権の自動割り当てを無効にする場合は、次のように入力します。

```
storage disk option modify -autoassign off -node node_name
```

2. ディスクの自動割り当ての設定を確認します。

```
storage disk option show
```

```
cluster1::> storage disk option show

Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                           Assign Policy
-------------  -------------  ------------  -------------  --------
cluster1-1     on             on            on             default
cluster1-2     on             on            on             default
```

関連情報

- "ストレージディスクオプションの変更"
- "ストレージディスクオプションの表示"

パーティショニングされていないディスクの**ONTAP**ディスク所有権を手動で割り当てる

ディスク所有権の自動割り当てを使用するようにHAペアが設定されていない場合は、所有権を手動で割り当てる必要があります。DS460Cシェルフだけが搭載されているHAペアを初期化する場合は、ルート ドライブの所有権を手動で割り当てる必要があります。

タスクの内容

- DS460Cシェルフだけのない初期化前のHAペアで所有権を手動で割り当てる場合は、オプション1を使用します。
- DS460Cシェルフしかないペアを初期化する場合は、オプション2を使用してルートドライブの所有権を手動で割り当てます。

オプション**1**：ほとんどの**HA**ペア

DS460Cシェルフだけのないペアで初期化を実行していない場合は、次の手順に従って手動で所有権を割り当てます。

タスクの内容

- 所有権を割り当てるディスクは、所有権を割り当てるノードに物理的にケーブル接続されたシェルフに含まれている必要があります。
- ローカル階層（アグリゲート）内のディスクを使用する場合：
  - ディスクをローカル階層（アグリゲート）で使用するには、そのディスクがノードに所有されていなければなりません。
  - ローカル階層（アグリゲート）で使用中のディスクの所有権を再割り当てすることはできません。

手順

1. CLIを使用して、所有権が未設定のディスクをすべて表示します。

   ```
   storage disk show -container-type unassigned
   ```

2. それぞれのディスクを割り当てます。

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。すでに別のノードで所有されているスペアディスクを再割り当てする場合は、「-force」オプションを使用する必要があります。

初期化するHAペアで、DS460Cシェルフしかない場合は、次の手順に従ってルートドライブの所有権を手動で割り当てます。

タスクの内容

- DS460Cシェルフのみを含むHAペアを初期化する場合は、ハーフドロワーのポリシーに準拠するようにルートドライブを手動で割り当てる必要があります。

  HAペアの初期化（ブートアップ）後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して残りのドライブ（ルートドライブ以外）と今後追加されるドライブ（障害ディスクの交換、「low spares」メッセージへの応答、容量の追加など）に所有権が割り当てられます。

  "ハーフドロワーポリシーの詳細"です。

- DS460Cシェルフに8TBを超えるNL-SASドライブを搭載する場合、RAIDにはHAペアごとに最低10本のドライブ（各ノードに5本）が必要です。

手順

1. DS460Cシェルフがフル装備されていない場合は、次の手順を実行します。フル装備されていない場合は、次の手順に進みます。

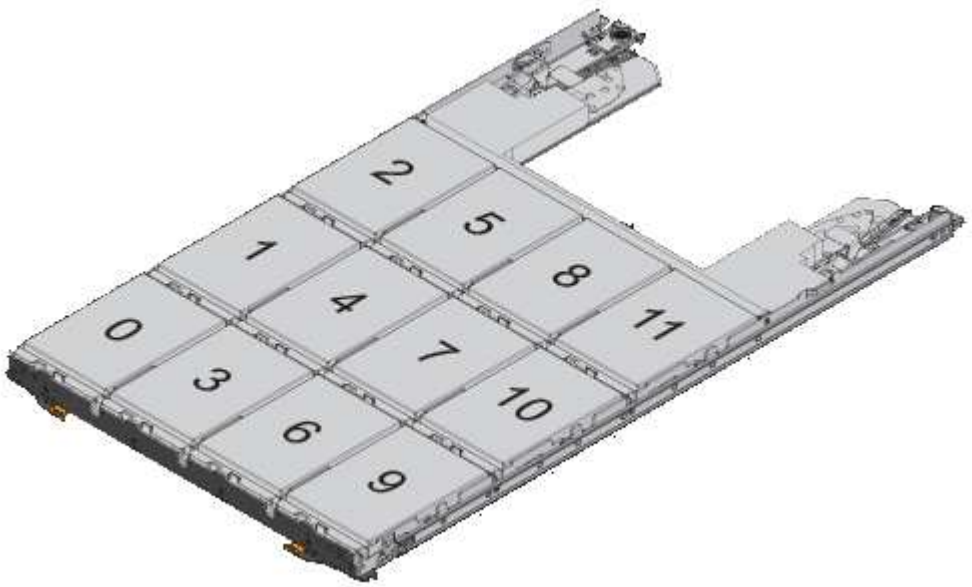
   a. まず、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。

      各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

   b. 残りのドライブについては、各ドロワーに均等に配置します。

      ドロワーの列への取り付けを前面から背面へ進めます。列がドライブで埋まりきらない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

      次の図は、DS460Cドロワー内のドライブ ベイの番号と場所を表しています。



2. ノード管理LIFまたはクラスタ管理LIFを使用してクラスタシェルにログインします。
3. 次の手順を使用して、ハーフドロワーポリシーに準拠するように各ドロワーのルートドライブを手動で割り当てます。

   ハーフドロワーポリシーでは、ドロワーのドライブの左半分（ベイ0$_{5}$）をノードAに、右半分（ベイ$_{6}$11）をノードBに割り当てます。

   a. 所有権が未設定のディスクをすべて表示します。
      `storage disk show -container-type unassigned`
   b. ルートディスクを割り当てます。
      `storage disk assign -disk disk_name -owner owner_name`

      ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。

の詳細については `storage disk`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "storage disk assign"
- "storage disk show"

ONTAPパーティショニングされたディスクの所有権を手動で割り当てる

Advanced Drive Partitioning (ADP)システムのコンテナディスクまたはパーティションの所有権は手動で割り当てることができます。DS460Cシェルフのみを含むHAペアを初期化する場合は、ルートパーティションを含むコンテナドライブの所有権を手動で割り当てる必要があります。

タスクの内容

- サポートされるADPの方式は、ストレージシステムのタイプによって異なります。root-data（RD）とroot-data-data（RD2）のどちらかです。

  FASストレージシステムはRDを使用し、AFFストレージシステムはRD2を使用します。

- DS460Cシェルフだけがないペアの所有権を手動で割り当てる場合は、オプション1を使用してルート/データ（RD）パーティショニングを使用してディスクを手動で割り当てるか、オプション2を使用してルート/データ（RD2）パーティショニングを使用してディスクを手動で割り当てることができます。
- DS460Cシェルフしかないペアを初期化する場合は、オプション3を使用して、ルートパーティションを含むコンテナドライブに所有権を手動で割り当てます。

オプション1：ルート/データ（RD）パーティショニングを使用してディスクを手動で割り当てる

ルート/データパーティショニングでは、HAペアがまとめて所有する所有権の3つのエンティティ（コンテナディスクと2つのパーティション）があります。

タスクの内容

- コンテナディスクと2つのパーティションがHAペアの一方のノードに所有されているかぎり、すべてHAペアの同じノードに所有されている必要はありません。ただし、ローカル階層でパーティションを使用する場合は、そのパーティションがローカル階層の所有者と同じノードに所有されている必要があります。
- 収容数が半分のシェルフのコンテナディスクで障害が発生して交換した場合、この場合、ONTAPでは所有権が常に自動割り当てされるとは限らないため、ディスク所有権の手動割り当てが必要になることがあります。
- コンテナディスクが割り当てられると、ONTAPのソフトウェアは、必要なパーティショニングとパーティションの割り当てを自動的に処理します。

手順

1. CLIを使用して、パーティショニングされたディスクの現在の所有権を表示します。

   ```
   storage disk show -disk disk_name -partition-ownership
   ```

2. CLIの権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

3. 所有権を割り当てるエンティティに応じて適切なコマンドを入力します。

   いずれかの所有権エンティティがすでに所有されている場合は、オプションを含める必要があります `-force`。

所有権を割り当てる所有権のエンティティ	使用するコマンド
コンテナディスク	`storage disk assign -disk disk_name -owner owner_name`
データパーティション	`storage disk assign -disk disk_name -owner owner_name -data true`
ルートパーティション	`storage disk assign -disk disk_name -owner owner_name -root true`

オプション2：ルート/データ/データ（RD2）パーティショニングを使用してディスクを手動で割り当てる

ルート/データ/データパーティショニングの場合、HAペアがまとめて所有する所有権の4つのエンティティ（コンテナディスクと3つのパーティション）があります。ルート/データ/データパーティショニングは、ルートパーティションとして小さなパーティションを1つ作成し、データ用に同じサイズの大きなパーティションを2つ作成します。

タスクの内容

- ルート/データ/データパーティショニングされたディスクに適切なパーティションを割り当てるには、コマンドでパラメータを使用する必要があります `disk assign`。これらのパラメータは、ストレージプールに含まれるディスクでは使用できません。デフォルト値はです `false`。
  - パラメータは `-data1 true`、パーティショニングされたroot-data1-data2ディスクのパーティションを割り当て `data1`ます。
  - パラメータは `-data2 true`、パーティショニングされたroot-data1-data2ディスクのパーティションを割り当て `data2`ます。
- 収容数が半分のシェルフのコンテナディスクで障害が発生して交換した場合、この場合、ONTAPでは所有権が常に自動割り当てされるとは限らないため、ディスク所有権の手動割り当てが必要になることがあります。
- コンテナディスクが割り当てられると、ONTAPのソフトウェアは、必要なパーティショニングとパーティションの割り当てを自動的に処理します。

手順

1. CLIを使用して、パーティショニングされたディスクの現在の所有権を表示します。

   ```
   storage disk show -disk disk_name -partition-ownership
   ```

2. CLIの権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

3. 所有権を割り当てるエンティティに応じて適切なコマンドを入力します。

   いずれかの所有権エンティティがすでに所有されている場合は、オプションを含める必要があります `-force`。

所有権を割り当てる所有権のエンティティ	使用するコマンド
コンテナディスク	`storage disk assign -disk disk_name -owner owner_name`
Data1パーティション	`storage disk assign -disk disk_name -owner owner_name -data1 true`
Data2パーティション	`storage disk assign -disk disk_name -owner owner_name -data2 true`

ルートパーティション	`storage disk assign -disk disk_name -owner owner_name -root true`

オプション3：ルートパーティションを含むDS460Cコンテナドライブを手動で割り当てる

DS460Cシェルフのみを含むHAペアを初期化する場合は、ハーフドロワーのポリシーに従って、ルートパーティションを含むコンテナドライブに所有権を手動で割り当てる必要があります。

タスクの内容

- DS460Cシェルフのみで構成されるHAペアを初期化する場合、ADPブートメニューのオプション9aおよび9bはドライブ所有権の自動割り当てをサポートしません。ハーフドロワーポリシーに従って、ルートパーティションを持つコンテナドライブを手動で割り当てる必要があります。

  HA ペアの初期化 (起動) 後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して、残りのドライブ (ルート パーティションを持つコンテナ ドライブ以外) と、障害が発生したドライブの交換、"スペア不足" メッセージへの対応、容量の追加など、将来追加されるドライブに所有権が割り当てられます。

- "ハーフドロワーポリシーの詳細"です。

手順

1. DS460Cシェルフがフル装備されていない場合は、次の手順を実行します。フル装備されていない場合は、次の手順に進みます。

   a. まず、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。

      各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

   b. 残りのドライブについては、各ドロワーに均等に配置します。

      ドロワーの列への取り付けを前面から背面へ進めます。行を埋めるための十分なドライブがない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

      次の図は、DS460Cドロワー内のドライブ ベイの番号と場所を表しています。

2. ノード管理LIFまたはクラスタ管理LIFを使用してクラスタシェルにログインします。

3. 各ドロワーについて、次の手順を実行してハーフドロワーポリシーに準拠し、ルートパーティションを含むコンテナドライブを手動で割り当てます。

   ハーフドロワーポリシーでは、ドロワーのドライブの左半分（ベイ0$_{5}$）をノードAに、右半分（ベイ$_{6}$11）をノードBに割り当てます。

   a. 所有権が未設定のディスクをすべて表示します。
      `storage disk show -container-type unassigned`
   b. ルートパーティションを含むコンテナドライブを割り当てます。
      `storage disk assign -disk disk_name -owner owner_name`

      ワイルドカード文字を使用すると、一度に複数のドライブを割り当てることができます。

関連情報

- "storage disk assign"
- "storage disk show"

ルート/データパーティショニングを使用して、**ONTAP**ノードにアクティブ/パッシブ構成を設定する

工場出荷時にルート/データパーティショニングを使用するようにHAペアが構成されている場合、アクティブ/アクティブ構成で使用するために、データパーティションの所有権がペアの両方のノードに分割されます。アクティブ/パッシブ構成でHAペアを使用する場合は、データローカル階層を作成する前にパーティションの所有権を更新する必要があります。

開始する前に

- アクティブノードにするノードとパッシブノードにするノードを決めておく必要があります。
- HAペアでストレージフェイルオーバーを設定する必要があります。

タスクの内容

このタスクは、2つのノード（ノードAとノードB）で実行します。

この手順は、パーティショニングされたディスクからデータローカル階層が作成されていないノードを対象としています。

詳細はこちらをご覧ください "高度なディスクパーティショニング"。

手順

コマンドはすべてクラスタシェルで入力します。

1. データパーティションの現在の所有権を表示します。

   `storage aggregate show-spare-disks`

   出力から、一方のノードが半数のデータパーティションを所有し、もう一方のノードが半数のデータパーティションを所有していることがわかります。すべてのデータパーティションがスペアである必要があります。

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.5                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                     BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                     BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                      BSAS    7200 block           753.8GB
```

```
73.89GB  828.0GB
 1.0.9                        BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. advanced権限レベルに切り替えます。

   `set advanced`

3. パッシブノードにするノードが所有する各データパーティションをアクティブノードに割り当てます。

   `storage disk assign -force -data true -owner active_node_name -disk disk_name`

   パーティションをディスク名の一部に含める必要はありません。

   再割り当てが必要なデータパーティションごとに、次の例のようなコマンドを入力します。

   `storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3`

4. すべてのパーティションがアクティブノードに割り当てられていることを確認します。

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                              Local
Local
                                                               Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
```

```
0B  828.0GB
 1.0.7                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                       BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                         Type     RPM Checksum         Usable
Usable     Size
 ---------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                        BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

cluster1-02は引き続きスペアルートパーティションを所有していることに注意してください。

5. admin権限に戻ります。

   ```
   set admin
   ```

6. データローカル階層を作成し、少なくとも1つのデータパーティションをスペアとして残します。

   ```
   storage aggregate create new_aggr_name -diskcount number_of_partitions -node
   active_node_name
   ```

   データローカル階層が作成され、アクティブノードが所有します。

関連情報

- "storage aggregate create"
- "storage aggregate show"
- "storage disk assign"

工場出荷時にルート/データ/データパーティショニングを使用するようにHAペアが構成されている場合、アクティブ/アクティブ構成で使用するために、データパーティションの所有権がペアの両方のノードに分割されます。アクティブ/パッシブ構成でHAペアを使用する場合は、データローカル階層を作成する前にパーティションの所有権を更新する必要があります。

開始する前に

- アクティブノードにするノードとパッシブノードにするノードを決めておく必要があります。
- HAペアでストレージフェイルオーバーを設定する必要があります。

タスクの内容

このタスクは、2つのノード（ノードAとノードB）で実行します。

この手順は、パーティショニングされたディスクからデータローカル階層が作成されていないノードを対象としています。

詳細はこちらをご覧ください "高度なディスクパーティショニング"。

手順

コマンドはすべてクラスタシェルで入力します。

1. データパーティションの現在の所有権を表示します。

   ```
   storage aggregate show-spare-disks -original-owner passive_node_name -fields
   local-usable-data1-size, local-usable-data2-size
   ```

   出力から、一方のノードが半数のデータパーティションを所有し、もう一方のノードが半数のデータパーティションを所有していることがわかります。すべてのデータパーティションがスペアである必要があります。

2. advanced権限レベルに切り替えます。

   ```
   set advanced
   ```

3. パッシブ ノードとして指定するノードが所有する各data1パーティションをアクティブ ノードに割り当てます。

   ```
   storage disk assign -force -data1 -owner active_node_name -disk disk_name
   ```

   パーティションをディスク名の一部として含める必要はありません。

4. パッシブノードになるノードが所有する data2 パーティションごとに、アクティブノードに割り当てます。

   ```
   storage disk assign -force -data2 -owner active_node_name -disk disk_name
   ```

   パーティションをディスク名の一部として含める必要はありません。

5. すべてのパーティションがアクティブノードに割り当てられていることを確認します。

storage aggregate show-spare-disks

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
```

```
Root Physical
 Disk                        Type      RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

cluster1-02は引き続きスペアルートパーティションを所有していることに注意してください。

6. admin権限に戻ります。

   ```
   set admin
   ```

7. データアグリゲートを作成します。少なくとも1つのデータパーティションをスペアとして残しておきます。

   ```
   storage aggregate create new_aggr_name -diskcount number_of_partitions -node
   active_node_name
   ```

   データアグリゲートが作成され、アクティブノードが所有します。

8. また、ONTAPで推奨されるローカル階層レイアウトを使用して、RAIDグループのレイアウトとスペア数のベストプラクティスを確認することもできます。

   ```
   storage aggregate auto-provision
   ```

関連情報

- "ストレージアグリゲートの自動プロビジョニング"
- "storage aggregate create"
- "storage aggregate show"
- "storage disk assign"

ディスクから**ONTAP**の所有権を削除する

ONTAPは、ディスク所有権情報をディスクに書き込みます。スペアディスクまたはそのシェルフをノードから取り外す前に、所有権情報を削除して、別のノードに適切に統合できるようにする必要があります。

ディスクがルート/データパーティショニング用にパーティショニングされていて、ONTAP 9 .10.1以降を実行している場合は、NetAppテクニカルサポートに連絡して所有権を削除してください。詳細については、を参照してください"技術情報アーティクル「Failed to remove the owner of disk」"。

開始する前に

所有権を削除するディスクが次の要件を満たしている必要があります。

- スペア ディスクである。

  ローカル階層で使用されているディスクから所有権を削除することはできません。

- Maintenance Centerに割り当てられていない。
- 完全消去の実行中ではない。
- 障害ディスクではない。

  障害ディスクから所有権を削除する必要はありません。

タスクの内容

ディスクの自動割り当てが有効になっている場合は、ノードからディスクを取り外す前に、ONTAPによって所有権が自動的に再割り当てされます。そのため、ディスクが取り外されるまで所有権の自動割り当てを無効にしてから再度有効にします。

手順

1. ディスク所有権の自動割り当てを有効にしている場合は、CLIを使用して無効にします。

   `storage disk option modify -node node_name -autoassign off`

2. 必要に応じて、ノードのHAパートナーに対して同じ手順を繰り返します。
3. ディスクからソフトウェア所有権情報を削除します。

   `storage disk removeowner disk_name`

   複数のディスクから所有権情報を削除するには、カンマで区切って指定します。

   例：

   ```
   storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
   ```

4. ディスクがルート/データパーティショニング用にパーティショニングされていて、ONTAP 9 .9.1以前を実行している場合は、パーティションから所有権を削除します。

   `storage disk removeowner -disk disk_name -root true`

   `storage disk removeowner -disk disk_name -data true`

   両方のパーティションがどのノードにも所有されなくなります。

5. 以前にディスク所有権の自動割り当てを無効にした場合は、ディスクを取り外したあとまたは再割り当てしたあとに再度有効にします。

   `storage disk option modify -node node_name -autoassign on`

6. 必要に応じて、ノードのHAパートナーに対して同じ手順を繰り返します。

関連情報

- "ストレージディスクオプションの変更"
- "ストレージディスクの所有者の削除"

障害が発生した**ONTAP**ディスクを取り外します。

完全な障害状態のディスクは、ONTAPで使用可能なディスクとみなされなくなり、ディスクシェルフからただちに取り外すことができます。ただし、障害が部分的に発生したディスクは、高速RAIDリカバリプロセスが完了するまで接続したままにしておく必要があります。

タスクの内容

障害が発生した場合、またはエラーメッセージが大量に表示されているためにディスクを取り外す場合は、このストレージシステムまたは他のストレージシステムでそのディスクを再度使用しないでください。

手順

1. CLIを使用して、障害ディスクのディスクIDを確認します。

   ```
   storage disk show -broken
   ```

   障害ディスクのリストにディスクが表示されない場合は、部分的に障害が発生しており、高速RAIDリカバリが実行中である可能性があります。この場合は、障害ディスクのリストにディスクが表示されるまで（高速RAIDリカバリプロセスが完了するまで）待ってから、ディスクを取り外してください。

2. 取り外すディスクの物理的な場所を確認します。

   ```
   storage disk set-led -action on -disk disk_name 2
   ```

   ディスク前面の障害LEDが点灯します。

3. ディスクシェルフモデルのハードウェアガイドの手順に従って、ディスクシェルフからディスクを取り外します。

関連情報

- "ストレージディスクセット主導"
- "storage disk show"

ディスク完全消去

ONTAPディスク完全消去の詳細

ディスク完全消去は、元のデータのリカバリが不可能になるように、指定したバイトパターンまたはランダムデータでディスクまたはSSDを上書きして、データを物理的に消去するプロセスです。完全消去プロセスを使用すると、ディスク上のデータをリカバリできなくなります。

この機能は、すべてのONTAP 9リリースのノードシェルから、およびONTAP 9 .6以降のメンテナンスモードで使用できます。

ディスク完全消去プロセスでは、1回の処理で最大7サイクル、デフォルトまたはユーザ指定の3回の上書きパ

ターンが使用されます。サイクルごとにランダムな上書きパターンが繰り返されます。

ディスク容量、パターン、およびサイクル数によっては、プロセスに数時間かかることがあります。完全消去はバックグラウンドで実行されます。完全消去プロセスは、開始、停止、およびステータスの表示が可能です。完全消去プロセスには、「フォーマットフェーズ」と「パターン上書きフェーズ」の2つのフェーズがあります。

フォーマットフェーズ

次の表に示すように、フォーマットフェーズで実行される処理は、完全消去するディスクのクラスによって異なります。

ディスククラス	フォーマットフェーズ処理
大容量HDD	スキップ
ハイパフォーマンスHDD	SCSIフォーマット処理
SSD	SCSI完全消去処理

パターン上書きフェーズ

指定した上書きパターンが指定したサイクル数だけ反復されます。

完全消去プロセスが完了すると、指定したディスクは完全に消去された状態になります。自動的にスペアのステータスには戻りません。新たに完全消去したディスクを別のローカル階層に追加できるようにするには、完全消去したディスクをスペアプールに戻す必要があります。

ONTAPディスク完全消去を実行できない状況について

このような状況ではディスク完全消去を実行できません。

- HAペアのシステムのテイクオーバーモードではサポートされません。
- 読み取り / 書き込みの問題が原因で障害が発生したディスクでは実行できません。
- ランダムパターンを使用する場合、一度に100を超えるディスクで実行することはできません。
- アレイLUNではサポートされません。

ONTAPディスク完全消去が中断された場合の動作

ユーザの介入や予期しない停電などによってディスク完全消去が中断された場合、ONTAPは完全消去していたディスクを既知の状態に戻しますが、完全消去プロセスを完了する前にも処理を実行する必要があります。

ディスク完全消去の処理には時間がかかります。停電、システムパニック、または手動操作によって完全消去プロセスが中断された場合は、完全消去プロセスを最初からやり直す必要があります。この場合、ディスクは完全消去済みとはみなされません。

ディスク完全消去のフォーマットフェーズが中断された場合、ONTAPは、中断によって破損したディスクをすべてリカバリする必要があります。ONTAPでは、システムのリブート後、1時間に1回、完全消去のフォーマットフェーズが完了していないターゲットディスクがないかどうかを確認します。そのようなディスクが検出されると、ONTAPはそれらのディスクをリカバリします。リカバリ方法はディスクの種類によって異なります。ディスクのリカバリが完了したら、そのディスクで完全消去プロセスを再実行できます。HDDの場合は、オプションを使用して、フォーマットフェーズを繰り返さないように指定できます。 `-s`

完全消去が必要なデータを含むローカル階層を作成またはバックアップする場合は、いくつかの簡単なガイドラインに従うことで、データ完全消去にかかる時間を短縮できます。

- 機密データが格納されているローカル階層のサイズが必要以上になっていないことを確認してください。

  必要以上に大きい場合、完全消去にはより多くの時間、ディスクスペース、帯域幅が必要になります。

- 機密データを含むローカル階層をバックアップする場合は、機密データが大量に含まれているローカル階層へのバックアップは避けてください。

  これにより、機密データを完全消去する前に、非機密データの移動に必要なリソースを削減できます。

ONTAPディスクを完全消去します。

ディスクを完全消去すると、運用を停止したシステムや動作しないシステムのディスクまたは一連のディスクからデータを削除して、データを決してリカバリできないようにすることができます。

CLIを使用したディスクの完全消去には、次の2つの方法があります。

ONTAP 9 .6以降では、メンテナンスモードでディスク完全消去を実行できます。

開始する前に

- Self-Encrypting Disk（SED；自己暗号化ディスク）を使用することはできません。

  SEDを完全消去するには、コマンドを使用する必要があります `storage encryption disk sanitize`。

  "保存データの暗号化"

  の詳細については `storage encryption disk sanitize`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. メンテナンスモードでブートします。
   a. と入力して、現在のシェルを終了し `halt`ます。

      Loaderプロンプトが表示されます。

   b. と入力して保守モードに切り替え `boot_ontap maint`ます。

      いくつかの情報が表示されると、メンテナンスモードのプロンプトが表示されます。

2. 完全消去するディスクがパーティショニングされている場合は、各ディスクのパーティショニングを解除します。

   ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用できます。NetAppサポートから指示があった場合にのみ実行してください。作業を進める前に、NetAppサポートに問い合わせることを推奨します。また、"NetAppナレッジベース: ONTAPでスペアドライブのパーティションを解除する方法"

   ```
   disk unpartition <disk_name>
   ```

3. 指定したディスクを完全消去します。

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-r]]] [-c <cycle_count>] <disk_list>
   ```

   完全消去中は、ノードの電源をオフにしたり、ストレージの接続を切断したり、ターゲットディスクを取り外したりしないでください。完全消去のフォーマットフェーズで処理が中断された場合は、ディスクを完全消去してスペアプールに戻す前に、フォーマットフェーズを再開して完了する必要があります。完全消去プロセスを中止する必要がある場合は、コマンドを使用します `disk sanitize abort`。指定したディスクで完全消去のフォーマットフェーズが進行中の場合、フェーズが完了するまで中止は実行されません。

`-p` `<pattern1>` `-p` `<pattern2>` `-p` `<pattern3>`1~3サイクルのユーザ定義の上書きパターンを16進数で指定します。このパターンは、完全消去するディスクに順に適用されます。デフォルトのパターンは3つのパスで、最初のパスに0x55、2番目のパスに0xaa、3番目のパスに0x3Cを使用します。

`-r`パターン化された上書きを、一部またはすべてのパスのランダムな上書きに置き換えます。

-c `<cycle_count>`指定した上書きパターンを適用する回数を指定します。デフォルト値は1サイクルです。最大値は7サイクルです。

`<disk_list>`完全消去するスペアディスクのIDを、スペースで区切って指定します。

4. 必要に応じて、ディスク完全消去プロセスのステータスを確認します。

   ```
   disk sanitize status [<disk_list>]
   ```

5. 完全消去プロセスが完了したら、各ディスクのディスクをスペアステータスに戻します。

   ```
   disk sanitize release <disk_name>
   ```

6. メンテナンスモードを終了します。

ディスクをノードシェルノードシェルのコマンドによって完全消去する（すべてのONTAP 9リリース）

ノードでノードシェルコマンドを使用してディスク完全消去機能を有効にしたあとに無効にすることはできません。

開始する前に

- ディスクはスペアディスクである必要があります。ノードに所有されていて、ローカル階層で使用されていないディスクである必要があります。

  ディスクがパーティショニングされている場合、どちらのパーティションもローカル階層で使用できません。

- Self-Encrypting Disk（SED；自己暗号化ディスク）を使用することはできません。

  SEDを完全消去するには、コマンドを使用する必要があります `storage encryption disk sanitize`。

  "保存データの暗号化"

- ストレージプールに含めることはできません。

手順

1. 完全消去するディスクがパーティショニングされている場合は、各ディスクのパーティショニングを解除します。

   ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用できます。NetAppサポートから指示があった場合にのみ実行してください。続行する前に**NetApp**サポートに連絡することを強くお勧めします。また、"NetAppナレッジベース: ONTAPでスペアドライブのパーティションを解除する方法" 。

   ```
   disk unpartition <disk_name>
   ```

2. 完全消去するディスクを所有するノードのノードシェルに切り替えます。

   ```
   system node run -node <node_name>
   ```

3. ディスク完全消去を有効にします。

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   このコマンドは取り消すことができないため、確認を求められます。

4. ノードシェルのadvanced権限レベルに切り替えます。

   ```
   priv set advanced
   ```

5. 指定したディスクを完全消去します。

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-r]]] [-c <cycle_count>] <disk_list>
   ```

完全消去中は、ノードの電源をオフにしたり、ストレージの接続を切断したり、ターゲットディスクを取り外したりしないでください。完全消去のフォーマットフェーズで処理が中断された場合は、ディスクを完全消去してスペアプールに戻す前に、フォーマットフェーズを再開して完了する必要があります。完全消去プロセスを中止する必要がある場合は、 disk sanitize abort コマンドを使用します。指定したディスクで完全消去のフォーマットフェーズが進行中の場合、フェーズが完了するまで中止は実行されません。

`-p <pattern1> -p <pattern2> -p <pattern3>`1~3サイクルのユーザ定義の上書きパターンを16進数で指定します。このパターンは、完全消去するディスクに順に適用されます。デフォルトのパターンは3つのパスで、最初のパスに0x55、2番目のパスに0xaa、3番目のパスに0x3Cを使用します。

`-r`パターン化された上書きを、一部またはすべてのパスのランダムな上書きに置き換えます。

`-c <cycle_count>`指定した上書きパターンを適用する回数を指定します。

デフォルト値は1サイクルです。最大値は7サイクルです。

`<disk_list>`完全消去するスペアディスクのIDを、スペースで区切って指定します。

6. ディスク完全消去プロセスのステータスを確認するには、次のコマンドを入力します。

   ```
   disk sanitize status [<disk_list>]
   ```

7. 完全消去プロセスが完了したら、ディスクのステータスをスペアに戻します。

   ```
   disk sanitize release <disk_name>
   ```

8. ノードシェルのadmin権限レベルに戻ります。

   ```
   priv set admin
   ```

9. ONTAP CLIに戻ります。

   ```
   exit
   ```

10. すべてのディスクがスペアステータスに戻ったかどうかを確認します。

    ```
    storage aggregate show-spare-disks
    ```

状況	そしたら…。
完全消去したすべてのディスクがスペアとして表示される	これで終わりです。ディスクが完全消去され、スペアステータスになります。

完全消去した一部のディスクがスペアとして表示されない	次の手順を実行します。
	a. advanced権限モードに切り替えます。
	`set -privilege advanced`
	b. 完全消去した未割り当てのディスクを各ディスクの適切なノードに割り当てます。
	`storage disk assign -disk <disk_name> -owner <node_name>`
	c. 各ディスクのディスクをスペア状態に戻します。
	`storage disk unfail -disk <disk_name> -s -q`
	d. adminモードに戻ります。
	`set -privilege admin`

の詳細については `storage aggregate show-spare-disks`、を"ONTAPコマンド リファレンス"参照してください。

結果

指定したディスクが完全消去され、ホットスペアとして指定されます。完全消去したディスクのシリアル番号がに書き込まれ `/etc/log/sanitized_disks`ます。

指定したディスクの完全消去ログ（各ディスクで何が完了したかを示す）がに書き込まれます `/mroot/etc/log/sanitization.log`。

関連情報

- "storage aggregate show"
- "storage disk assign"
- "ストレージディスクの故障なし"
- "ストレージ暗号化ディスクサニタイズ"

ディスクの管理用**ONTAP**コマンド

コマンドと `storage aggregate`コマンドを使用して、ディスクを管理でき `storage disk`ます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

状況	使用するコマンド
スペアディスクのリストを表示する（所有者別のパーティショニングされたディスクを含む）	`storage aggregate show-spare-disks`
ローカル階層別のディスクのRAIDタイプ、現在の使用状況、およびRAIDグループを表示する	`storage aggregate show-status`
物理ディスクのRAIDタイプ、現在の使用状況、ローカル階層、およびRAIDグループ（スペアを含む）を表示する	`storage disk show -raid`
障害が発生したディスクのリストを表示します。	`storage disk show -broken`
ディスクのクラスタ構成前（nodescope）ドライブ名を表示する	`storage disk show -primary-paths`（アドバンスト）
特定のディスクまたはシェルフのLEDを点灯する	`storage disk set-led`
特定のディスクに対するチェックサム方式を表示する	`storage disk show -fields checksum-compatibility`
すべてのスペア ディスクに対するチェックサム方式を表示する	`storage disk show -fields checksum-compatibility -container-type spare`
ディスクの接続および配置の情報を表示する	`storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay`
特定のディスクのクラスタ構成前のディスク名を表示する	`storage disk show -disk diskname -fields diskpathnames`
Maintenance Centerに割り当てられたディスクの一覧を表示する	`storage disk show -maintenance`
SSDの書き込み回数上限値を表示する	`storage disk show -ssd-wear`
共有ディスクのパーティショニングを解除する	`storage disk unpartition`（diagnosticレベルで使用可能）
初期化されていないすべてのディスクを初期化する	`storage disk zerospares`
指定した1つ以上のディスク上で進行中の完全消去プロセスを停止する	`system node run -node nodename -command disk sanitize`

ストレージ暗号化に関するディスク情報を表示する	`storage encryption disk show`
リンクされたすべてのキー管理サーバから認証キーを取得する	`security key-manager restore`

関連情報

- "storage aggregate show"
- "ストレージディスクセット主導"
- "storage disk show"
- "storage disk zerospares"
- "storage disk show | more"

スペース使用量情報を表示する**ONTAP**コマンド

コマンドと `volume`コマンドを使用し `storage aggregate`て、ローカル階層、ボリューム、およびそれらのSnapshotでのスペースの使用状況を確認します。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

表示する情報	使用するコマンド

ローカル階層（使用済みスペースと使用可能スペースの割合、Snapshotリザーブのサイズ、その他のスペース使用量に関する情報を含む）	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

ローカル階層でのディスクとRAIDグループの使用方法およびRAIDのステータス	`storage aggregate show-status`
特定のSnapshotを削除した場合に再利用されるディスクスペースの量	`volume snapshot compute-reclaimable`

ボリュームによって使用されているスペースの量	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

包含ローカル階層でボリュームによって使用されているスペースの量	`volume show-footprint`

関連情報

- "storage aggregate show"
- "ストレージアグリゲートショースペース"
- "ストレージアグリゲートのステータス表示"

ストレージシェルフに関する情報を表示するONTAPコマンド

ディスクシェルフの構成情報やエラー情報を表示するには、コマンドを使用し `storage shelf show`ます。

表示する項目	使用するコマンド
シェルフの構成とハードウェアのステータスに関する一般的な情報	`storage shelf show`
特定のシェルフの詳細情報（スタックIDなど）	`storage shelf show -shelf`
シェルフごとの対応可能な未解決のエラー	`storage shelf show -errors`
ベイ情報	`storage shelf show -bay`
接続情報	`storage shelf show -connectivity`
冷却に関する情報（温度センサー、冷却ファンなど）	`storage shelf show -cooling`
I/Oモジュールに関する情報	`storage shelf show -module`
ポート情報	`storage shelf show -port`
電源に関する情報（Power Supply Unit（PSU;電源装置）、電流センサー、電圧センサーなど）	`storage shelf show -power`

関連情報

- "収納棚ショー"

RAID構成の管理

ONTAPローカル階層のデフォルトのRAIDポリシー

すべての新しいローカル階層に対するデフォルトのRAIDポリシーはRAID-DPまたはRAID-TECです。RAIDポリシーは、ディスク障害が発生した場合のパリティ保護を決定します。

RAID-DPは、単一または二重ディスク障害の発生時にダブルパリティ保護を提供します。RAID-DPは、次のローカル階層タイプのデフォルトのRAIDポリシーです。

- オールフラッシュローカル階層
- Flash Poolローカル階層
- 高パフォーマンスハードディスクドライブ（HDD）ローカル階層

RAID-TECは、AFFを含むすべてのディスクタイプとプラットフォームでサポートされます。大容量のディスクを含むローカル階層では、同時にディスク障害が発生する可能性が高くなります。RAID-TECはトリプルパリティ保護を提供することでこのリスクを軽減し、最大3本のディスクで同時に障害が発生してもデータを保護します。RAID-TECは、6TB以上のディスクを含む大容量HDDローカル階層に対するデフォルトのRAIDポリシーです。

各RAIDポリシータイプに必要なディスクの最小数：

- RAID-DP：5本
- RAID-TEC：7本

ディスクの**ONTAP RAID**保護レベル

ONTAPでは、ローカル階層に対して3つのレベルのRAID保護がサポートされます。RAID保護のレベルによって、ディスク障害が発生した場合にデータリカバリに使用できるパリティディスクの数が決まります。

RAID保護を使用すると、RAIDグループ内でデータディスク障害が発生した場合、ONTAPは障害ディスクをスペアディスクと交換し、パリティデータを使用して障害ディスクのデータを再構築できます。

- * RAID 4 *

  RAID 4保護を使用すると、ONTAPは1つのスペアディスクを使用して、RAIDグループ内の1つの障害ディスクを交換し、データを再構築できます。

- * RAID-DP *

  RAID-DP保護を使用すると、ONTAPは最大2本のスペアディスクを使用して、RAIDグループ内で同時に障害が発生した最大2本のディスクを交換し、データを再構築できます。

- * RAID-TEC *

  RAID-TEC保護を使用すると、ONTAPは最大3本のスペアディスクを使用して、RAIDグループ内で同時に障害が発生した最大3本のディスクを交換し、データを再構築できます。

ONTAPローカル階層のドライブと**RAID**グループの情報

一部のローカル階層の管理作業では、ローカル階層を構成するドライブのタイプ、サイズ、チェックサム、およびステータス、他のローカル階層と共有するかどうか、およびRAIDグループのサイズと構成を把握しておく必要があります。

ステップ

1. ローカル階層のドライブをRAIDグループ別に表示します。

   ```
   storage aggregate show-status aggr_name
   ```

ローカル階層内の各RAIDグループのドライブが表示されます。

ドライブ（データ、パリティ、ダブルパリティ）のRAIDタイプは列で確認できます `Position`。列にと表示されている `shared`場合 `Position`、ドライブは共有されます。HDDの場合はパーティショニングされたディスクです。SSDの場合はストレージプールの一部です。

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

関連情報

- "ストレージアグリゲートのステータス表示"

ONTAP RAID-DPから**RAID-TEC**への変換

トリプルパリティの保護を強化するには、RAID-DPをRAID-TECに変換します。ローカル階層で使用されているディスクのサイズが4TiBを超える場合は、RAID-TECを推奨します。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

変換するローカル階層には少なくとも7本のディスクが必要です。

タスクの内容

- ハードディスクドライブ（HDD）のローカル階層をRAID-DPからRAID-TECに変換できます。これには、Flash Poolローカル階層のHDD階層も含まれます。

手順

1. ローカル階層がオンラインで、少なくとも6本のディスクがあることを確認します。

   `storage aggregate show-status -aggregate aggregate_name`

2. ローカル階層をRAID-DPからRAID-TECに変換します。

   `storage aggregate modify -aggregate aggregate_name -raidtype raid_tec`

3. ローカル階層のRAIDポリシーがRAID-TECであることを確認します。

   `storage aggregate show aggregate_name`

関連情報

- "storage aggregate modify"
- "ストレージアグリゲートのステータス表示"

ONTAP RAID-TECから**RAID-DP**への変換

ローカル階層のサイズを縮小し、トリプルパリティが不要になった場合は、RAIDポリシーをRAID-TECからRAID-DPに変換して、RAIDパリティに必要なディスクの数を減らすことができます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

RAID-TECの最大RAIDグループサイズは、RAID-DPの最大RAIDグループサイズよりも大きくなります。最大RAID-TECグループサイズがRAID-DPの制限内に収まらない場合は、RAID-DPに変換できません。

タスクの内容

RAIDタイプ間の変換の影響については、コマンドのを参照してください "パラメータ" `storage aggregate modify`。

手順

1. ローカル階層がオンラインで、少なくとも6本のディスクがあることを確認します。

   ```
   storage aggregate show-status -aggregate aggregate_name
   ```

2. ローカル階層をRAID-TECからRAID-DPに変換します。

   ```
   storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
   ```

3. ローカル階層のRAIDポリシーがRAID-DPであることを確認します。

   ```
   storage aggregate show aggregate_name
   ```

関連情報

- "storage aggregate modify"
- "ストレージアグリゲートのステータス表示"

ONTAP RAIDグループのサイジングに関する考慮事項

最適なRAIDグループサイズを設定するには、さまざまな要素について優先度を考慮する必要があります。設定する（ローカル階層）アグリゲートにとって最も重要な要素（RAIDのリビルド速度、ドライブ障害によるデータ損失のリスクに対する保証、I/Oパフォーマンスの最適化、データストレージスペースの最大化）を決定する必要があります。

より大容量の RAID グループを作成すると ' パリティに使用されるストレージ容量（パリティの負荷）と同じ容量のデータ・ストレージに使用できる容量が最大化されます一方、大規模なRAIDグループでディスク障害が発生すると再構築時間が長くなり、パフォーマンスに影響が及ぶ期間が長くなります。また、RAIDグループ内のディスク数が多いほど、同じRAIDグループ内で複数のディスクに障害が発生する可能性が高くなります。

HDDまたはアレイ**LUN RAID**グループ

HDDまたはアレイLUNを構成するRAIDグループのサイジングを行う際は、次のガイドラインに従う必要があります。

- ローカル階層（アグリゲート）内のすべてのRAIDグループでディスク数を同じにする必要があります。

  1つのローカル階層上の複数のRAIDグループに含まれるディスク数の上限を50%以下にすることもできますが、パフォーマンスのボトルネックにつながる場合があるため、この方法を使用することを推奨します。

- RAIDグループのディスク数の推奨範囲は12~20です。

  信頼性の高いパフォーマンスディスクでは、必要に応じて最大28のRAIDグループサイズをサポートできます。

- 上記の2つのガイドラインを満たすディスク数が複数ある場合は、より多くのディスク数を選択してください。

Flash Poolローカル階層（アグリゲート）のSSD RAIDグループ

SSD RAIDグループサイズは、Flash Poolローカル階層（アグリゲート）のHDD RAIDグループのRAIDグループサイズと同じにすることはできません。通常は、パリティに必要なSSDの数を最小限に抑えるために、Flash Poolローカル階層のSSD RAIDグループは1つだけにします。

SSDローカル階層（アグリゲート）のSSD RAIDグループ

SSDを構成するRAIDグループのサイジングを行う際は、次のガイドラインに従う必要があります。

- ローカル階層（アグリゲート）内のすべてのRAIDグループで同数のドライブを配置する必要があります。

  RAIDグループは完全に同じサイズにする必要はありませんが、可能な場合は、同じローカル階層内に他のRAIDグループの半分未満のRAIDグループを配置しないようにしてください。

- RAID-DPの場合、RAIDグループサイズの推奨範囲は20~28です。

ONTAP RAIDグループのサイズのカスタマイズ

ローカル階層に含めるストレージの容量に適したRAIDグループサイズになるように、RAIDグループのサイズをカスタマイズできます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

タスクの内容

標準ローカル階層の場合は、各ローカル階層のRAIDグループのサイズを個別に変更します。Flash Poolローカル階層の場合は、SSD RAIDグループとHDD RAIDグループのサイズを個別に変更できます。

次に、RAIDグループサイズの変更に関する注意事項の概要を示します。

- デフォルトでは、最後に作成されたRAIDグループ内のディスクまたはアレイLUNの数が新しいRAIDグループサイズよりも少ない場合、新しいサイズに達するまで、最後に作成されたRAIDグループにディスクまたはアレイLUNが追加されます。
- そのローカル階層内の他の既存のRAIDグループのサイズは、明示的にディスクを追加しないかぎり変更されません。
- RAIDグループをローカル階層の現在の最大RAIDグループサイズよりも大きくすることはできません。
- すでに作成されているRAIDグループのサイズを縮小することはできません。
- 新しいサイズは、そのローカル階層内のすべてのRAIDグループ（Flash Poolローカル階層の場合は、該当するタイプのRAIDグループ（SSDまたはHDD）に適用されます。

手順

1. 該当するコマンドを使用します。

状況	入力するコマンド

Flash Poolローカル階層のSSD RAIDグループの最大サイズを変更する	`storage aggregate modify -aggregate aggr_name -cache-raid-group-size size`
他のRAIDグループの最大サイズを変更する	`storage aggregate modify -aggregate aggr_name -maxraidsize size`

例

ローカル階層n1_a4のRAIDグループの最大サイズをディスクまたはアレイLUN 20に変更するコマンドの例を次に示します。

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

Flash Poolローカル階層n1_cache_a2のSSDキャッシュRAIDグループの最大サイズを24に変更するコマンドの例を次に示します。

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

関連情報

- "storage aggregate modify"

Flash Poolローカル階層を管理します。

Flash Pool ONTAPローカル階層のキャッシングポリシー

Flash Poolローカル階層のボリュームに対するキャッシングポリシーでは、作業データセット用の高性能なキャッシュとしてフラッシュを導入し、アクセス頻度の低いデータには低コストのHDDを使用することができます。複数のFlash Poolローカル階層にキャッシュを提供する場合は、Flash Pool SSDパーティショニングを使用して、Flash Pool内のローカル階層間でSSDを共有します。

キャッシングポリシーは、Flash Poolのローカル階層にあるボリュームに適用されます。キャッシングポリシーを変更する前に、その仕組みを理解しておく必要があります。

ほとんどの場合、デフォルトのキャッシングポリシーを `auto`使用するのが最善のキャッシングポリシーです。キャッシングポリシーを変更する必要があるのは、別のポリシーでワークロードのパフォーマンスが向上する場合だけです。誤ったキャッシングポリシーを設定すると、ボリュームのパフォーマンスが大幅に低下し、時間が経つにつれてパフォーマンスの低下が徐 々 に増大する可能性があります。

キャッシングポリシーは、読み取りキャッシングポリシーと書き込みキャッシングポリシーを組み合わせたものです。ポリシー名は、読み取りキャッシングポリシーと書き込みキャッシングポリシーの名前をハイフンで区切って連結します。ポリシー名にハイフンが含まれていない場合、書き込みキャッシングポリシーはになります `none`（ポリシーを除く） `auto`。

読み取りキャッシングポリシーでは、HDDに格納されたデータに加えてデータのコピーがキャッシュに配置されるため、以降の読み取りパフォーマンスが最適化されます。書き込み処理用にキャッシュにデータを挿入する読み取りキャッシングポリシーの場合、キャッシュは _write-through キャッシュとして機能します。

書き込みキャッシングポリシーを使用してキャッシュに挿入されたデータはキャッシュにのみ存在し、HDD

にコピーが存在しません。Flash PoolキャッシュはRAIDで保護されています。書き込みキャッシュを有効にすると、書き込み処理のデータをキャッシュから即座に読み取りできるようになりますが、HDDへのデータの書き込みは、古くなってキャッシュから取り除かれるまで保留されます。

Flash Poolのローカル階層から単一階層のローカル階層にボリュームを移動すると、ボリュームのキャッシングポリシーが失われます。あとでボリュームをFlash Poolのローカル階層に戻すと、のデフォルトのキャッシングポリシーが割り当てられます。 `auto`2つのFlash Poolローカル階層間でボリュームを移動した場合、キャッシングポリシーは維持されます。

キャッシングポリシーを変更する

CLIでパラメータを使用してコマンドを実行 `volume create`すると、`Flash Pool`ローカル階層にあるボリュームのキャッシングポリシーを変更できます。 `-caching-policy`

Flash Poolローカル階層にボリュームを作成すると、デフォルトでは、 `auto`キャッシングポリシーがボリュームに割り当てられます。

Flash Poolのキャッシングポリシーを管理します。

Flash Poolローカル階層の**ONTAP**キャッシングポリシーを変更するかどうかを確認する

Flash Poolローカル階層内のボリュームにキャッシュ保持ポリシーを割り当てて、ボリュームデータをFlash Poolキャッシュに保存する期間を決定できます。ただし、キャッシュ保持ポリシーを変更しても、ボリュームのデータがキャッシュに保存される時間に影響を及ぼさない場合があります。

タスクの内容

データが次のいずれかの条件に当てはまる場合は、キャッシュ保持ポリシーを変更しても影響がない可能性があります。

- ワークロードがシーケンシャルである。
- ソリッドステートドライブ（SSD）にキャッシュされたランダムブロックがワークロードによって再度読み取られることはありません。
- ボリュームのキャッシュサイズが小さすぎます。

手順

次の手順では、データが満たす必要がある条件を確認します。このタスクは、advanced権限モードでCLIを使用して実行する必要があります。

1. CLIを使用してワークロードのボリュームを表示します。

   ```
   statistics start -object workload_volume
   ```

2. ボリュームのワークロードのパターンを確認します。

   ```
   statistics show -object workload_volume -instance volume-workload -counter
   sequential_reads
   ```

3. ボリュームのヒット率を確認します。

```
statistics show -object wafl_hya_vvol -instance volume -counter
read_ops_replaced_percent|wc_write_blks_overwritten_percent
```

4. ボリュームのとを `Project Cache Alloc`確認し `Cacheable Read`ます。

```
system node run -node node_name wafl awa start aggr_name
```

5. AWAの概要を表示します。

```
system node run -node node_name wafl awa print aggr_name
```

6. ボリュームのヒット率をと比較します `Cacheable Read`。

   ボリュームのヒット率がよりも高い場合は `Cacheable Read`、SSDにキャッシュされたランダムブロックがワークロードによって再読み取りされません。

7. ボリュームの現在のキャッシュサイズをと比較します `Project Cache Alloc`。

   ボリュームの現在のキャッシュサイズがより大きい場合 `Project Cache Alloc`は、ボリュームのキャッシュサイズが小さすぎます。

関連情報

- "statistics show"
- "statistics start"

ONTAP Flash Poolローカル階層のキャッシングポリシーを変更する

ボリュームのキャッシングポリシーを変更する必要があるのは、別のキャッシングポリシーを使用するとパフォーマンスが向上すると予想される場合だけです。Flash Poolローカル階層上のボリュームのキャッシングポリシーを変更できます。

開始する前に

キャッシングポリシーを変更するかどうかを決定する必要があります。

タスクの内容

ほとんどの場合、使用できるキャッシングポリシーはのデフォルトのキャッシングポリシー `auto`です。キャッシングポリシーを変更する必要があるのは、別のポリシーでワークロードのパフォーマンスが向上する場合だけです。誤ったキャッシングポリシーを設定すると、ボリュームのパフォーマンスが大幅に低下し、時間が経つにつれてパフォーマンスの低下が徐 々 に増大する可能性があります。キャッシングポリシーを変更する場合は注意が必要です。キャッシングポリシーを変更したボリュームでパフォーマンスに問題が発生した場合は、キャッシングポリシーをに戻す必要があります `auto`。

ステップ

1. CLIを使用してボリュームのキャッシングポリシーを変更してください。

```
volume modify -volume volume_name -caching-policy policy_name
```

例

次の例は、という名前のボリュームのキャッシングポリシーをポリシーに `none`変更します `vol2`。

```
volume modify -volume vol2 -caching-policy none
```

ONTAP Flash Poolローカル階層のキャッシュ保持ポリシーを設定する

Flash Poolローカル階層内のボリュームにキャッシュ保持ポリシーを割り当てることができます。キャッシュ保持ポリシーが「high」のボリューム内のデータは長くキャッシュに残り、キャッシュ保持ポリシーが「low」のボリューム内のデータはすぐに削除されます。これにより、優先度の高い情報に長期にわたって高速アクセスできるようにすることで、重要なワークロードのパフォーマンスが向上します。

開始する前に

キャッシュ保持ポリシーがデータをキャッシュに保持する期間に影響を与えないような状況がシステムにあるかどうかを確認しておく必要があります。

手順

CLIをadvanced権限モードで使用して、次の手順を実行します。

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. ボリュームのキャッシュ保持ポリシーを確認します。

   デフォルトでは'キャッシュ保持ポリシーは"normal"です

3. キャッシュ保持ポリシーを設定します。

   ```
   volume modify -volume volume_name -vserver vserver_name -caching-policy
   policy_name
   ```

4. ボリュームのキャッシュ保持ポリシーが選択したオプションに変更されたことを確認します。
5. 権限の設定をadminに戻します。

   ```
   set -privilege admin
   ```

ストレージプールを使用するONTAP Flash Poolローカル階層用のFlash Pool SSDパーティショニング

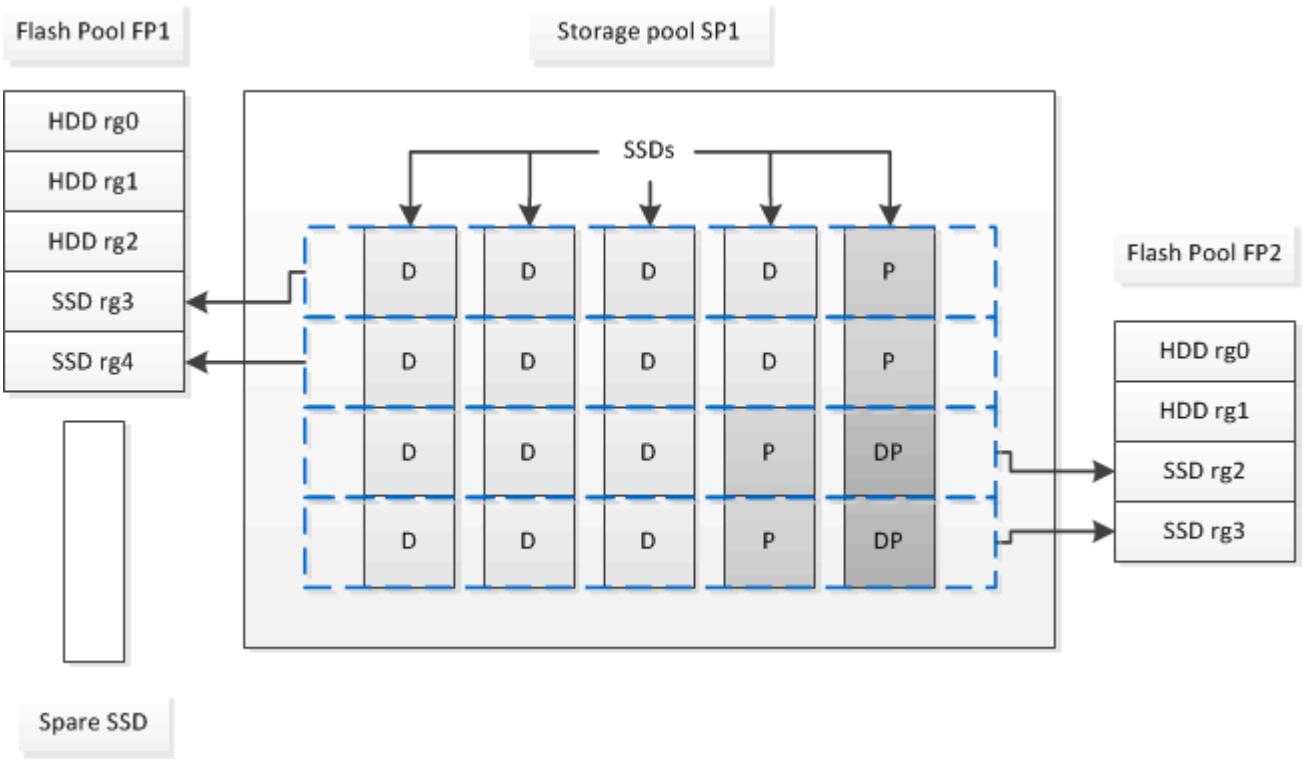
複数のFlash Poolローカル階層にキャッシュを提供する場合は、Flash Poolソリッドステートドライブ（SSD）パーティショニングを使用します。Flash Pool SSDパーティショニングを使用すると、Flash Poolを使用するすべてのローカル階層でSSDを共有できます。これにより、パリティのコストを複数のローカル階層に分散させ、SSDキャッシュ割り当ての柔軟性を高めるとともに、SSDのパフォーマンスを最大限に高めることができます。

Flash Poolローカル階層で使用するSSDは、ストレージプールに配置する必要があります。ストレージプールでは、ルート/データパーティショニング用にパーティショニングされたSSDは使用できません。ストレージプールに配置したSSDは、スタンドアロンディスクとして管理できなくなります。また、Flash Poolに関連付けられているローカル階層を削除してストレージプールを削除しないかぎり、ストレージプールから削除することはできません。

SSDストレージプールは4つの割り当て単位に均等に分割されます。ストレージプールに追加されるSSDは4つのパーティションに分割され、1つのパーティションが4つの割り当て単位のそれぞれに割り当てられます。ストレージプール内のSSDは同じHAペアに所有されている必要があります。デフォルトでは、HAペアの各ノードに2つの割り当て単位が割り当てられます。割り当て単位は、割り当て先のローカル階層を所有するノードが所有している必要があります。いずれかのノードのローカル階層でさらにFlash Cacheが必要な場合は、デフォルトの割り当て単位数を変更して、一方のノードの割り当て単位数を減らしてパートナーノードの割り当て単位数を増やすことができます。

スペアSSDを使用してSSDストレージプールに追加します。HAペアの両方のノードが所有するFlash Poolローカル階層にストレージプールが割り当て単位を提供する場合は、どちらのノードでもスペアSSDを所有できます。ただし、HAペアの一方のノードが所有するFlash Poolローカル階層にのみストレージプールが割り当て単位を提供する場合は、その同じノードがSSDスペアを所有する必要があります。

次の図は、Flash Pool SSDパーティショニングの例を示しています。SSDストレージプールは、2つのFlash Poolローカル階層にキャッシュを提供します。



ストレージプールSP1は、5本のSSDと1本のホットスペアSSDで構成されます。ストレージプールの割り当て単位のうち2つがFlash Pool FP1に割り当てられ、2つがFlash Pool FP2に割り当てられます。FP1のキャッシュRAIDタイプはRAID 4です。したがって、FP1に提供された割り当て単位には、パリティ用に指定されたパーティションが1つだけ含まれます。FP2のキャッシュのRAIDタイプはRAID-DPです。したがって、FP2に提供される割り当て単位には、パリティパーティションとダブルパリティパーティションが含まれます。

この例では、2つの割り当て単位が各Flash Poolローカル階層に割り当てられます。ただし、1つのFlash Poolローカル階層により大きなキャッシュが必要な場合、そのFlash Poolローカル階層に3つの割り当て単位を割り当て、他のローカル階層には1つだけ割り当てることができます。

ONTAP Flash Poolの候補と最適なキャッシュサイズを確認する

既存のローカル階層をFlash Poolローカル階層に変換する前に、ローカル階層がI/Oバウンドであるかどうか、およびワークロードと予算に応じた最適なFlash Poolキャッシュ

サイズを確認できます。また、既存のFlash Poolローカル階層のキャッシュのサイズが正しく設定されているかどうかを確認することもできます。

> ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

開始する前に

分析しているローカル階層の負荷がピークに達したおよその時間を把握しておく必要があります。

手順

1. advancedモードに切り替えます。

   ```
   set advanced
   ```

2. 既存のローカル階層がFlash Poolローカル階層への変換に適しているかどうかを確認する必要がある場合は、負荷のピーク時におけるローカル階層内のディスクのビジー率と、それがレイテンシにどのような影響を及ぼしているかを確認します。

   ```
   statistics show-periodic -object disk:raid_group -instance raid_group_name
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

   Flash Poolキャッシュを追加してレイテンシを削減することがこのローカル階層に適しているかどうかを判断できます。

   次のコマンドは、ローカル階層「aggr1」の最初のRAIDグループの統計を表示します。

   ```
   statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

3. Automated Workload Analyzer（AWA）を起動します。

   ```
   storage automated-working-set-analyzer start -node node_name -aggregate
   aggr_name
   ```

   指定したローカル階層に関連付けられているボリュームのワークロードデータの収集が開始されます。

4. advancedモードを終了します。

   ```
   set admin
   ```

   ピーク負荷が1つ以上の間隔で発生するまで、AWAの実行を許可します。AWAは、指定したローカル階層に関連付けられているボリュームのワークロードの統計情報を収集し、期間内で最大1週間にわたってデータを分析します。AWAを複数の週にわたって実行すると、直近の週から収集されたデータのみがレポートされます。キャッシュサイズの見積もりは、データ収集期間中に確認された最も高い負荷に基づいています。データ収集期間全体で負荷が高くなる必要はありません。

5. advancedモードに切り替えます。

   ```
   set advanced
   ```

6. ワークロードの分析を表示します。

   ```
   storage automated-working-set-analyzer show -node node_name -instance
   ```

7. AWAを停止します。

   ```
   storage automated-working-set-analyzer stop node_name
   ```

   すべてのワークロードデータがフラッシュされ、分析に使用できなくなります。

8. advancedモードを終了します。

   ```
   set admin
   ```

関連情報

- "statistics show-periodic"
- "ストレージ自動ワーキングセットアナライザーの表示"
- "ストレージ自動ワーキングセットアナライザーの開始"
- "ストレージ自動ワーキングセットアナライザーの停止"

物理SSDを使用してONTAP Flash Poolローカル階層を作成する

Flash Poolローカル階層を作成するには、HDD RAIDグループで構成された既存のローカル階層で該当する機能を有効にし、そのローカル階層に1つ以上のSSD RAIDグループを追加します。そのローカル階層には、SSD RAIDグループ（SSDキャッシュ）とHDD RAIDグループの2セットのRAIDグループが作成されます。

> ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

タスクの内容

ローカル階層にSSDキャッシュを追加してFlash Poolローカル階層を作成したあとで、SSDキャッシュを削除してローカル階層を元の構成に戻すことはできません。

デフォルトでは、SSDキャッシュのRAIDレベルは、HDD RAIDグループのRAIDレベルと同じです。このデフォルトの設定は、最初のSSD RAIDグループを追加するときにオプションを指定することで変更できます `raidtype`。

開始する前に

- Flash Poolローカル階層に変換する、HDDで構成された有効なローカル階層を特定しておく必要があります。
- ローカル階層に関連付けられたボリュームが書き込みキャッシュに対応しているかどうかを確認し、対応していない場合は必要な手順を実行して問題を解決しておく必要があります。
- 追加するSSDを決めておく必要があります。これらのSSDはFlash Poolローカル階層の作成先となるノードが所有している必要があります。

- 追加するSSDとローカル階層内の既存のHDDの両方について、チェックサム方式を確認しておく必要があります。
- 追加するSSDの数を決め、SSD RAIDグループに最適なRAIDグループ サイズを確認しておく必要があります。

  SSDキャッシュ内で使用するRAIDグループが少ないほど、必要なパリティ ディスク数が少なくなりますが、RAIDグループを拡張するとRAID-DPが必要になります。

- SSDキャッシュで使用するRAIDレベルを決めておく必要があります。
- システムの最大キャッシュ サイズを決めて、ローカル階層にSSDキャッシュを追加してもそのサイズを超えないことを確認しておく必要があります。
- Flash Poolローカル階層の構成要件を確認しておく必要があります。

手順

System ManagerまたはONTAP CLIを使用して、Flash Poolのローカル階層を作成できます。

System Manager

ONTAP 9.12.1以降では、System Managerを使用して、物理SSDを使用するFlash Poolローカル階層を作成できます。

手順

1. [ストレージ]>[階層]*を選択し、既存のローカルHDDストレージ階層を選択します。
2. 次に、*[Flash Poolキャッシュの追加]*を選択します ⋮ 。
3. [*キャッシュとして専用**SSD**を使用する]を選択します。
4. ディスクタイプとディスク数を選択します。
5. RAIDタイプを選択します。
6. [保存（ Save ）] を選択します。
7. ストレージ層を見つけて選択する⋮
8. [詳細]*を選択します。Flash Poolが「enabled」*と表示されていることを確認します。

CLI

手順

1. ローカル階層をFlash Poolローカル階層の対象としてマークします。

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   この手順が失敗した場合は、ターゲットのローカル階層が書き込みキャッシュに対応しているかどうかを確認します。

2. コマンドを使用して、ローカル階層にSSDを追加し `storage aggregate add`ます。
   - SSDは、IDまたはパラメータと `disktype`パラメータを使用して指定できます `diskcount`。
   - HDDとSSDでチェックサム方式が異なる場合やローカル階層がチェックサムが混在したローカル階層の場合は、パラメータを使用してローカル階層に追加するディスクのチェックサム方式を指定する必要があります `checksumstyle`。
   - SSDキャッシュに別のRAIDタイプを指定するには、パラメータを使用し `raidtype`ます。
   - キャッシュRAIDグループサイズを使用するRAIDタイプのデフォルトと異なるサイズにする場合は、パラメータを使用してこの時点で変更する必要があります `-cache-raid-group-size`。

関連情報

- "ストレージアグリゲートの追加"
- "storage aggregate modify"

SSDストレージプールを使用して**Flash Pool**ローカル階層を作成する

ONTAP Flash Poolローカル階層で**SSD**ストレージプールが使用されているかどうかを確認する

SSDストレージプールから既存のHDDローカル階層に1つ以上の割り当て単位を追加することで、Flash Poolローカル階層を設定できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

SSDストレージプールを使用してキャッシュを提供する場合と、単独のSSDを使用する場合では、Flash Poolローカル階層の管理方法が異なります。

ステップ

1. ローカル階層のドライブをRAIDグループ別に表示します。

   ```
   storage aggregate show-status aggr_name
   ```

   ローカル階層で1つ以上のSSDストレージプールを使用している場合は、SSD RAIDグループの列の値`Position`がと表示され `Shared`、RAIDグループ名の横にストレージプールの名前が表示されます。

関連情報

- "ストレージアグリゲートのステータス表示"

SSDストレージプールを作成して**ONTAP**ローカル階層にキャッシュを追加する

ソリッドステートドライブ（SSD）を追加して既存のローカル階層をFlash Poolローカル階層に変換することで、キャッシュをプロビジョニングできます。

2~4つのFlash Poolローカル階層にSSDキャッシュを提供するためのソリッドステートドライブ（SSD）ストレージプールを作成できます。Flash Poolのローカル階層を使用すると、作業データセットにはフラッシュを導入して高性能なキャッシュを使用しながら、アクセス頻度の低いデータには低コストのHDDを使用することができます。

タスクの内容

- ディスクを作成するとき、またはストレージプールにディスクを追加するときは、ディスクリストを指定する必要があります。

  ストレージプールではパラメータはサポートされません `diskcount`。

- ストレージプールで使用するSSDは同じサイズである必要があります。

System Manager

System Managerを使用して**SSD**キャッシュを追加する（**ONTAP 9 12.1**以降）

ONTAP 9.12.1以降では、System Managerを使用してSSDキャッシュを追加できます。

ストレージプールオプションはAFFシステムでは使用できません。

手順

1. [*Cluster]、[Disks]の順にクリックし、[*Show/Hide *]をクリックします。
2. タイプ*を選択し、スペアSSDがクラスタに存在することを確認します。
3. [ストレージ]、[階層]の順にクリックし、[*ストレージプールの追加]をクリックします。
4. ディスクタイプを選択します。
5. ディスクサイズを入力します。
6. ストレージプールに追加するディスクの数を選択します。
7. 推定キャッシュサイズを確認します。

System Managerを使用して**SSD**キャッシュを追加する（**ONTAP 9 .7**のみ）

ONTAP 9 .7以降またはONTAP 9よりも前のONTAPバージョンを使用している場合は、CLIの手順を使用してください。12.1

手順

1. *（クラシックバージョンに戻る）*をクリックします。
2. ストレージ > アグリゲートとディスク > アグリゲート * をクリックします。
3. ローカル階層を選択し、*[操作]>[キャッシュの追加]*をクリックします。
4. キャッシュソースとして「ストレージプール」または「専用SSD」を選択します。
5. （新しいエクスペリエンスに切り替える） * をクリックします。
6. [ストレージ]>[階層]*をクリックして、新しいローカル階層のサイズを確認します。

CLI

- SSDストレージプールの作成にはCLIを使用*

手順

1. 使用可能なスペアSSDの名前を確認します。

   ```
   storage aggregate show-spare-disks -disk-type SSD
   ```

   ストレージプールで使用されるSSDは、HAペアのどちらのノードでも所有できます。

2. ストレージプールを作成します。

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,…
```

3. * オプション： * 新しく作成したストレージ・プールを検証します。

```
storage pool show -storage-pool sp_name
```

結果

ストレージプールが提供するストレージがまだFlash Poolキャッシュに割り当てられていなくても、ストレージプールに配置されたSSDはクラスタ上でスペアとして表示されなくなります。SSDを単独のドライブとしてRAIDグループに追加することはできません。ストレージをプロビジョニングできるのは、SSDが属しているストレージプールの割り当て単位を使用する場合のみです。

関連情報

- "storage aggregate show"
- "ストレージプールの作成"
- "ストレージプールショー"

SSDストレージプールの割り当て単位を使用して**ONTAP Flash Pool**ローカル階層を作成する

SSDストレージプールから既存のHDDローカル階層に1つ以上の割り当て単位を追加することで、Flash Poolローカル階層を設定できます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

12.1以降では、再設計されたSystem Managerを使用して、ストレージプールの割り当て単位を使用してONTAP 9ローカル階層を作成できます。

開始する前に

- Flash Poolローカル階層に変換する、HDDで構成された有効なローカル階層を特定しておく必要があります。
- ローカル階層に関連付けられたボリュームが書き込みキャッシュに対応しているかどうかを確認し、対応していない場合は必要な手順を実行して問題を解決しておく必要があります。
- このFlash Poolローカル階層にSSDキャッシュを提供するSSDストレージプールを作成しておく必要があります。

  使用するストレージプールの割り当て単位は、Flash Poolローカル階層の所有者ノードに所有されている必要があります。

- ローカル階層に追加するキャッシュの容量を決めておく必要があります。

  ローカル階層にキャッシュを追加するには、割り当て単位を使用します。ストレージプールに余裕がある場合は、ストレージプールにSSDを追加することで、割り当て単位のサイズをあとから拡張できます。

- SSDキャッシュに使用するRAIDタイプを決めておく必要があります。

SSDストレージプールからローカル階層にキャッシュを追加したあとに、キャッシュRAIDグループのRAIDタイプを変更することはできません。

- システムの最大キャッシュ サイズを決めて、ローカル階層にSSDキャッシュを追加してもそのサイズを超えないことを確認しておく必要があります。

  合計キャッシュサイズに追加されるキャッシュの量は、コマンドを使用して確認できます `storage pool show`。

- Flash Poolローカル階層の構成要件を確認しておく必要があります。

タスクの内容

キャッシュのRAIDタイプをHDD RAIDグループと異なるタイプにする場合は、SSDの容量を追加するときにキャッシュのRAIDタイプを指定する必要があります。ローカル階層にSSDの容量を追加したあとで、キャッシュのRAIDタイプを変更することはできません。

ローカル階層にSSDキャッシュを追加してFlash Poolローカル階層を作成したあとで、SSDキャッシュを削除してローカル階層を元の構成に戻すことはできません。

System Manager

ONTAP 9 12.1以降では、System Managerを使用してSSDストレージプールにSSDを追加できます。

手順

1. [ストレージ>階層]をクリックし、既存のローカルHDDストレージ階層を選択します。
2. をクリック し、*[Flash Poolキャッシュの追加]*を選択します。
3. ［ストレージプールを使用する］を選択します。
4. ストレージプールを選択します。
5. キャッシュサイズとRAID構成を選択します。
6. [保存（ Save ）] をクリックします。
7. ストレージ層を再度見つけてクリックします
8. 「* More Details」を選択し、Flash Poolの表示が「* Enabled」になっていることを確認します。

CLI

手順

1. ローカル階層をFlash Poolローカル階層の対象としてマークします。

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   この手順が失敗した場合は、ターゲットのローカル階層が書き込みキャッシュに対応しているかどうかを確認します。

2. 使用可能なSSDストレージプールの割り当て単位を表示します。

   ```
   storage pool show-available-capacity
   ```

3. ローカル階層にSSDの容量を追加します。

   ```
   storage aggregate add aggr_name -storage-pool sp_name -allocation-units
   number_of_units
   ```

   キャッシュのRAIDタイプをHDD RAIDグループと異なるタイプにする場合は、このコマンドの入力時にパラメータを使用して変更する必要があります `raidtype`。

   新しいRAIDグループを指定する必要はありません。ONTAPでは、HDD RAIDグループとは別のRAIDグループにSSDキャッシュが自動的に配置されます。

   キャッシュのRAIDグループサイズは設定できません。このサイズは、ストレージプール内のSSDの数によって決まります。

   キャッシュがローカル階層に追加され、ローカル階層がFlash Poolローカル階層になります。ローカル階層に追加された各割り当て単位は、それぞれ独自のRAIDグループになります。

4. SSDキャッシュが存在することとサイズを確認します。

   ```
   storage aggregate show aggregate_name
   ```

キャッシュのサイズは、に表示され `Total Hybrid Cache Size`ます。

関連情報

- "NetAppテクニカルレポート4070：『Flash Pool Design and Implementation Guide』"
- "ストレージアグリゲートの追加"
- "storage aggregate modify"
- "ストレージプールショー"
- "ストレージプールの利用可能な容量の表示"

SSDストレージプールに**SSD**が追加された場合の**ONTAP**キャッシュサイズへの影響の判定

ストレージプールにSSDを追加するとプラットフォームモデルのキャッシュ制限を超えてしまう場合、ONTAPは新しく追加した容量をどのFlash Poolローカル階層にも割り当てません。その結果、新しく追加した容量の一部またはすべてを使用できなくなる可能性があります。

タスクの内容

割り当て単位がFlash Poolローカル階層にすでに割り当てられているSSDストレージプールにSSDを追加すると、それらの各ローカル階層のキャッシュサイズとシステムの合計キャッシュサイズが拡張されます。ストレージプールの割り当て単位がどれも割り当てられていない場合、そのストレージプールにSSDを追加しても、1つ以上の割り当て単位がキャッシュに割り当てられるまでSSDのキャッシュサイズには影響しません。

手順

1. ストレージプールに追加するSSDの使用可能なサイズを確認します。

   ```
   storage disk show disk_name -fields usable-size
   ```

2. ストレージプールの未割り当ての割り当て単位の数を確認します。

   ```
   storage pool show-available-capacity sp_name
   ```

   ストレージプール内の未割り当ての割り当て単位がすべて表示されます。

3. 次の式を使用して、追加するキャッシュの容量を計算します。

   （4 -未割り当ての割り当て単位の数）×25%×使用可能なサイズ×SSDの数

関連情報

- "storage disk show"
- "ストレージプールの利用可能な容量の表示"

ONTAP SSDストレージプールへの**SSD**の追加

SSDストレージプールにソリッドステートドライブ（SSD）を追加すると、ストレージプールの物理サイズと使用可能なサイズ、および割り当て単位のサイズが拡張されます。割り当て単位のサイズが大きいほど、ローカル階層にすでに割り当てられている割

り当て単位にも影響します。

開始する前に

この処理を実行してもHAペアのキャッシュ制限を超えないことを確認しておく必要があります。ONTAPでは、SSDストレージプールへのSSDの追加時にキャッシュ制限を超えてもかまいません。その場合、新しく追加したストレージ容量が使用できなくなる可能性があります。

タスクの内容

既存のSSDストレージプールにSSDを追加する場合は、ストレージプール内の既存のSSDを所有しているノードと同じHAペアのどちらかのノードが所有しているSSDを追加する必要があります。HAペアのどちらのノードが所有するSSDも追加できます。

ストレージプールに追加するSSDは、ストレージプールで現在使用されているディスクと同じサイズである必要があります。

System Manager

ONTAP 9 12.1以降では、System Managerを使用してSSDストレージプールにSSDを追加できます。

手順

1. [ストレージ>階層]をクリックし、[ストレージプール]セクションを探します。
2. ストレージプールを探してをクリックし、*[ディスクの追加]*を選択します。
3. ディスクタイプを選択し、ディスク数を選択します。
4. 概算キャッシュサイズを確認します。

CLI

手順

1. * オプション：ストレージプールの現在の割り当て単位のサイズと使用可能なストレージを表示します。

   ```
   storage pool show -instance sp_name
   ```

2. 使用可能なSSDを探します。

   ```
   storage disk show -container-type spare -type SSD
   ```

3. ストレージプールにSSDを追加します。

   ```
   storage pool add -storage-pool sp_name -disk-list disk1,disk2…
   ```

   この処理によってどのFlash Poolローカル階層のサイズがどのくらい拡張されるかが表示され、処理を確認するように求められます。

関連情報

- "storage disk show"
- "ストレージプールショー"
- "ストレージプールの追加"

ONTAPには、SSDストレージプールを管理するためのコマンドが用意されて `storage pool`います。

状況	使用するコマンド
ストレージプールがローカル階層に提供しているストレージの容量を表示する	`storage pool show-aggregate`
両方のRAIDタイプ（割り当て単位のデータサイズ）の全体的なキャッシュ容量に追加されるキャッシュの量を表示する	`storage pool show -instance`
ストレージプール内のディスクを表示する	`storage pool show-disks`
ストレージプールの未割り当ての割り当て単位を表示する	`storage pool show-available-capacity`
ストレージプールの1つ以上の割り当て単位の所有権をHAパートナーから別のHAパートナーに変更する	`storage pool reassign`

関連情報

- "ストレージプールの再割り当て"
- "ストレージプールショー"
- "ストレージプールの集計を表示"
- "ストレージプールの利用可能な容量の表示"
- "ストレージプールのディスク表示"

FabricPool階層の管理

ONTAP FabricPoolによるデータ階層化の詳細

FabricPoolを使用すると、データのアクセス頻度に応じてデータを自動的に階層化できます。

FabricPoolは、AFFシステムではオールフラッシュ（オールSSD）アグリゲートを使用し、FASシステムではオールフラッシュ（オールSSD）アグリゲートまたはHDDアグリゲートをパフォーマンス階層として、オブジェクトストアをクラウド階層として使用するハイブリッドストレージソリューションです。FabricPoolを使用すると、パフォーマンス、効率、保護を犠牲にすることなくストレージコストを削減できます。

クラウド階層は、NetApp StorageGRIDまたはONTAP S3（ONTAP 9 .8以降）、または次のいずれかのサービスプロバイダに配置できます。

- アリババクラウド

- Amazon S3
- Amazon Commercial Cloud Services
- Google Cloud
- IBMクラウド
- Microsoft Azure Blob Storage

ONTAP 9.7以降では、S3_Compatibleオブジェクト ストア プロバイダを選択することで、汎用のS3 APIをサポートする追加のオブジェクト ストア プロバイダを使用できます。

関連情報

- "NetAppクラウド階層化ドキュメント"

ONTAP FabricPoolの使用要件

FabricPool構成を最適化するには、FabricPoolの使用に関するいくつかの考慮事項と要件を理解しておく必要があります。

一般的な考慮事項と要件

ONTAP 9.4

- FabricPoolの次の機能を使用するには、ONTAP 9.4以降のリリースが必要です。
  - の `auto`"階層化ポリシー"
  - 階層化の最小クーリング期間の指定
  - Inactive Data Reporting（IDR）
  - FabricPoolのクラウド階層としてのクラウド用Microsoft Azure Blob Storageの使用
  - ONTAP SelectでのFabricPoolの使用

ONTAP 9.5

- FabricPoolの次の機能を使用するには、ONTAP 9.5以降のリリースが必要です。
  - 階層化のスペース不足しきい値の指定
  - FabricPoolのクラウド階層としてのIBM Cloud Object Storageの使用
  - クラウド階層のNetApp Volume Encryption（NVE）。デフォルトで有効になります。

ONTAP 9.6

- FabricPoolの次の機能を使用するには、ONTAP 9.6以降のリリースが必要です。
  - `all`階層化ポリシー
  - HDDアグリゲートについてのInactive Data Reportingを手動で有効化
  - ONTAP 9 .6にアップグレードすると、アグリゲートの作成時にSSDアグリゲートについてのInactive Data Reportingが自動的に有効になります。ただし、CPUが4個未満、RAMが6GB未満のローエンドシステム、またはWAFLバッファキャッシュサイズが3GB未満のシステムは例外です。

ONTAPはシステムの負荷を監視します。負荷が高い状態が4分間続くと、IDRは無効になり、自動的には有効になりません。IDRを手動で再度有効にすることはできますが、手動で有効にしたIDRは自動的には無効になりません。

- FabricPoolのクラウド階層としてのAlibaba Cloud Object Storageの使用
- FabricPoolのクラウド階層としてのGoogle Cloud Platformの使用
- クラウド階層のデータコピーを使用しないボリューム移動

ONTAP 9.7

- FabricPoolの次の機能を使用するには、ONTAP 9.7以降のリリースが必要です。
  - 非透過型HTTPおよびHTTPSプロキシ：ホワイトリストに登録されたアクセスポイントのみにアクセスを提供し、監査およびレポート機能を提供します。
  - FabricPoolミラーリングによるコールドデータの2つのオブジェクトストアへの同時階層化
  - MetroClusterコウセイノFabricPoolミラア
  - FabricPoolに接続されたアグリゲートでNDMPダンプおよびリストアがデフォルトで有効になります。

> バックアップアプリケーションでNDMP以外のプロトコル（NFSやSMBなど）を使用すると、高パフォーマンス階層にバックアップされているすべてのデータがホットになり、そのデータのクラウド階層への階層化に影響する可能性があります。NDMP以外の読み取りでは、クラウド階層から高パフォーマンス階層にデータが戻される可能性があります。

"FabricPoolでのNDMPバックアップおよびリストアのサポート"

ONTAP 9.8

- 次のFabricPool機能を使用するには、ONTAP 9 .8以降が実行されている必要があります。
  - クラウド読み出し
  - FabricPool with SnapLock Enterprise.SnapLock Enterpriseを搭載したFabricPoolには、Feature Product Variance Request（FPVR）が必要です。FPVRを作成するには、営業チームにお問い合わせください。
  - 最小クーリング期間（最大183日）
  - ユーザ作成のカスタムタグを使用したオブジェクトのタグ付け
  - HDD FabricPoolアグリゲート

    HDD FabricPoolは、CPUコアを6つ以上搭載したシステムでのみ、SAS、FSAS、BSAS、MSATAディスクでサポートされます。

サポートされている最新モデルを確認します "Hardware Universe"。

ONTAP 9 10.1

- FabricPoolの次の機能を使用するには、ONTAP 9 .10.1以降が実行されている必要があります。

- PUTスロットル
- 温度識別型Storage Efficiency（TSSE）。

ONTAP 9 12.1

- 次のFabricPool機能を使用するには、ONTAP 9.12.1以降が実行されている必要があります。
  - SVMの移行
  - FabricPool、FlexGroup、SVM-DRの連携がサポートされます。（9.12.1より前のバージョンでは、これらの機能のいずれか2つが連携して動作しましたが、3つすべてが連携して動作するわけではありません）

ONTAP 9 .14.1

- FabricPoolの次の機能を使用するには、ONTAP 9.14.1以降が実行されている必要があります。
  - クラウド書き込み
  - 積極的な先読み

ローカル階層（アグリゲート）

FabricPoolでは、次のアグリゲートタイプがサポートされます。

- AFFシステムでは、FabricPoolにSSDアグリゲートのみを使用できます。
- FASシステムでは、FabricPoolにSSDアグリゲートまたはHDDアグリゲートのいずれかを使用できます。
- Cloud Volumes ONTAP および ONTAP Select では、 FabricPool に SSD アグリゲートまたは HDD アグリゲートのいずれかを使用できます。SSDアグリゲートを使用することを推奨します。

SSDとHDDの両方を含むFlash Poolアグリゲートはサポートされていません。

クラウド階層

FabricPoolでは、次のオブジェクトストアをクラウド階層として使用できます。

- Alibaba Cloud Object Storage Service（標準、低頻度アクセス）
- Amazon S3（Standard、Standard-IA、One Zone-IA、Intelligent-Tiering、Glacier Instant Retrieval）
- Amazon Commercial Cloud Services（C2S）
- Google Cloud Storage（マルチリージョナル、リージョナル、ニアライン、コールドライン、アーカイブ）
- IBM Cloud Object Storage（Standard、Vault、Cold Vault、Flex）
- Microsoft Azure Blob Storage（ホットおよびクール）
- NetApp ONTAP S3 （ ONTAP 9.8 以降）
- NetApp StorageGRID（StorageGRID 10.3以降）

Glacier Flexible RetrievalとGlacier Deep Archiveはサポートされていません。

- 使用するオブジェクトストア “bucket” (コンテナ) はすでに設定されている必要がありますまた ' 少なくとも 10 GB のストレージスペースが必要であり ' 名前を変更することはできません
- 接続後にローカル階層からクラウド階層の接続を解除することはできませんが、を使用してローカル階層を別のクラウド階層に接続することもできます"FabricPoolミラー"。

クラスタ間**LIF**

FabricPoolを使用するクラスタの高可用性（HA）ペアでは、クラウド階層と通信するために2つのクラスタ間LIFが必要です。NetAppでは、追加のHAペアでクラスタ間LIFを作成して、それらのノードのローカル階層にもクラウド階層をシームレスに接続することを推奨しています。

クラスタ間LIFを無効にするか削除すると、クラウド階層への通信が中断されます。

> SnapMirrorとSnapVaultの同時レプリケーション処理は、クラウド階層へのネットワーク リンクを共有するため、初期化とRTOはクラウド階層で利用可能な帯域幅とレイテンシに依存します。接続リソースが飽和状態になると、パフォーマンスが低下する可能性があります。複数のLIFを事前設定すると、このようなネットワークの飽和を大幅に減らすことができます。

ルーティングが異なるノードで複数のクラスタ間LIFを使用している場合はNetApp、異なるIPspaceに配置することを推奨します。設定時にFabricPoolは複数のIPspaceから選択できますが、IPspace内の特定のクラスタ間LIFを選択することはできません。

ネットワーク タイム プロトコル（**NTP**）

クラスター間で時刻が同期されるようにするには、ネットワーク タイム プロトコル (NTP) 構成が必要です。"NTPの設定方法について学ぶ" 。

ONTAP の **Storage Efficiency** 機能

データをクラウド階層に移動する際に圧縮、重複排除、コンパクションなどのStorage Efficiencyが維持されるため、必要なオブジェクトストレージ容量と転送コストを削減できます。

> ONTAP 9.15.1以降では、FabricPoolはインテルQuickAssistテクノロジー（QAT4）をサポートしています。これにより、より積極的でパフォーマンスの高いストレージ効率を実現できます。

アグリゲートインライン重複排除はローカル階層でサポートされますが、関連するStorage Efficiencyはクラウド階層に格納されているオブジェクトに引き継がれません。

「すべて」のボリューム階層化ポリシーを使用している場合、追加のストレージ効率化を適用する前にデータが階層化される可能性があるため、バックグラウンドの重複排除プロセスに関連するStorage Efficiencyが低下することがあります。

NetAppクラウド階層化ライセンス

FabricPool、サードパーティのオブジェクト ストレージ プロバイダー (Amazon S3 など) をAFFおよびFASシステムのクラウド層として接続する場合、容量ベースのライセンスが必要です。クラウド階層としてStorageGRIDまたはONTAP S3 を使用する場合、またはCloud Volumes ONTAP、 Amazon FSx for NetApp ONTAP、または Azure NetAppファイルを使用して階層化する場合は、クラウド階層化ライセンスは必要ありません。

NetApp Cloud Tiering ライセンス (既存のFabricPoolライセンスへのアドオンまたは拡張機能を含む) は、NetAppコンソールでアクティブ化されます。詳細はこちら"クラウド階層化ライセンスの設定"。

StorageGRID整合性制御

StorageGRIDの整合性制御は、StorageGRIDがオブジェクトの追跡に使用するメタデータがノード間でどのように分散されるか、およびクライアント要求に対するオブジェクトの可用性に影響します。NetAppでは、FabricPoolターゲットとして使用するバケットには、デフォルトのread-after-new-write整合性制御を使用することを推奨しています。

FabricPoolターゲットとして使用するバケットにはAvailable整合性制御を使用しないでください。

SANプロトコルでアクセスするデータの階層化に関するその他の考慮事項

SANプロトコルでアクセスされるデータを階層化する場合、接続に関する考慮事項があるため、NetAppではONTAP S3やStorageGRIDなどのプライベートクラウドを使用することを推奨しています。

WindowsホストがあるSAN環境でFabricPoolを使用する場合は、データをクラウドに階層化する際にオブジェクト ストレージを長時間にわたって使用できなくなると、Windowsホスト上のNetApp LUNのファイルがアクセスできなくなったり、表示されなくなったりすることがあります。参照"NetAppナレッジベース: FabricPool S3 オブジェクト ストアが利用できないときに Windows SAN ホストがファイルシステムの破損を報告しました"。

サービス品質（**QoS**）

- スループットの下限（最小QoS）を使用する場合は、アグリゲートをFabricPoolに接続する前に、ボリュームの階層化ポリシーをに設定する必要があります `none`。

  それ以外の階層化ポリシーでは、アグリゲートをFabricPoolに接続できません。FabricPoolが有効な場合、QoSポリシーではスループットの下限は適用されません。

FabricPoolでサポートされない機能

- WORMとオブジェクトのバージョン管理が有効になっているオブジェクトストア。
- オブジェクトストアバケットに適用される情報ライフサイクル管理（ILM）ポリシー

  FabricPoolは、クラウド階層のデータを障害から保護するために、データレプリケーションとイレイジャーコーディングについてのみ、StorageGRIDの情報ライフサイクル管理ポリシーをサポートしています。ただし、FabricPoolは、ユーザメタデータやタグに基づくフィルタリングなどの高度なILMルールをサポートしていません。ILMには通常、移動や削除に関するさまざまなポリシーが含まれています。これらのポリシーは、FabricPoolのクラウド階層内のデータに影響を与える可能性があります。オブジェクトストアで設定されているILMポリシーとFabricPoolを併用すると、データが失われる可能性があります。

- ONTAP CLIコマンドまたは7-Mode Transition Toolを使用した7-Modeデータの移行
- RAID SyncMirror（MetroCluster構成を除く）
- SnapLockボリューム（ONTAP 9 .7以前のリリースを使用している場合）
- "スナップショットの改ざん防止"

改ざん防止スナップショットは、削除できない改ざん防止機能を提供します。FabricPoolではデータを削除する機能が必要なため、同じボリュームでFabricPoolロックとSnapshotロックを有効にすることはできません。

- FabricPool対応アグリゲートに対するSMTapeを使用したテープバックアップ
- 自動負荷分散機能
- 以外のスペースギャランティを使用するボリューム `none`

  ルートSVMボリュームとCIFS監査ステージングボリュームを除き、FabricPoolでは、以外のスペースギャランティを使用するボリュームを含むアグリゲートにクラウド階層を接続することはサポートされていません `none`。たとえば、スペースギャランティがのボリュームは `volume` (`-space-guarantee` `volume`サポートされません。

- クラスタ"DP_Optimizedライセンス"
- Flash Poolアグリゲート

ONTAP FabricPoolポリシーによるデータの効率的な階層化

FabricPool階層化ポリシーを使用すると、データがホットまたはコールドになったときに階層間でデータを効率的に移動できます。階層化ポリシーについて理解しておくと、ストレージ管理のニーズに適したポリシーを選択するのに役立ちます。

FabricPool階層化ポリシーの種類

FabricPool 階層化ポリシーは、 FabricPool 内のボリュームのユーザデータブロックをクラウド階層に移動するタイミングとそのタイミングを、ホット（アクティブ）のボリューム「 temperature 」またはコールド（非アクティブ）に基づいて決定します。ボリューム「温度」は、頻繁にアクセスされると増加し、アクセスされない場合は減少します。一部の階層化ポリシーには、階層化の最小クーリング期間が関連付けられています。最小クーリング期間は、データが「コールド」とみなされてクラウド階層に移動されるために、 FabricPool のボリューム内のユーザデータが非アクティブのままになる時間を設定します。

ブロックがコールドとして識別されると、階層化の対象としてマークされます。毎日のバックグラウンド階層化スキャンでコールドブロックが検索されます。同じボリュームから十分な4KBブロックが収集されると、それらは4MBオブジェクトに連結され、ボリューム階層化ポリシーに基づいてクラウド階層に移動されます。

> 階層化ポリシーを使用するボリューム内のデータ `all`はすぐにコールドとしてマークされ、できるだけ早くクラウド階層への階層化が開始されます。毎日の階層化スキャンの実行を待つ必要はありません。

FabricPoolボリュームの階層化ステータスは、コマンドを使用して表示できます `volume object-store tiering show`。の詳細については `volume object-store tiering show`、を"ONTAPコマンド リファレンス"参照してください。

FabricPool階層化ポリシーはボリュームレベルで指定します。次の4つのオプションがあります。

- 階層化ポリシー（デフォルト）は `snapshot-only`、アクティブなファイルシステムに関連付けられていないボリュームSnapshotのユーザデータブロックをクラウド階層に移動します。

  階層化の最小クーリング期間は2日です。階層化の最小クーリング期間のデフォルト設定は、advanced権限レベルのパラメータを `volume create`使用して変更できます `-tiering-minimum-cooling-

`days volume modify`。有効な値は、ONTAP 9 .8以降を使用した場合の2183日です。9.8より前のバージョンのONTAPを使用している場合、有効な値は263日です。

- `auto`階層化ポリシーはONTAP 9.4以降のリリースでのみサポートされ、Snapshotとアクティブなファイルシステムの両方のコールドユーザデータブロックをクラウド階層に移動します。

  デフォルトの階層化の最小クーリング期間は31日で、アクティブなファイルシステムとSnapshotの両方についてボリューム全体に適用されます。

  階層化の最小クーリング期間のデフォルト設定は、advanced権限レベルのパラメータを `volume create`使用して変更できます `-tiering-minimum-cooling-days volume modify`。有効な値は2～183日です。

- `all`階層化ポリシー（ONTAP 9.6以降でのみサポート）は、アクティブなファイルシステムとSnapshotの両方のすべてのユーザデータブロックをクラウド階層に移動します。階層化ポリシーに代わる `backup`ものです。

  > `all`クライアントトラフィックが正常な読み取り/書き込みボリュームでは、ボリューム階層化ポリシーを使用しないでください。

  階層化スキャンの実行と同時にデータがクラウド階層に移動するため、階層化の最小クーリング期間は適用されません。この設定は変更できません。

- `none`階層化ポリシーは、ボリュームのデータを高パフォーマンス階層に保持し、コールドデータをクラウド階層に移動しません。

  階層化ポリシーをに設定すると、 `none`新しい階層化が行われなくなります。以前にクラウド階層に移動されたボリュームデータは、ホットになるまでクラウド階層に残り、自動的にローカル階層に戻ります。

  データがクラウド階層に移動されることはないため、階層化の最小クーリング期間は適用されません。この設定は変更できません。

  階層化ポリシーがに設定されているボリューム内のコールドブロックが読み取られると、 `none`それらはホットになり、ローカル階層に書き込まれます。

  > `volume show`
  > コマンド出力には、ボリュームの階層化ポリシーが表示されます。FabricPoolで使用されたことがないボリュームの場合、出力に階層化ポリシーが表示され `none`ます。

> SVM DR関係では、ソースボリュームとデスティネーションボリュームでFabricPoolアグリゲートを使用する必要はありませんが、同じ階層化ポリシーを使用する必要があります。

FabricPoolでボリュームの階層化ポリシーを変更した場合の動作

ボリュームの階層化ポリシーは、を実行することで変更できます `volume modify`。階層化ポリシーを変更することが、データがコールドと認識されてクラウド階層に移動されるまでの時間にどのように影響するかを理解しておく必要があります。

- 階層化ポリシーをまたは `none`に `auto`変更する `snapshot-only`と、アクティブなファイルシステムのすでにコールドなユーザデータブロックがONTAPからクラウド階層に送信されます。これは、それらのユーザデータブロックが以前はクラウド階層に送信されなかった場合でも同様です。
- 階層化ポリシーを別のポリシーからに変更する `all`と、ONTAPはアクティブなファイルシステムとSnapshot内のすべてのユーザブロックをできるだけ早くクラウドに移動します。ONTAP 9.8より前のバージョンでは、次の階層化スキャンが実行されるまでブロックが待機する必要がありました。

  移動されたブロックを高パフォーマンス階層に戻すことはできません。

- 階層化ポリシーをからまたはに `snapshot-only`変更して `auto`も、 `none`すでにクラウド階層に移動されたアクティブなファイルシステムブロックはパフォーマンス階層に戻されません。

  ボリュームの読み取りは、データを高パフォーマンス階層に戻すために必要です。

- ボリュームの階層化ポリシーを変更すると、階層化の最小クーリング期間は常にそのポリシーのデフォルト値にリセットされます。

ボリュームを移動した場合の階層化ポリシーへの影響

- ボリュームを対応アグリゲートに移動したりFabricPool対応アグリゲートから移動したりする際に、別の階層化ポリシーを明示的に指定しないかぎり、ボリュームの階層化ポリシーは元のままです。

  ただし、階層化ポリシーが有効になるのは、ボリュームがFabricPool対応アグリゲートに含まれている場合のみです。

- ボリュームのパラメータの既存の値は `-tiering-minimum-cooling-days`、デスティネーションに別の階層化ポリシーを指定しないかぎり、ボリュームとともに移動されます。

  別の階層化ポリシーを指定した場合は、そのポリシーのデフォルトの階層化の最小クーリング期間が使用されます。デスティネーションがFabricPoolかどうかは関係ありません。

- アグリゲート間でボリュームを移動し、同時に階層化ポリシーも変更できます。
- 処理に階層化ポリシーが関係する `auto`場合は、特に注意が必要です `volume move`。

  次の表に、ソースとデスティネーションの両方がFabricPool対応アグリゲートである場合の、に関するポリシーの変更を実行した処理 `auto`の結果を示し `volume move`ます。

ボリュームの階層化ポリシー	移動時に設定する階層化ポリシー	ボリューム移動後の結果
`all`	`auto`	すべてのデータが高パフォーマンス階層に移動されます。
`snapshot-only`、 `none`、または `auto`	`auto`	データブロックは、ソースと同じデスティネーションの階層に移動されます。
`auto`または `all`	`snapshot-only`	すべてのデータが高パフォーマンス階層に移動されます。

auto	all	すべてのユーザデータがクラウド階層に移動されます。
snapshot-only,auto`または `all	none	すべてのデータが高パフォーマンス階層に保持されます。

ボリュームをクローニングした場合の階層化ポリシーへの影響

- ONTAP 9.8以降、クローン ボリュームは常に階層化ポリシーとクラウド読み出しポリシーの両方を親ボリュームから継承します。

  ONTAP 9 .8より前のリリースでは、親に階層化ポリシーが設定されている場合を除き、クローンは親から階層化ポリシーを継承します。 all

- 親ボリュームにクラウド読み出しポリシーが設定されている場合、 never`クローンボリュームにはクラウド読み出しポリシーまたは `all`階層化ポリシーと、対応するクラウド読み出しポリシーが `default`設定されている必要があります `never。
- 親ボリュームのクラウド読み出しポリシーをに変更する `never`には、クローンボリュームにクラウド読み出しポリシーがすべて設定され `never`ている必要があります。

ボリュームをクローニングするときは、次のベストプラクティスに注意してください。

- `-tiering-policy`クローンのオプションと `tiering-minimum-cooling-days`オプションは、クローンに固有のブロックの階層化動作のみを制御します。そのため、親FlexVolでは、どのクローンよりも同じ量または少ない量のデータしか移動しない階層化設定を使用することを推奨します。
- 親FlexVolのクラウド読み出しポリシーでは、すべてのクローンの読み出しポリシーと同じ量かそれよりも多くのデータを移動する必要があります。

階層化ポリシーとクラウド移行との相互運用性

FabricPoolのクラウドデータ読み出しは階層化ポリシーで制御されます。階層化ポリシーは、読み取りパターンに基づいてクラウド階層から高パフォーマンス階層へのデータの読み出しを決定します。読み取りパターンにはシーケンシャルとランダムがあります。

次の表に、階層化ポリシーと各ポリシーのクラウドデータ読み出しルールを示します。

階層化ポリシー	読み出し動作
なし	シーケンシャルリードとランダムリード
Snapshotのみ	シーケンシャルリードとランダムリード
自動	ランダムリード
すべて	データ読み出しなし

ONTAP 9 .8以降では、クラウド移行制御 `cloud-retrieval-policy`オプションによって、階層化ポリシーで制御

されるデフォルトのクラウド移行（読み出し）動作が上書きされます。

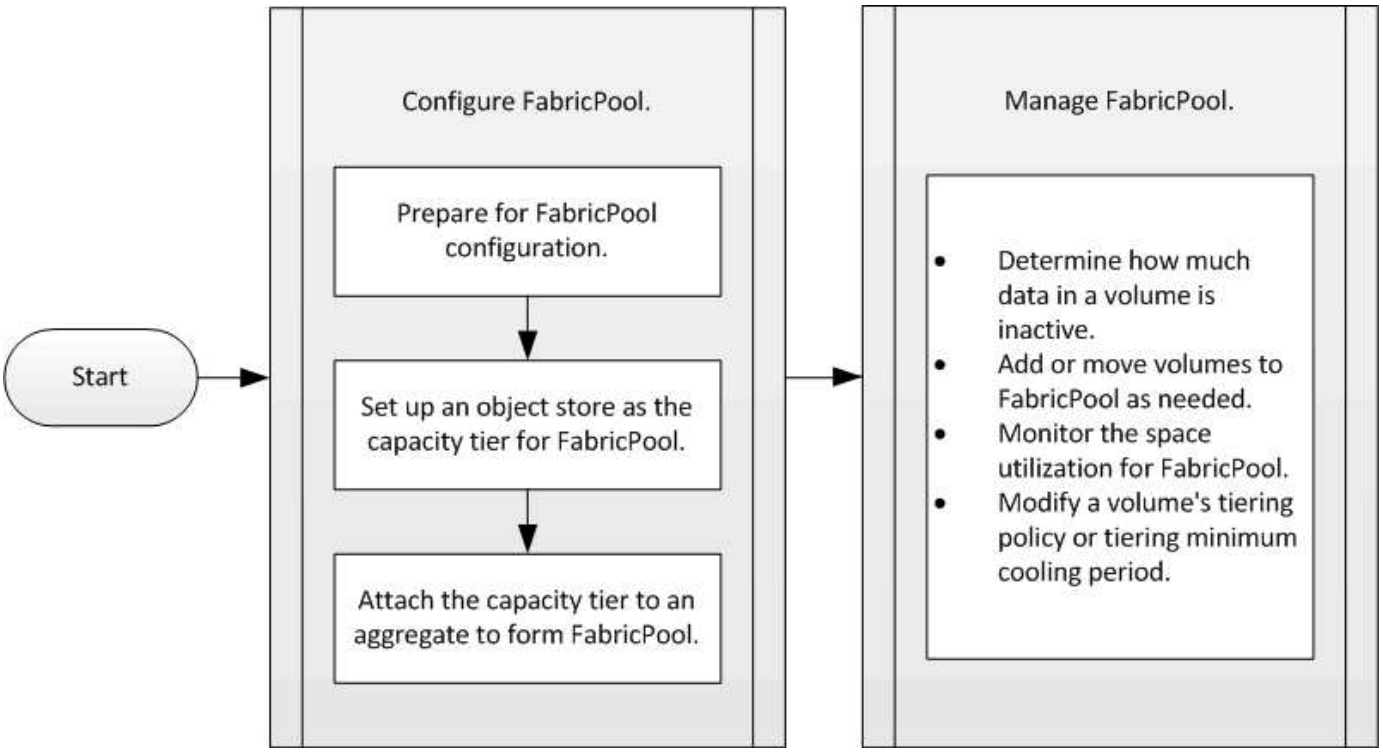
次の表に、サポートされているクラウド読み出しポリシーとその読み出し動作を示します。

クラウド読み出しポリシー	読み出し動作
デフォルト	どのデータを移行するかは階層化ポリシーによって決定されるため、「デフォルト」のクラウドデータの読み出しに変更はありません," `cloud-retrieval-policy`。このポリシーは、ホストされているアグリゲートのタイプに関係なく、すべてのボリュームのデフォルト値です。
オンリード	クライアントによって読み取られたデータはすべてクラウド階層から高パフォーマンス階層に移行されます。
しない	クライアントによって読み取られたデータはクラウド階層から高パフォーマンス階層に移行されません。
プロモート	• 階層化ポリシー「 none 」の場合、すべてのクラウドデータはクラウド階層からパフォーマンス階層にプルされます • 階層化ポリシー「スナップショットのみ」の場合、「 AFS データ」はプルされます。

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

ONTAP FabricPool の設定と管理タスクについて学習します

FabricPoolのワークフロー図を使用して、設定タスクと管理タスクを計画できます。



FabricPoolの設定

FabricPool構成の準備

ONTAP FabricPoolの使用を開始する

FabricPoolを設定すると、アクセス頻度に基づいてデータを格納するストレージ階層（ローカルの高パフォーマンス階層またはクラウド階層）を管理する際に役立ちます。

FabricPool 構成に必要な準備は、クラウド階層として使用するオブジェクトストアによって異なります。

ONTAPクラスタへのFabricPoolライセンスのインストール

過去に使用したことがあるFabricPoolライセンスは変更され、 NetAppコンソール内でサポートされていない構成に対してのみ保持されます。 2021 年 8 月 21 日より、 NetApp Cloud Tiering を使用してNetAppコンソール内でサポートされている階層化構成に対して、 NetApp Cloud Tiering BYOL ライセンスが導入されました。

"NetApp Cloud Tiering BYOLライセンスの詳細" 。

NetAppコンソールでサポートされている構成では、コンソールを使用してONTAPクラスターの階層化のライセンスを取得する必要があります。これには、 NetAppコンソール アカウントを設定し、使用する予定の特定のオブジェクト ストレージ プロバイダーの階層化を設定する必要があります。コンソールは現在、Amazon S3、Azure Blob ストレージ、Google Cloud Storage、S3 互換オブジェクト ストレージ、 StorageGRID のオブジェクト ストレージへの階層化をサポートしています。

"NetAppクラウド階層化サービスの詳細" 。

コンソール内でサポートされていない構成のいずれかがある場合は、System Manager を使用してFabricPool

ライセンスをダウンロードしてアクティブ化できます。

- ダークサイトでのONTAPインストール
- IBM Cloud Object StorageまたはAlibaba Cloud Object Storageにデータを階層化するONTAPクラスタ

FabricPoolライセンスはクラスタ全体のライセンスです。このライセンスには、クラスタ内のFabricPoolに関連付けられたオブジェクトストレージ用に購入する使用量の制限が設定されています。クラスタ全体での使用量が、設定されている使用量制限の容量を超えないようにする必要があります。ライセンスの使用量の制限を増やす必要がある場合は、営業担当者にお問い合わせください。

FabricPoolライセンスには、無期限のライセンスとタームベース（1年または3年）のライセンスがあります。

NetAppコンソールでサポートされていない既存のクラスター構成のFabricPoolを初めて注文する場合は、10 TB の空き容量を持つ期間ベースのFabricPoolライセンスが利用できます。無期限のライセンスには空き容量は含まれていません。NetApp StorageGRIDまたはONTAP S3をクラウド階層として使用する場合は、ライセンスは必要ありません。Cloud Volumes ONTAPでは、いずれのプロバイダを使用する場合も、FabricPoolライセンスは必要ありません。

以下のタスクを実行する場合、System Managerを使用してクラスタにライセンス ファイルをアップロードする必要があります。

手順

1. からFabricPoolライセンスのNetAppライセンスファイル（NLF）をダウンロードします"NetAppサポートサイト"。
2. System Managerを使用して次の操作を実行し、FabricPoolライセンスをクラスタにアップロードします。
   a. [クラスタ]>[設定]ペインの[ライセンス]*カードで、をクリックします →。
   b. [ライセンス]ページで、をクリックします + Add。
   c. [* ライセンスの追加 *] ダイアログボックスで、 [* 参照] をクリックしてダウンロードした NLF を選択し、 [* 追加] をクリックしてファイルをクラスタにアップロードします。

関連情報

"ONTAP FabricPool（FP）ライセンスの概要"

"NetAppソフトウェアライセンスの検索"

"NetApp TechComm TV ： FabricPool 関連ビデオ"

StorageGRID用の**ONTAP**クラスタへの**CA**証明書のインストール

CA証明書を使用すると、クライアントアプリケーションとStorageGRIDの間に信頼された関係が作成されます。

StorageGRIDの証明書のチェックを無効にする予定でないかぎり、StorageGRID CA証明書をクラスタにインストールして、ONTAPがFabricPoolのオブジェクトストアとしてStorageGRIDで認証できるようにする必要があります。

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

タスクの内容

認証局（CA）証明書のインストールと使用が推奨されるベストプラクティスですが、ONTAP 9.4以降では、StorageGRIDにCA証明書をインストールする必要はありません。

手順

1. StorageGRID管理者に問い合わせて、を入手して "StorageGRIDシステムのCA証明書"ください。
2. `security certificate install`コマンドでパラメータを指定し `-type `server-ca`て、StorageGRID CA証明書をクラスタにインストールします。

   入力するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）とStorageGRID CA証明書のカスタム共通名が一致している必要があります。

期限切れの証明書を更新する

期限切れの証明書を更新するには、信頼されたCAを使用して新しいサーバ証明書を生成することを推奨します。また、ダウンタイムを最小限に抑えるために、StorageGRIDサーバとONTAPクラスタで証明書を同時に更新する必要があります。

関連情報

- "StorageGRIDのリソース"
- "セキュリティ証明書のインストール"

ONTAP S3のクラスタにCA証明書をインストールする

CA証明書を使用すると、クライアントアプリケーションとONTAP S3オブジェクトストアサーバの間に信頼された関係が作成されます。ONTAPをリモートクライアントからアクセス可能なオブジェクトストアとして使用する前に、CA証明書をインストールしておく必要があります。

ONTAP S3の証明書のチェックを無効にする予定がないかぎり、ONTAP S3のCA証明書をクラスタにインストールして、ONTAPがFabricPoolのオブジェクトストアとしてONTAP S3で認証できるようにする必要があります。

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

手順

1. ONTAP S3システムのCA証明書を取得します。
2. `security certificate install`コマンドでパラメータを指定し `-type `server-ca`て、ONTAP S3 CA証明書をクラスタにインストールします。

   入力するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）とONTAP S3 CA証明書のカスタム共通名が一致している必要があります。

期限切れの証明書を更新する

期限切れの証明書を更新するには、信頼されたCAを使用して新しいサーバ証明書を生成することを推奨します。また、ダウンタイムを最小限に抑えるために、ONTAP S3サーバとONTAPクラスタで証明書を同時に更新する必要があります。

System Managerを使用して、ONTAPクラスタで期限切れの証明書を更新できます。

手順

1. [クラスタ]>[設定]*に移動します。
2. セクションまでスクロールし、[証明書]*ペインを見つけてをクリックします。
3. [信頼された認証局]タブで、更新する証明書の名前を探します。
4. 証明書名の横にあるをクリックし、*[Renew]*を選択します。
5. ウィンドウで、証明書情報をコピーして貼り付けるか、[証明書の詳細]*領域にインポートします。
6. [更新]*をクリックします。

関連情報

- "S3構成"
- "セキュリティ証明書のインストール"

FabricPoolのクラウド階層として使用するオブジェクトストアのセットアップ

FabricPoolのクラウド階層として使用するオブジェクトストアの設定の概要

FabricPool FabricPoolのセットアップで、クラウド階層として使用するオブジェクトストア（StorageGRID、ONTAP S3、Alibaba Cloud Object Storage、Amazon S3、Google Cloud Storage、IBM Cloud Object Storage、Microsoft Azure Blob Storage）の設定情報を指定します。

ONTAP FabricPoolクラウド階層としての**StorageGRID**のセットアップ

StorageGRID をFabricPoolのクラウド層として設定できます。SANプロトコルでアクセスされるデータを階層化する場合、接続性を考慮して、 NetAppStorageGRIDなどのプライベートクラウドの使用を推奨しています。

FabricPoolで**StorageGRID**を使用する場合の考慮事項

- 証明書のチェックを明示的に無効にした場合を除き、StorageGRIDのCA証明書をインストールする必要があります。
- オブジェクトストアバケットでStorageGRIDオブジェクトのバージョン管理を有効にしないでください。
- FabricPoolライセンスは必要ありません。
- NetApp AFFシステムからストレージが割り当てられた仮想マシンにStorageGRIDノードが導入されている場合は、ボリュームでFabricPool階層化ポリシーが有効になっていないことを確認してください。

  StorageGRIDノードで使用するボリュームでFabricPool階層化を無効にすると、トラブルシューティングとストレージの処理が簡単になります。

> FabricPoolを使用して、StorageGRIDに関連するデータをStorageGRID自体に階層化しないでください。StorageGRIDデータをStorageGRIDに階層化すると、トラブルシューティングや運用が複雑になります。

タスクの内容

ONTAP 9 .8以降では、StorageGRIDのロードバランシングが有効になっています。サーバのホスト名が複数のIPアドレスに解決されると、ONTAPは返されたすべてのIPアドレス（最大16個のIPアドレス）を使用してクライアント接続を確立します。接続が確立されると、ラウンドロビン方式でIPアドレスが取得されます。

手順

ONTAP System ManagerまたはONTAP CLIを使用して、StorageGRIDをFabricPoolのクラウド階層としてセットアップできます。

System Manager

1. [*ストレージ]、[階層]、[クラウド階層の追加]の順にクリックし、オブジェクトストアプロバイダとして[StorageGRID]を選択します。
2. 必要な情報を入力します。
3. CloudMirror を作成する場合は、 * FabricPool ミラーとして追加 * をクリックします。

FabricPoolミラーを使用すると、データストアをシームレスに置き換えることができ、災害発生時にデータを利用できるようになります。

CLI

1. コマンドでパラメータを指定して `-provider-type SGWS`、StorageGRIDの設定情報を指定し `storage aggregate object-store config create`ます。

   - `storage aggregate object-store config create`指定された情報でONTAPがStorageGRIDにアクセスできない場合、コマンドは失敗します。
   - パラメータを使用し `-access-key`て、StorageGRIDオブジェクトストアへの要求を認証するためのアクセスキーを指定します。
   - パラメータを使用し `-secret-password`て、StorageGRIDオブジェクトストアへの要求を認証するためのパスワード（シークレットアクセスキー）を指定します。
   - StorageGRID パスワードが変更された場合は、 ONTAP に格納されている対応するパスワードをただちに更新する必要があります。

     これにより、ONTAPは引き続きStorageGRID内のデータにアクセスできます。

   - パラメータをに `false`設定する `-is-certificate-validation-enabled` と、`StorageGRID`の証明書チェックが無効になります。署名付き証明書を使用する (-is -certificate-validation-enabled true`ことを推奨します）。サードパーティの認証局から取得した証明書を使用することを推奨します。

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. コマンドを使用して、StorageGRIDの設定情報を表示して確認します `storage aggregate object-store config show`。

`storage aggregate object-store config modify`
コマンドを使用して、`FabricPool`の`StorageGRID`設定情報を変更できます。

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"

- "ストレージ集約オブジェクトストア構成表示"

ONTAP S3をFabricPoolクラウド階層としてセットアップする

ONTAP 9 .8以降を実行している場合は、ONTAP S3をFabricPoolのクラウド階層としてセットアップできます。

開始する前に

- ONTAP S3サーバの名前と、リモートクラスタ上の関連付けられているLIFのIPアドレスを確認しておく必要があります。

  サーバ名は、クライアントアプリケーションによってFully Qualified Domain Name（FQDN；完全修飾ドメイン名）として使用されます。ONTAP以外で、使用中のSVMデータLIFを参照しているDNSレコードを確認します。

- ローカルクラスタにが存在している必要がありクラスタ内LIFます。

  ローカルクラスタの階層化を設定した場合は、ローカル階層（ONTAP CLIではストレージアグリゲートとも呼ばれます）がローカルバケットに接続されます。FabricPoolは、クラスタ内トラフィックにクラスタLIFを使用します。

  クラスタLIFのリソースが飽和状態になると、パフォーマンスが低下する可能性があります。これを回避するために、NetAppでは、ローカルバケットに階層化する場合は4ノード以上のクラスタを使用し、ローカル階層にはHAペア、ローカルバケットにはHAペアを使用することを推奨しています。単一のHAペアのローカルバケットへの階層化は推奨されません。

- ONTAP S3を使用してリモートのFabricPool容量（クラウド）階層化を有効にするには、FabricPoolクライアントと"データLIFの設定"オブジェクトストアサーバで実行する必要があります"クラスタ間LIFを設定"。

タスクの内容

ONTAP 9 .8以降では、ONTAP S3サーバのロードバランシングが有効になっています。サーバのホスト名が複数のIPアドレスに解決されると、ONTAPは返されたすべてのIPアドレス（最大16個のIPアドレス）を使用してクライアント接続を確立します。接続が確立されると、ラウンドロビン方式でIPアドレスが取得されます。

手順

ONTAP System ManagerまたはONTAP CLIを使用して、ONTAP S3をFabricPoolのクラウド階層としてセットアップできます。

System Manager

1. ストレージ>階層>クラウド階層の追加*をクリックし、オブジェクトストアプロバイダとしてONTAP S3を選択します。
2. 必要な情報を入力します。
3. CloudMirror を作成する場合は、 * FabricPool ミラーとして追加 * をクリックします。

FabricPoolミラーを使用すると、データストアをシームレスに置き換えることができ、災害発生時にデータを利用できるようになります。

CLI

1. S3サーバとLIFのエントリをDNSサーバに追加します。

オプション	説明
• 外部 DNS サーバーを使用する場合 *	S3サーバの名前とIPアドレスをDNSサーバ管理者に渡します。
• ローカルシステムの DNS hosts テーブル * を使用している場合	次のコマンドを入力します。 `dns host create -vserver <svm_name> -address ip_address -hostname <s3_server_name>`

2. コマンドでパラメータを `-provider-type` `ONTAP_S3`使用して、ONTAP S3の設定情報を指定し `storage aggregate object-store config create`ます。

   - `storage aggregate object-store config create`指定した情報でローカルのONTAPシステムがONTAP S3サーバにアクセスできない場合、コマンドは失敗します。
   - パラメータを使用し `-access-key`て、ONTAP S3サーバへの要求を認証するためのアクセスキーを指定します。
   - パラメータを使用して `-secret-password`、ONTAP S3サーバへの要求を認証するためのパスワード（シークレットアクセスキー）を指定します。
   - ONTAP S3サーバのパスワードが変更された場合は、ローカルのONTAPシステムに格納されている対応するパスワードをただちに更新する必要があります。

     これにより、中断なくONTAP S3オブジェクトストア内のデータにアクセスできます。

   - パラメータをに `false`設定する `-is-certificate-validation-enabled`と、ONTAP S3の証明書のチェックが無効になります。署名付き証明書を使用する (-is-certificate-validation-enabled true`ことを推奨します）。サードパーティの認証局から取得した証明書を使用することを推奨します。

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. コマンドを使用して、ONTAP _S3の設定情報を表示して確認します `storage aggregate object-store config show`。

`storage aggregate object-store config modify`
コマンドを使用して、FabricPoolの設定情報を変更でき `ONTAP_S3`ます。

関連情報

- "SMB用のLIFの作成"
- "NFS用のLIFの作成"
- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"
- "ストレージ集約オブジェクトストア構成表示"

ONTAP FabricPoolクラウド階層としての**Alibaba**クラウドオブジェクトストレージのセットアップ

ONTAP 9 .6以降を実行している場合は、Alibabaクラウドオブジェクトストレージをを FabricPoolのクラウド階層としてセットアップできます。

FabricPoolで**Alibaba**クラウドオブジェクトストレージを使用する場合の考慮事項

- あ"NetAppクラウド階層化ライセンス"Alibaba Cloud Object Storage に階層化する場合、必要です。詳細については、以下を参照してください。 "ONTAPクラスタへのFabricPoolライセンスのインストール" 。
- AFFシステム、FASシステム、およびONTAP Selectでは、FabricPoolで次のAlibabaオブジェクトストレージサービスクラスがサポートされます。
  - Alibaba Object Storage Service標準
  - Alibaba Object Storage Serviceの低頻度アクセス

    "Alibaba Cloud ：ストレージクラスの概要"

上記以外のストレージクラスについては、NetApp営業担当者にお問い合わせください。

手順

1. コマンドでパラメータを `-provider-type AliCloud`使用して、Alibaba Cloud Object Storage の設定情報を指定します `storage aggregate object-store config create`。
   - `storage aggregate object-store config create`指定された情報でONTAPがAlibabaクラウドオブジェクトストレージにアクセスできない場合、コマンドは失敗します。

- パラメータを使用し `-access-key`て、Alibaba Cloud Object Storageオブジェクトストアへの要求を認証するためのアクセスキーを指定します。
- Alibaba Cloud Object Storageのパスワードが変更された場合は、ONTAPに格納されている対応するパスワードをただちに更新する必要があります。

  これにより、ONTAPは引き続きAlibabaクラウドオブジェクトストレージ内のデータにアクセスできます。

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. コマンドを使用して、Alibaba Cloud Object Storageの設定情報を表示して確認します `storage aggregate object-store config show`。

   FabricPoolのAlibabaクラウドオブジェクトストレージの設定情報は、 `storage aggregate object-store config modify`コマンドを使用して変更できます。

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"
- "ストレージ集約オブジェクトストア構成表示"

Amazon S3を**ONTAP FabricPool**クラウド階層としてセットアップする

FabricPoolのクラウド層として Amazon S3 を設定できます。ONTAP 9.5以降を実行している場合は、Amazon Commercial Cloud Services（C2S）をFabricPool用にセットアップできます。

FabricPoolで**Amazon S3**を使用する場合の考慮事項

- あ"NetAppクラウド階層化ライセンス"Amazon S3 に階層化する場合必要です。
- ONTAPがAmazon S3オブジェクトサーバとの接続に使用するLIFは10Gbpsポートに配置することを推奨します。
- AFFシステム、FASシステム、およびONTAP Selectでは、FabricPoolで次のAmazon S3ストレージクラスがサポートされます。
  - Amazon S3標準
  - Amazon S3標準-低頻度アクセス（Standard-IA）
  - Amazon S3 1ゾーン-低頻度アクセス（1ゾーン- IA）
  - Amazon S3のインテリジェントな階層化
  - Amazon Commercial Cloud Services
  - ONTAP 9.11.1以降では、Amazon S3 Glacier Instant Retrieval（FabricPoolではGlacier Flexible RetrievalやGlacier Deep Archiveはサポートされません）

"Amazon Web Servicesドキュメント：「Amazon S3 Storage Classes」"

上記以外のストレージクラスについては、営業担当者にお問い合わせください。

- Cloud Volumes ONTAPでは、FabricPoolがAmazon Elastic Block Store（EBS）の汎用SSD（gp2）ボリュームとスループット最適化HDD（st1）ボリュームからの階層化をサポートしています。

手順

1. コマンドでパラメータを `-provider-type` `AWS_S3`使用して、Amazon S3の設定情報を指定し `storage aggregate object-store config create`ます。

   - C2Sアクセス用のクレデンシャルを取得するには、パラメータを使用し `-auth-type` `CAP`ます。

     パラメータを使用する場合 `-auth-type CAP`は、パラメータを使用して完全な`URL`を指定し、`C2S`アクセス用の一時的なクレデンシャルを要求する必要があります `-cap-url`。

   - `storage aggregate object-store config create`指定された情報でONTAPがAmazon S3にアクセスできない場合、コマンドは失敗します。
   - パラメータを使用し `-access-key`て、Amazon S3オブジェクトストアへの要求を認証するためのアクセスキーを指定します。
   - パラメータを使用し `-secret-password`て、Amazon S3オブジェクトストアへの要求を認証するためのパスワード（シークレットアクセスキー）を指定します。
   - Amazon S3のパスワードが変更された場合は、ONTAPに格納されている対応するパスワードをただちに更新する必要があります。

     これにより、ONTAPは引き続きAmazon S3内のデータにアクセスできます。

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. コマンドを使用して、Amazon S3の設定情報を表示して確認します `storage aggregate object-store config show`。

   FabricPoolのAmazon S3の設定情報は、 `storage aggregate object-store config modify`コマンドを使用して変更できます。

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"
- "ストレージ集約オブジェクトストア構成表示"

Google Cloud StorageをONTAP FabricPoolクラウド階層としてセットアップする

ONTAP 9 .6以降を実行している場合は、FabricPoolのクラウド階層としてGoogle Cloud Storageをセットアップできます。

FabricPoolでGoogle Cloud Storageを使用する場合のその他の考慮事項

- あ"NetAppクラウド階層化ライセンス"Google Cloud Storage に階層化する場合、必須です。
- ONTAPがGoogle Cloud Storageオブジェクトサーバとの接続に使用するLIFは10Gbpsポートに配置することを推奨します。
- AFFシステム、FASシステム、およびONTAP Selectでは、FabricPoolで次のGoogle Cloud Objectストレージクラスがサポートされます。
  - Google Cloudマルチリージョナル
  - Google Cloudリージョナル
  - Google Cloud Nearline
  - Google Cloud Coldline

    "Google Cloud ：ストレージクラス"

手順

1. コマンドでパラメータを `-provider-type` `GoogleCloud`使用して、Google Cloud Storageの設定情報を指定し `storage aggregate object-store config create`ます。
   - `storage aggregate object-store config create`指定された情報でONTAPがGoogle Cloud Storageにアクセスできない場合、コマンドは失敗します。
   - パラメータを使用し `-access-key`て、Google Cloud Storageオブジェクトストアへの要求を認証するためのアクセスキーを指定します。
   - Google Cloud Storageのパスワードが変更された場合は、ONTAPに保存されている対応するパスワードをすぐに更新する必要があります。

     これにより、ONTAPは引き続きGoogle Cloud Storage内のデータにアクセスできます。

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud  -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. コマンドを使用して、Google Cloud Storageの設定情報を表示して確認します `storage aggregate object-store config show`。

`storage aggregate object-store config modify`
コマンドを使用して、FabricPoolのGoogle Cloud Storageの設定情報を変更できます。

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"
- "ストレージ集約オブジェクトストア構成表示"

ONTAP FabricPoolクラウド階層としての**IBM Cloud Object Storage**のセットアップ

ONTAP 9 .5以降を実行している場合は、IBM Cloud Object StorageをFabricPoolのクラウド階層としてセットアップできます。

FabricPoolで**IBM Cloud Object Storage**を使用する場合の考慮事項

- あ"NetAppクラウド階層化ライセンス"IBM Cloud Object Storage に階層化する場合、必要です。
- ONTAPがIBM Cloudオブジェクトサーバとの接続に使用するLIFは10Gbpsポートに配置することを推奨します。

手順

1. コマンドでパラメータを `-provider-type` `IBM_COS`使用して、IBM Cloud Object Storageの設定情報を指定し `storage aggregate object-store config create`ます。

   - `storage aggregate object-store config create`指定された情報でONTAPがIBM Cloud Object Storageにアクセスできない場合、コマンドは失敗します。
   - パラメータを使用し `-access-key`て、IBM Cloud Object Storageオブジェクトストアへの要求を認証するためのアクセスキーを指定します。
   - パラメータを使用し `-secret-password`て、IBM Cloud Object Storageオブジェクトストアへの要求を認証するためのパスワード（シークレットアクセスキー）を指定します。
   - IBM Cloud Object Storageのパスワードが変更された場合は、ONTAPに格納されている対応するパスワードをただちに更新する必要があります。

     これにより、ONTAPは引き続きIBM Cloud Object Storage内のデータにアクセスできます。

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. コマンドを使用して、IBM Cloud Object Storageの設定情報を表示して確認します `storage aggregate object-store config show`。

`storage aggregate object-store config modify`
コマンドを使用して、FabricPoolのIBMクラウドオブジェクトストレージの設定情報を変更できます。

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"
- "ストレージ集約オブジェクトストア構成表示"

ONTAP FabricPoolクラウド階層としての**Azure Blob Storage**のセットアップ

ONTAP 9.4以降を実行している場合は、Azure Blob StorageをFabricPoolのクラウド階層としてセットアップできます。

FabricPoolで**Microsoft Azure Blob Storage**を使用する場合の考慮事項

- あ"NetAppクラウド階層化ライセンス"Azure Blob Storage に階層化する場合、必須です。
- Cloud Volumes ONTAPでAzure Blob Storageを使用している場合は、FabricPoolライセンスは必要ありません。
- ONTAPがAzure Blob Storageオブジェクトサーバとの接続に使用するLIFは、10Gbpsポートに配置することを推奨します。
- FabricPoolは現在、オンプレミスのAzureサービスであるAzure Stackをサポートしていません。
- Microsoft Azure Blob Storageのアカウントレベルでは、FabricPoolでサポートされるのはホットストレージ階層とクールストレージ階層のみです。

  FabricPoolでは、BLOBレベルの階層化はサポートされていません。また、Azureのアーカイブストレージ階層への階層化もサポートされていません。

タスクの内容

FabricPoolは現在、オンプレミスのAzureサービスであるAzure Stackをサポートしていません。

手順

1. コマンドでパラメータを `-provider-type` `Azure_Cloud`使用して、Azure Blob Storageの設定情報を指定し `storage aggregate object-store config create`ます。

   - `storage aggregate object-store config create`指定された情報でONTAPがAzure Blob Storageにアクセスできない場合、コマンドは失敗します。
   - パラメータを使用して `-azure-account`、Azure Blob Storageアカウントを指定します。
   - パラメータを使用し `-azure-private-key`て、Azure Blob Storageへの要求を認証するためのアクセスキーを指定します。
   - Azure Blob Storageのパスワードが変更された場合は、ONTAPに格納されている対応するパスワードをただちに更新する必要があります。

     これにより、ONTAPは引き続きAzure Blob Storage内のデータにアクセスできます。

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. コマンドを使用して、Azure Blob Storageの設定情報を表示して確認します `storage aggregate object-store config show`。

```
`storage aggregate object-store config modify`
コマンドを使用して、FabricPoolのAzure Blob Storageの設定情報を変更できます。
```

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成の変更"
- "ストレージ集約オブジェクトストア構成表示"

MetroCluster構成で**ONTAP FabricPool**のオブジェクトストアを設定する

ONTAP 9 .7以降を実行している場合は、MetroCluster構成にミラーされたFabricPoolをセットアップして、2つの異なる障害ゾーンにあるオブジェクトストアにコールドデータを階層化できます。

タスクの内容

- MetroClusterのFabricPoolを使用するには、基盤となるミラーアグリゲートと関連するオブジェクトストア設定が同じMetroCluster設定に所有されている必要があります。
- リモートMetroClusterサイトで作成されたオブジェクトストアにアグリゲートを接続することはできません。
- オブジェクトストア設定は、アグリゲートが属するMetroCluster構成に作成する必要があります。

開始する前に

- MetroCluster構成がセットアップされ、適切に設定されている。
- 2つのオブジェクトストアが適切なMetroClusterサイトにセットアップされている。
- コンテナは各オブジェクトストアで設定されます。
- 2つのMetroCluster構成でIPスペースが作成または識別され、名前が一致している。

ステップ

1. コマンドを使用して、各MetroClusterサイトのオブジェクトストア設定情報を指定し `storage object-store config create`ます。

   この例では、MetroCluster構成の一方のクラスタにのみFabricPoolが必要です。オブジェクトストアバケットごとに1つずつ、2つのオブジェクトストア設定をそのクラスタ用に作成します。

```
storage aggregate
    object-store config create -object-store-name mcc1-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
    -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
<true|false> -provider <provider-type>
    -is-ssl-enabled <true|false> ipspace <IPSpace>
```

この例では、MetroCluster構成の2つ目のクラスタにFabricPoolをセットアップします。

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

関連情報

- "ストレージオブジェクトストア構成の作成"

オブジェクトストアをローカル階層に接続する前に、オブジェクトストアプロファイラを使用してオブジェクトストアのレイテンシとスループットのパフォーマンスをテストできます。

> オブジェクトストアプロファイラの結果は、ONTAPとクラウド階層のオブジェクトストア間の接続に4MBのPUTを使用し、バイト範囲のランダムリードを4MB~256KBの範囲で測定したものです。（32KBを超えるGETを使用できるのは、SnapMirrorなどの内部ONTAP機能のみです）。
>
> ワークロードの競合やクライアントアプリケーション固有の動作が考慮されていないため、オブジェクトストアプロファイラの結果は階層化のパフォーマンスを完全に示すものではありません。

開始する前に

- オブジェクトストアプロファイラでクラウド階層を使用するには、ONTAPにクラウド階層を追加する必要があります。
- ONTAP CLIのadvanced権限モードに切り替える必要があります。

手順

1. オブジェクトストアプロファイラを起動します。

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. 結果を表示します。

   ```
   storage aggregate object-store profiler show
   ```

関連情報

- "ストレージ集約オブジェクトストアプロファイラー表示"
- "ストレージ集約オブジェクトストアプロファイラーの開始"

クラウド階層として使用するオブジェクトストアのセットアップが完了したら、使用するローカル階層をFabricPoolに接続して指定します。ONTAP 9.5以降では、対象となるFlexGroupボリュームコンスティチュエントを含むローカル階層を接続することもできます。

> ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

タスクの内容

ローカル階層へのクラウド階層の接続は永続的な操作です。接続後にローカル階層からクラウド階層の接続を

解除することはできません。ただし、を使用し"FabricPoolミラー"て別のクラウド階層にローカル階層を接続することもできます。

開始する前に

ONTAP CLIを使用してFabricPool用のローカル階層をセットアップする場合は、ローカル階層がすでに存在している必要があります。

> System Managerを使用してFabricPoolのローカル階層をセットアップする場合は、ローカル階層を作成してFabricPoolで使用するようにセットアップすることができます。

手順

ONTAP System ManagerまたはONTAP CLIを使用して、FabricPoolオブジェクトストアにローカル階層を接続できます。

System Manager

1. [ストレージ]>[階層]*に移動し、クラウド階層を選択してをクリックします。
2. ローカル階層の接続*を選択します。
3. [プライマリとして追加]で、ボリュームが接続可能であることを確認します。
4. 必要に応じて、*ボリュームをシンプロビジョニングに変換*を選択します。
5. [保存（ Save ）] をクリックします。

CLI

CLIを使用してオブジェクトストアをアグリゲートに接続するには、次の手順を実行します。

1. オプション：ボリューム内のアクセス頻度の低いデータの量を確認するには、の手順に従います"Inactive Data Reportingによるボリューム内のアクセス頻度の低いデータ量の確認"。

   ボリューム内のアクセス頻度の低いデータの量を確認すると、FabricPoolに使用するアグリゲートを決定するのに役立ちます。

2. コマンドを使用して、オブジェクトストアをアグリゲートに接続し `storage aggregate object-store attach`ます。

   FabricPoolで使用されたことがないアグリゲートで、既存のボリュームが含まれている場合、ボリュームにはデフォルトの階層化ポリシーが割り当てられ `snapshot-only`ます。

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

   オプションを使用すると、FlexGroupボリュームのコンスティチュエントを含むアグリゲートを接続できます `allow-flexgroup true`。

3. コマンドを使用して、オブジェクトストアの情報を表示し、接続したオブジェクトストアが使用可能であることを確認します `storage aggregate object-store show`。

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   myaggr       Amazon01B1           available
   ```

関連情報

- "ストレージ集約オブジェクトストアアタッチ"
- "ストレージ集約オブジェクトストア表示"

ONTAP 9 .8以降では、ONTAP S3を使用してローカルのオブジェクトストレージにデータを階層化できます。

データをローカルバケットに階層化すると、別のローカル階層にデータを移動する代わりに簡単に使用できます。この手順では、ローカルクラスタの既存のバケットを使用するか、またはONTAPで新しいStorage VMとバケットを自動的に作成することができます。

プライマリローカルバケットを接続したあとは、接続を解除できないことに注意してください。

開始する前に

- このワークフローではS3ライセンスが必要です。このワークフローでは、新しいS3サーバと新しいバケットを作成するか、既存のバケットを使用します。このライセンスはに含まれてい"ONTAP One"ます。このワークフローにはFabricPoolライセンスは必要ありません。
- "ローカルFabricPool階層化用のONTAP S3アクセスの有効化"です。

手順

1. ローカルバケットにデータを階層化する：**[**ストレージ**]>[**階層**]***をクリックし、[SSD]ペインでローカル階層を選択し、をクリックし⋮て[ローカルバケットに階層化]*を選択します。
2. [Primary tier]セクションで、[Existing]または[New]を選択します。
3. [保存（ Save ）] をクリックします。

FabricPoolの管理

Inactive Data Reportingでアクセス頻度の低い**ONTAP**データを分析

ボリューム内のアクセス頻度の低いデータの量を確認することで、ストレージ階層を効率よく使用することができます。Inactive Data Reportingの情報は、FabricPoolに使用するアグリゲート、FabricPoolとの間でボリュームを移動するかどうか、ボリュームの階層化ポリシーを変更するかどうかを決定するのに役立ちます。

開始する前に

Inactive Data Reporting機能を使用するには、ONTAP 9 .4以降を実行している必要があります。

タスクの内容

- Inactive Data Reportingは一部のアグリゲートではサポートされません。

  次のようなFabricPoolを有効にできない場合は、Inactive Data Reportingを有効にできません。

  - ルートアグリゲート
  - 9.7より前のバージョンのONTAPを実行しているMetroClusterアグリゲート
  - Flash Pool（ハイブリッドアグリゲートまたはSnapLockアグリゲート）
- 適応圧縮が有効になっているボリュームがあるアグリゲートでは、Inactive Data Reportingがデフォルトで有効になります。
- ONTAP 9内のすべてのSSDアグリゲートに対してInactive Data Reportingがデフォルトで有効になりま

す。6.

- Inactive Data Reportingは、ONTAP 9 .4およびONTAP 9 .5のFabricPoolアグリゲートに対してデフォルトで有効になります。
- ONTAP 9以降では、HDDアグリゲートを含むONTAP CLIを使用して、FabricPool以外のアグリゲートに対してInactive Data Reportingを有効にすることができます。6.

手順

ONTAP System ManagerまたはONTAP CLIを使用して、アクセス頻度の低いデータの量を確認できます。

System Manager

1. 次のいずれかのオプションを選択します。
   - 既存のHDDアグリゲートがある場合は、*[ストレージ]>[階層]*に移動し、Inactive Data Reportingを有効にするアグリゲートのをクリックします ⋮ 。
   - クラウド階層が設定されていない場合は、 * ダッシュボード * に移動し、 * 容量 * の下の * 非アクティブデータレポートの有効化 * リンクをクリックします。

CLI

CLIを使用して**Inactive Data Reporting**を有効にするには：

1. Inactive Data Reportingを表示するアグリゲートがFabricPoolで使用されていない場合は、コマンドでパラメータを指定して `-is-inactive-data-reporting-enabled true`、アグリゲートのInactive Data Reportingを有効にします `storage aggregate modify`。

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

   FabricPoolに使用されていないアグリゲートでは、Inactive Data Reporting機能を明示的に有効にする必要があります。

   FabricPool対応アグリゲートにはすでにInactive Data Reporting機能が搭載されているため、Inactive Data Reportingを有効にすることはできません。また、有効にする必要はありません。パラメータは `-is-inactive-data-reporting-enabled`、FabricPool対応アグリゲートに対しては機能しません。

   コマンドのパラメータ `storage aggregate show`は、 `-fields is-inactive-data-reporting-enabled`アグリゲートでInactive Data Reportingが有効になっているかどうかを表示します。

2. ボリューム上のアクセス頻度の低いデータの量を表示するには、パラメータを指定してコマンドを `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent`使用し `volume show`ます。

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
------- ------ ---------------------------------
----------------------------------------
vsim1   vol0   0B                                 0%
vs1     vs1rv1 0B                                 0%
vs1     vv1    10.34MB                            0%
vs1     vv2    10.38MB                            0%
4 entries were displayed.
```

   - `performance-tier-inactive-user-data`フィールドには、アグリゲートに格納されているアクセス頻

度の低いユーザデータの量が表示されます。

- フィールドに `performance-tier-inactive-user-data-percent`は、アクティブなファイルシステムとSnapshot全体でアクセス頻度の低いデータの割合が表示されます。
- FabricPool に使用されていないアグリゲートの場合、Inactive Data Reportingは階層化ポリシーを使用してコールドとしてレポートするデータの量を決定します。
  - 階層化ポリシーの場合は `none`31日が使用されます。
  - および `auto`の `snapshot-only`Inactive Data Reportingでは、を使用し `tiering-minimum-cooling-days`ます。
  - ポリシーの場合、 `ALL`Inactive Data Reportingでは、データが1日以内に階層化されることが想定されます。

    期間が終了するまで ' 出力には ' 値ではなく ' 非アクティブなデータの量が表示されます
- FabricPool に含まれるボリュームの場合、アクセス頻度の低いデータとして報告される ONTAP は、ボリュームに設定されている階層化ポリシーによって異なります。
  - 階層化ポリシーの場合 `none`、ONTAPはボリューム全体のうち、少なくとも31日間アクセスされていないデータの量を報告します。パラメータは階層化ポリシーで `none`は使用できません `-tiering-minimum-cooling-days`。
  - `ALL` `snapshot-only`階層化ポリシー、、およびで `auto`は、Inactive Data Reportingはサポートされません。

関連情報

- "storage aggregate modify"

FabricPoolのボリュームを管理します。

FabricPool対応の**ONTAP**ローカル階層にボリュームを作成する

FabricPoolにボリュームを追加するには、FabricPool対応のローカル階層で新しいボリュームを直接作成するか、別のローカル階層からFabricPool対応のローカル階層に既存のボリュームを移動します。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

FabricPoolのボリュームを作成するときに、階層化ポリシーを指定できます。階層化ポリシーを指定しない場合、作成されたボリュームはデフォルトの階層化ポリシーを使用し `snapshot-only`ます。階層化ポリシーがまたは `auto`のボリュームについては `snapshot-only`、階層化の最小クーリング期間も指定できます。

開始する前に

- ボリュームで階層化ポリシーを使用するように設定し `auto`たり、階層化の最小クーリング期間を指定したりするには、ONTAP 9 .4以降が必要です。
- FlexGroupボリュームを使用するには、ONTAP 9 .5以降が必要です。

- ボリュームで階層化ポリシーを使用するように設定 `all`するには、ONTAP 9 .6以降が必要です。
- パラメータを使用するようにボリュームを設定 `-cloud-retrieval-policy`するには、ONTAP 9 .8以降が必要です。

手順

1. コマンドを使用して、FabricPool用の新しいボリュームを作成し `volume create`ます。
   - `-tiering-policy`オプションのパラメータを使用すると、ボリュームの階層化ポリシーを指定できます。

     次のいずれかの階層化ポリシーを指定できます。

     - `snapshot-only` （デフォルト）
     - `auto`
     - `all`
     - `backup`（廃止予定）
     - `none`

       "FabricPool階層化ポリシーの種類"
   - オプションのパラメータを `-cloud-retrieval-policy`使用すると、advanced権限レベルのクラスタ管理者は、階層化ポリシーで制御されるデフォルトのクラウド移行または読み出し動作を上書きできます。

     次のいずれかのクラウド読み出しポリシーを指定できます。

     - `default`

       どのデータを移行するかは階層化ポリシーによって決定されるため、cloud-retrieval-policyを使用したクラウドデータの読み出しに変更はありませ `default`ん。これは、動作がONTAP 9 .8より前のリリースと同じであることを意味します。

       - 階層化ポリシーがまたはの `snapshot-only`場合、 `none`「default」は、クライアントによって読み取られたデータがすべてクラウド階層から高パフォーマンス階層に移行されることを意味します。
       - 階層化ポリシーがの場合、 `auto`クライアントによるランダムリードはすべて移行されますが、シーケンシャルリードは移行されません。
       - 階層化ポリシーが指定されている場合 `all`、クライアントによって読み取られたデータはクラウド階層から移行されません。
     - `on-read`

       クライアントによって読み取られたデータはすべてクラウド階層から高パフォーマンス階層に移行されます。
     - `never`

       クライアントによって読み取られたデータはクラウド階層から高パフォーマンス階層に移行されません。
     - `promote`

- 階層化ポリシーの場合 `none`、すべてのクラウドデータがクラウド階層から高パフォーマンス階層に移行されます。
- 階層化ポリシーの場合 `snapshot-only`、アクティブなファイルシステムのすべてのデータがクラウド階層から高パフォーマンス階層に移行されます。

◦ `-tiering-minimum-cooling-days`advanced権限レベルでオプションのパラメータを使用すると、または`auto`階層化ポリシーを使用するボリュームの階層化の最小クーリング期間を指定でき`snapshot-only`ます。

ONTAP 9 .8以降では、階層化の最小クーリング日数に2_{183}の値を指定できます。9.8より前のバージョンのONTAPを使用している場合は、$_{2}$63の値を階層化の最小クーリング日数に指定できます。

FabricPool用のボリュームの作成例

次の例は、FabricPool対応のローカル階層「myFabricPool」に「myvol1」というボリュームを作成します。階層化ポリシーはに `auto`、階層化の最小クーリング期間は45日に設定されています。

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

関連情報

"FlexGroupボリユウムノカンリ"

FabricPool対応の**ONTAP**ローカル階層にボリュームを移動する

は、"ボリューム移動"ONTAPがボリュームをあるローカル階層（ソース）から別のローカル階層（デスティネーション）に無停止で移動する方法です。ボリュームの移動はさまざまな理由に基づいて実行できますが、最も一般的な理由はハードウェア ライフサイクル管理、クラスタ拡張、および負荷分散です。

ローカル階層、接続されたクラウド階層、およびボリューム（ボリューム階層化ポリシー）の両方で行われる変更は、機能に大きな影響を与える可能性があるため、ボリューム移動とFabricPoolの連携について理解しておくことが重要です。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

デスティネーションローカル階層

ボリューム移動のデスティネーションローカル階層に接続されたクラウド階層がない場合、クラウド階層に格納されているソースボリュームのデータはデスティネーションローカル階層のローカル階層に書き込まれます。

ONTAP 9.8以降では、ボリュームが有効になっている場合、"Inactive Data Reporting"FabricPoolはボリュームのヒートマップを使用してコールドデータをただちにキューに入れ、デスティネーションローカル階層に書き込まれるとすぐに階層化を開始します。

ONTAP 9.8より前のバージョンでは、ボリュームを別のローカル階層に移動すると、ローカル階層のブロック

の非アクティブ期間がリセットされます。たとえば、20日間非アクティブでまだ階層化されていないデータがローカル階層にある「自動」ボリューム階層化ポリシーを使用するボリュームでは、ボリューム移動後、データの温度が0日にリセットされます。

ボリューム移動の最適化

ONTAP 9.6以降では、ボリューム移動のデスティネーションローカル階層がソースローカル階層と同じバケットを使用する場合、バケットに格納されているソースボリューム上のデータがローカル階層に戻されません。階層化されたデータは保存されたままになり、ローカル階層間で移動しなければならないのはホットデータだけです。この最適化されたボリューム移動により、ネットワーク効率が大幅に向上します。

たとえば、300 TB の最適化されたボリュームの移動は、300 TB のコールド データがローカル層から別の層に移動されても、オブジェクト ストアへの 300 TB の読み取りと 300 TB の書き込みがトリガーされないことを意味します。

ボリュームの移動が最適化されていない場合、ネットワークとコンピューティングのトラフィック（読み取り/取得と書き込み/プット）が増加し、ONTAPクラスタとオブジェクトストアの需要が増加します。パブリックオブジェクトストアへの階層化のコストが上昇する可能性があります。

一部の構成は最適化されたボリューム移動と互換性がありません

- ボリューム移動時の階層化ポリシーの変更
- 異なる暗号化キーを使用するソースとデスティネーションのローカル階層
- FlexCloneボリューム
- FlexCloneノオヤホリユウム
- MetroCluster（ONTAP 9.8以降での最適化されたボリューム移動をサポート）
- 非同期FabricPoolミラーバケット

ボリューム移動のデスティネーションローカル階層にクラウド階層が接続されている場合は、クラウド階層に格納されているソースボリューム上のデータが最初にデスティネーションローカル階層のローカル階層に書き込まれます。このアプローチがボリューム階層化ポリシーに適している場合は、デスティネーションローカル階層のクラウド階層に書き込まれます。

最初にローカル階層にデータを書き込むと、ボリューム移動のパフォーマンスが向上し、カットオーバー時間が短縮されます。ボリューム移動の実行時にボリューム階層化ポリシーが指定されていない場合、デスティネーション ボリュームはソース ボリュームの階層化ポリシーを使用します。

ボリューム移動の実行時に別の階層化ポリシーを指定した場合、指定した階層化ポリシーでデスティネーションボリュームが作成され、ボリューム移動は最適化されません。

ボリュームメタデータ

ボリューム移動が最適化されているかどうかに関わらず、ONTAPはローカルデータと階層化データの両方について、場所、ストレージ効率、権限、使用パターンなどに関する膨大な量のメタデータを保存します。メタデータは常にローカル階層に保持され、階層化されません。ボリュームをあるローカル階層から別のローカル階層に移動する場合は、この情報をデスティネーションローカル階層にも移動する必要があります。

間隔

ボリュームの移動は完了するまでにまだ時間がかかり、最適化されたボリュームの移動には、同量の非階層化データの移動とほぼ同じ時間がかかることが予想されます。

報告されている「スループット」が `volume move show`このコマンドは、クラウド層から移動されるデータに関するスループットを表すのではなく、ボリューム データがローカルで更新されるという観点からスループットを表します。

SVM DR関係では、ソースボリュームとデスティネーションボリュームで同じ階層化ポリシーを使用する必要があります。

手順

1. コマンドを使用して `volume move start`、ソースローカル階層からデスティネーションローカル階層にボリュームを移動します。

ボリューム移動例

次の例は、 `vs1`SVMという名前のボリュームをFabricPool対応のローカル階層に `dest_FabricPool`移動します `myvol2`。

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool
```

FabricPoolの**ONTAP**ボリュームがクラウドに直接書き込まれるようにする

ONTAP 9 14.1以降では、FabricPoolの新規または既存のボリュームに対してクラウドへの直接書き込みを有効または無効にすることで、NFSクライアントが階層化スキャンを待たずにクラウドに直接データを書き込むことができます。SMBクライアントは、クラウドの書き込みが有効なボリュームの高パフォーマンス階層に引き続き書き込みます。cloud-writeモードはデフォルトで無効になっています。

クラウドに直接書き込む機能は、ローカル階層でクラスタでサポートできない大量のデータがクラスタに転送されるなど、移行のような場合に役立ちます。クラウド書き込みモードを使用しない場合は、移行中に少量のデータが転送されてから階層化され、移行が完了するまで再び転送されて階層化されます。クラウド書き込みモードを使用すると、データがローカル階層に転送されないため、この種の管理は不要になります。

開始する前に

- クラスタ管理者またはSVM管理者である必要があります。
- advanced権限レベルが必要です。
- 読み取り/書き込みタイプのボリュームである必要があります。
- ボリュームの階層化ポリシーが「すべて」である必要があります。

ボリューム作成時のクラウドへの直接書き込みを可能にする

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. ボリュームを作成し、クラウド書き込みモードを有効にします。

```
volume create -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled <true|false> -aggregate <local tier name>
```

次の例は、FabricPoolローカル階層（aggr1）に、クラウド書き込みを有効にしてvol1という名前のボリュームを作成します。

```
volume create -vserver vs1 -volume vol1 -is-cloud-write-enabled true
-aggregate aggr1
```

既存のボリュームのクラウドへの直接書き込みを可能にする

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. ボリュームを変更してクラウド書き込みモードを有効にします。

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled true
```

次の例は、vol1という名前のボリュームを変更して、クラウドへの書き込みを有効にします。

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled true
```

ボリュームのクラウドへの直接書き込みを無効にする

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. ボリュームでクラウド書き込みモードを無効にします。

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled false
```

次の例は、vol1という名前のボリュームでクラウド書き込みモードを無効にします。

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled false
```

FabricPoolで**ONTAP**ボリュームが積極的に読み取りヘッドを実行できるようにする

ONTAP 9 14.1以降では、FabricPool内のボリュームに対してアグレッシブ先読みモードを有効または無効にすることができます。ONTAP 9.13.1では、アグレッシブ先読みモードはクラウドプラットフォームでのみ導入されました。ONTAP9.14.1以降では、オンプレミスプラットフォームを含む、FabricPoolがサポートするすべてのプラットフォームでアグレッシブ先読みモードが利用可能になりました。デフォルトでは、この機能は無効になっています。

アグレッシブな先読みが_disabled_の場合、FabricPoolはクライアントアプリケーションが必要とするファイルブロックのみを読み取ります。ファイル全体を読み取る必要はありません。その結果、特に大容量のGBおよびTBサイズのファイルでは、ネットワークトラフィックが減少する可能性があります。ボリュームでの先読みを_Enabling_Aggressiveにすると、この機能がオフになり、FabricPoolはオブジェクトストアからファイル全体を優先的にシーケンシャルに読み取ります。これにより、GETスループットが向上し、クライアントによるファイルに対する読み取りのレイテンシが低減されます。デフォルトでは、階層化されたデータがシーケンシャルに読み取られてもコールドのままで、ローカル階層には書き込まれません。

積極的な先読みにより、ネットワークの効率性が向上し、階層化されたデータのパフォーマンスが向上します。

タスクの内容

`aggressive-readahead-mode`このコマンドには2つのオプションがあります。

- none:先読みは無効です。
- file_prefetch:クライアントアプリケーションよりも先にファイル全体がメモリに読み込まれます。

開始する前に

- クラスタ管理者またはSVM管理者である必要があります。
- advanced権限レベルが必要です。

ボリューム作成時のアグレッシブ先読みモードの有効化

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. ボリュームを作成し、アグレッシブ先読みモードを有効にします。

```
volume create -volume <volume name>  -aggressive-readahead-mode
<none|file_prefetch>
```

次の例は、file_prefetchオプションを指定して、アグレッシブ先読みを有効にしたvol1という名前のボリュームを作成します。

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

アグレッシブ先読みモードを無効にする

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. アグレッシブ先読みモードを無効にします。

```
volume modify -volume <volume name>  -aggressive-readahead-mode none
```

次の例は、vol1という名前のボリュームを変更して、アグレッシブ先読みモードを無効にします。

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

ボリュームのアグレッシブ先読みモードを表示する

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. アグレッシブ先読みモードを表示します。

```
volume show -fields aggressive-readahead-mode
```

ユーザが作成したカスタムタグを使用して**ONTAP FabricPool**ボリュームを管理します。

ONTAP 9 8以降では、FabricPoolでユーザが作成したカスタムタグを使用したオブジェクトのタグ付けがサポートされています。これにより、オブジェクトの分類やソートが可能になり、管理が容易になります。admin権限レベルのユーザは、新しいオブジェクトタグの作成、既存のタグの変更、削除、表示を行うことができます。

ボリューム作成時に新しいタグを割り当てる

作成する新しいボリュームから階層化される新しいオブジェクトに1つ以上のタグを割り当てる場合は、新しいオブジェクトタグを作成します。タグを使用すると、階層化オブジェクトを分類およびソートしてデータ管理を容易にすることができます。ONTAP 9 8以降では、System Managerを使用してオブジェクトタグを作成できます。

タスクの内容

タグは、StorageGRIDに接続されたFabricPoolにのみ設定できます。これらのタグはボリュームの移動中も保持されます。

- ボリュームごとに最大 4 つのタグが許可されます。
- CLIでは、各オブジェクトタグはキーと値のペアを等号で区切って指定する必要があります。
- CLIでは、複数のタグをカンマで区切る必要があります。
- 各タグ値の最大文字数は127文字です。
- 各タグキーの1文字目はアルファベットかアンダースコアにする必要があります。

  キーに使用できる文字は英数字とアンダースコアのみです。最大文字数は127文字です。

オブジェクトタグは、ONTAP System ManagerまたはONTAP CLIで割り当てることができます。

例 **8.** 手順

System Manager

1. [ストレージ]>[階層]に移動します。
2. タグ付けするボリュームを含むストレージ階層を探します。
3. [* Volumes （ボリューム）] タブをクリックします
4. タグを付けるボリュームを探し、*オブジェクトタグ*列で*クリックしてタグを入力*を選択します。
5. キーと値を入力します。
6. [適用（ Apply ）] をクリックします。

CLI

1. コマンドでオプションを指定して `-tiering-object-tags`、指定したタグを使用して `volume create`新しいボリュームを作成します。複数のタグをカンマで区切って指定できます。

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1>
[,<key2=value2>,<key3=value3>,<key4=value4> ]
```

次の例は、3つのオブジェクトタグを使用するfp_volume1という名前のボリュームを作成します。

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

既存のタグの変更

タグの名前を変更したり、オブジェクトストア内の既存のオブジェクトのタグを置き換えたり、あとで追加する予定の新しいオブジェクトに別のタグを追加したりできます。

例 **9.** 手順

System Manager

1. [ストレージ]>[階層]に移動します。
2. 変更するタグを含むボリュームが含まれているストレージ階層を探します。
3. [* Volumes （ボリューム）] タブをクリックします
4. 変更するタグが付いたボリュームを探し、*オブジェクトタグ*列でタグ名をクリックします。
5. タグを変更します。
6. [適用（ Apply ）] をクリックします。

CLI

1. `volume modify`コマンドにオプションを指定して `-tiering-object-tags`、既存のタグを変更します。

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [ ,<key2=value2>,
<key3=value3>,<key4=value4> ]
```

次の例では、既存のタグの名前を変更します `type=abc`に `type=xyz`。

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

タグの削除

ボリュームまたはオブジェクトストア内のオブジェクトに対して設定されていなくなったオブジェクトタグは、削除できます。

例 **10.** 手順

System Manager

1. [ストレージ]>[階層]に移動します。
2. 削除するタグを含むボリュームが含まれているストレージ階層を探します。
3. [* Volumes （ボリューム）] タブをクリックします
4. 削除するタグが付いたボリュームを探し、*オブジェクトタグ*列でタグ名をクリックします。
5. タグを削除するには、ごみ箱のアイコンをクリックします。
6. [適用（ Apply ）] をクリックします。

CLI

1. `volume modify(`""`既存のタグを削除するには、コマンドでオプションのあとに空の値を指定し `-tiering-object-tags`ます）。

   次の例は、fp_volume1の既存のタグを削除します。

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

ボリュームの既存のタグを表示する

新しいタグをリストに追加する前に、ボリュームの既存のタグを表示して使用可能なタグを確認できます。

手順

1. `volume show`コマンドでオプションを指定して `tiering-object-tags`、ボリューム上の既存のタグを表示します。

   ```
   volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
   tiering-object-tags
   ```

FabricPoolボリュームでのオブジェクトのタグ付けステータスの確認

1つ以上のFabricPoolでタグ付けが完了しているかどうかを確認できます。

手順

1. コマンドでオプションを指定して `-fields needs-object-retagging`、`vol show`タグ付けが進行中かどうか、完了しているかどうか、または設定されていないかどうかを確認します。

   ```
   vol show -fields needs-object-retagging  [ -instance | -volume <volume
   name>]
   ```

   次のいずれかの値が表示されます。

- `true`：このボリュームに対してオブジェクトタグ付けスキャナがまだ実行されていないか、再実行する必要があります。
- `false`：このボリュームのオブジェクトタグ付けスキャナによるタグ付けが完了しました
- `<->`：オブジェクトタグ付けスキャナはこのボリュームには適用されません。ボリュームがFabricPoolにない場合に発生します。

FabricPool対応の**ONTAP**ローカル階層のスペース使用量の監視

FabricPoolのパフォーマンス階層とクラウド階層に格納されているデータの量を把握しておく必要があります。この情報は、ボリュームの階層化ポリシーの変更、FabricPoolライセンスで許可された使用量の制限の拡張、またはクラウド階層のストレージスペースの拡張が必要かどうかを判断するのに役立ちます。

ONTAP 9.7より前のバージョンでは、ローカル階層を表すために_aggregate_という用語が使用されていました。ONTAPのバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。ローカル階層の詳細については、を参照してください"ディスクとローカル階層"。

手順

1. 次のいずれかのコマンドを使用して情報を表示し、FabricPool対応のローカル階層のスペース使用量を監視します。

表示する項目	使用するコマンド
ローカル階層のクラウド階層の使用済みサイズ	`storage aggregate show`パラメータを指定した場合 `-instance`
ローカル階層内のスペース使用量の詳細（オブジェクトストアの参照される容量を含む）	`storage aggregate show-space`パラメータを指定した場合 `-instance`
ローカル階層に接続されているオブジェクトストアのスペース使用量（ライセンススペースの使用量など）	`storage aggregate object-store show-space`
ローカル階層内のボリュームとそのデータおよびメタデータの容量のリスト	`volume show-footprint`

CLIコマンドに加えて、Active IQ Unified Manager（旧OnCommand Unified Manager）とFabricPool .4以降のクラスタでサポートされるONTAP 9 Advisor、またはSystem Managerを使用してスペース使用量を監視できます。

次の例は、FabricPoolのスペース使用量および関連情報を表示する方法を示しています。

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                      ...
                                                 Aggregate Display Name:
MyFabricPool
                                                                      ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                      ...
                                                          Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                    Total Logical Used
Size: -
                                                    Logical Used
Percentage: -
                                              Logical Unreferenced
Capacity: -
                                            Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
                           ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume : rootvol

Feature                             Used       Used%
--------------------------------- ---------- -----
Volume Footprint                  KB          %
Volume Guarantee                  MB          %
Flexible Volume Metadata          KB          %
Delayed Frees                     KB          %
Total Footprint                   MB          %

Vserver : vs1
Volume : vol

Feature                             Used       Used%
--------------------------------- ---------- -----
Volume Footprint                  KB          %
Footprint in Performance Tier     KB          %
Footprint in Amazon01             KB          %
Flexible Volume Metadata          MB          %
Delayed Frees                     KB          %
Total Footprint                   MB          %
...
```

2. 必要に応じて、次のいずれかの操作を実行します。

状況	そしたら…。
ボリュームの階層化ポリシーを変更する	の手順に従います"ボリュームの階層化ポリシーや階層化の最小クーリング期間の変更によるストレージ階層化の管理"。
FabricPoolライセンスの使用制限を増やす	NetAppまたはパートナーの営業担当者にお問い合わせください。 "NetAppのサポート"
クラウド階層のストレージスペースを拡張する	クラウド階層に使用するオブジェクトストアのプロバイダにお問い合わせください。

関連情報

- "ストレージ集約オブジェクト"
- "storage aggregate show"

- "ストレージアグリゲートショースペース"

ONTAPボリュームの階層化ポリシーと最小クーリング期間を変更する

ボリュームの階層化ポリシーを変更することで、アクセス頻度が低くなったデータ（*COM*）をクラウド階層に移動するかどうかを制御できます。`auto`階層化ポリシーが設定されたボリュームの場合`snapshot-only`、アクセス頻度の低いユーザデータがクラウド階層に移動されるまでの階層化の最小クーリング期間も指定できます。

開始する前に

ボリュームを階層化ポリシーに変更`auto`したり、階層化の最小クーリング期間を変更したりするには、ONTAP 9 .4以降が必要です。

タスクの内容

ボリュームの階層化ポリシーを変更すると、そのボリュームに対する以降の階層化の動作のみ変更されます。変更前までさかのぼってデータがクラウド階層に移動されることはありません。

階層化ポリシーを変更すると、データがコールドと認識されてクラウド階層に移動されるまでの時間に影響することがあります。

"FabricPoolでボリュームの階層化ポリシーを変更した場合の動作"

SVM DR関係では、ソースボリュームとデスティネーションボリュームでFabricPoolアグリゲートを使用する必要はありませんが、同じ階層化ポリシーを使用する必要があります。

手順

1. コマンドでパラメータを指定して`-tiering-policy`、既存のボリュームの階層化ポリシーを変更します`volume modify`。

   次のいずれかの階層化ポリシーを指定できます。

   - `snapshot-only`（デフォルト）
   - `auto`
   - `all`
   - `none`

     "FabricPool階層化ポリシーの種類"

2. ボリュームでまたは`auto`階層化ポリシーを使用している場合`snapshot-only`に階層化の最小クーリング期間を変更するには、`advanced`権限レベルでオプションのパラメータを指定してコマンドを`-tiering-minimum-cooling-days`実行します`volume modify`。

   階層化の最小クーリング日数には2^{183}の値を指定できます。9.8より前のバージョンのONTAPを使用している場合は、2^{63}の値を階層化の最小クーリング日数に指定できます。

ボリュームの階層化ポリシーと階層化の最小クーリング期間の変更例

次の例は、SVM「vs1」内のボリューム「myvol」の階層化ポリシーをに変更し、階層化の最小クーリング期

間を45日に変更します `auto`。

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

Archive volumes with FabricPool（ビデオ）

このビデオでは、System Managerを使用して、FabricPoolでクラウド階層にボリュームをアーカイブする方法の概要を紹介します。

"NetAppのビデオ：Archiving volumes with FabricPool（backup + volume move）"

関連情報

"NetApp TechComm TV ： FabricPool 関連ビデオ"

ONTAPボリュームのデフォルトの**FabricPool**階層化ポリシーを変更する

ONTAP 9で導入されたオプションを使用して、クラウド階層から高パフォーマンス階層へのユーザデータの読み出しを制御するボリュームのデフォルトの階層化ポリシーを変更できます `-cloud-retrieval-policy`。8.

開始する前に

- オプションを使用してボリュームを変更 `-cloud-retrieval-policy`するには、ONTAP 9 .8以降が必要です。
- この処理を実行するには、advanced権限レベルが必要です。
- での階層化ポリシーの動作について理解しておく必要があります `-cloud-retrieval-policy`。

  "階層化ポリシーとクラウド移行との相互運用性"

ステップ

1. コマンドでオプションを指定して `-cloud-retrieval-policy`、既存のボリュームの階層化ポリシーの動作を変更します `volume modify`。

   ```
    volume create -volume <volume_name> -vserver <vserver_name> - tiering-
   policy <policy_name> -cloud-retrieval-policy
   ```

   ```
   vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
   promote
   ```

ONTAP FabricPoolのノードごとの**PUT**レートのしきい値を設定する

ストレージ管理者は、PUTスロットルを使用してノードあたりの最大PUT速度の上限しきい値を設定できます。

PUT throttlingは、ネットワークリソースまたはオブジェクトストアエンドポイントのリソースに制約がある場合に便利です。ごくまれに、パワー不足のオブジェクトストアや、FabricPoolの使用開始日（TBまたはPBのコールドデータの階層化が開始されたとき）にリソースの制約が発生する可能性があります。

PUTスロットルはノード単位です。PUTスロットルのput-rate-limitの最小値は8MB/秒です。put-rate-limitを8MB/秒未満に設定すると、そのノードのスループットは8MB/秒になります。複数のノードを同時に階層化すると、より多くの帯域幅が消費され、非常に限られた容量のネットワークリンクが飽和状態になる可能性があります。

FabricPool PUT処理では、リソースを他のアプリケーションと競合することはありません。FabricPool PUT処理は、クライアントアプリケーションやSnapMirrorなどの他のONTAPワークロードによって自動的に低い優先度（「Bully」）に設定されます。を使用したPUTスロットリングは `put-rate-limit`、FabricPool階層化に関連するネットワークトラフィックを削減する場合に便利ですが、同時に発生するONTAPトラフィックとは関係ありません。

開始する前に

Advanced権限レベルが必要です。

手順

1. ONTAP CLIを使用してFabricPool PUT処理をスロットルします。

```
storage aggregate object-store put-rate-limit modify -node <name>
-default <true|false> -put-rate-bytes-limit <integer>[KB|MB|GB|TB|PB]
```

関連情報

- "ストレージアグリゲートのオブジェクトストアのPUT速度制限の変更"

ONTAP FabricPoolオブジェクトの削除とデフラグをカスタマイズする

FabricPoolは、接続されたオブジェクト ストレージからブロックを削除しません。代わりに、オブジェクト内のブロックの一定の割合がONTAPで参照されなくなった時点で、FabricPoolはオブジェクトを削除します。

たとえば、Amazon S3に階層化された4MBのオブジェクトには、1,024個の4KBブロックがあります。デフラグと削除は、205個未満の4KBブロック（1,024個の20%）がONTAPによって参照されるまで発生しません。十分な数のブロック（1,024個）に参照がない場合、元の4MBオブジェクトが削除され、新しいオブジェクトが作成されます。

再利用されていないスペースのしきい値の割合をカスタマイズして、オブジェクトストアごとに異なるデフォルトレベルに設定できます。デフォルト設定は次のとおりです。

オブジェクト ストア	ONTAP 9.8以降	ONTAP 9.7 から 9.4	ONTAP 9.3以前	Cloud Volumes ONTAP
Amazon S3	20%	20%	0%	30%

Google Cloud Storage	20%	12%	N/A	35%
Microsoft Azure Blob Storage	25%	15%	N/A	35%
NetApp ONTAP S3	40%	N/A	N/A	N/A
NetApp StorageGRID	40%	40%	0%	N/A

解放されていないスペースのしきい値

デフォルトの再利用されていないスペースのしきい値設定を変更すると、オブジェクトの断片化の許容量が増減します。断片化を減らすと、追加のオブジェクトストアリソース（読み取りと書き込み）を犠牲にして、クラウド階層で使用される物理容量が削減されます。

しきい値の削減

追加のコストを回避するには、ストレージ コストを削減しながら読み取りコストを増加させるオブジェクトストレージの価格設定スキームを使用する際に、再利用されないスペースのしきい値を削減することを検討します。たとえば、AmazonのStandard-IAやAzure Blob StorageのCoolなどです。

たとえば、法的な理由で保存された10年前のプロジェクトのボリュームを階層化すると、Standard-IAやCoolなどの価格設定スキームを使用する場合、標準価格設定スキームを使用する場合よりもコストが低くなる可能性があります。このようなボリュームの読み取りは、オブジェクトのデフラグに必要な読み取りも含めて高価ですが、頻繁に発生することはほとんどありません。

しきい値の増加

また、オブジェクトの断片化によってONTAPで参照されるデータに必要以上に多くのオブジェクトストアの容量が使用される場合は、再利用されていないスペースのしきい値を増やすことを検討してください。たとえば、すべてのオブジェクトが最大許容範囲まで均等に断片化されるという最悪のシナリオで再利用されていないスペースのしきい値を20%に設定すると、クラウド階層の合計容量の80%がONTAPで参照されなくなる可能性があります。例：

ONTAPで参照される2TBとONTAPで参照されない8TBを合わせて、クラウド階層で使用される総容量は10TBになります。

この場合は、解放されていないスペースのしきい値を増やすか、ボリュームの最小クーリング日数を増やして、参照されていないブロックで使用される容量を減らすことができます。

システムでオブジェクトがデフラグされてストレージ効率が向上すると、より効率的な新しいオブジェクトに参照ブロックを書き込むことで、基盤となるファイルが断片化される可能性があります。再利用されていないスペースのしきい値を大幅に増やすと、ストレージ効率に優れたオブジェクトを作成できますが、シーケンシャル読み取りのパフォーマンスは低下します。

この追加アクティビティにより、AWS、Azure、Googleなどのサードパーティ S3プロバイダのコストが増加します。

NetAppでは、未解放スペースのしきい値を60%を超えないようにすることを推奨しています。

再利用されていないスペースのしきい値を変更する

オブジェクトストアごとに再利用されていないスペースのしきい値をカスタマイズできます。

開始する前に

Advanced権限レベルが必要です。

手順

1. デフォルトの再利用されていないスペースのしきい値を変更するには、をカスタマイズして次のコマンドを実行します。

```
storage aggregate object-store modify -aggregate <name> -object-store
-name <name> -unreclaimed-space-threshold <%> (0%-99%)
```

関連情報

- "ストレージ集約オブジェクトストア変更"

ONTAPデータを高パフォーマンス階層に昇格

ONTAP 9 8以降では、advanced権限レベルのクラスタ管理者は、との `cloud-retrieval-policy`設定を組み合わせて使用して、クラウド階層からパフォーマンス階層にデータをプロアクティブに昇格できます `tiering-policy`。

タスクの内容

この処理は、ボリュームでFabricPoolの使用を停止する場合や、階層化ポリシーが設定されている場合に、リストアしたSnapshotデータを高パフォーマンス階層に戻す場合に実行します `snapshot-only`。

FabricPoolボリュームのすべてのデータを高パフォーマンス階層に昇格

クラウド階層内のFabricPoolボリューム上のすべてのデータをプロアクティブに読み出して、高パフォーマンス階層に昇格することができます。

手順

1. コマンドを使用して `volume modify` `none`、および `cloud-retrieval-policy`をに `promote`設定し `tiering-policy`ます。

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

ファイルシステムのデータを高パフォーマンス階層に昇格

クラウド階層内のリストアされたSnapshotからアクティブなファイルシステムのデータをプロアクティブに読み出して、高パフォーマンス階層に昇格することができます。

手順

1. コマンドを使用して `volume modify` `snapshot-only`、および `cloud-retrieval-policy`をに `promote`設定し `tiering-policy`ます。

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

高パフォーマンス階層への昇格ステータスの確認

高パフォーマンス階層への昇格ステータスを確認して、処理がいつ完了するかを確認できます。

手順

1. volume `object-store`コマンドにオプションを指定して `tiering`、高パフォーマンス階層への昇格のステータスを確認します。

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                  Vserver: vs1
                                   Volume: v1
                                Node Name: node1
                              Volume DSID: 1023
                           Aggregate Name: a1
                                    State: ready
                      Previous Run Status: completed
                Aborted Exception Status: -
              Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                Scanner Percent Complete: -
                     Scanner Current VBN: -
                        Scanner Max VBNs: -
     Time Waiting Scan will be scheduled: -
                          Tiering Policy: snapshot-only
    Estimated Space Needed for Promotion: -
                       Time Scan Started: -
  Estimated Time Remaining for scan to complete: -
                   Cloud Retrieve Policy: promote
```

スケジュールされた移行と階層化を開始

ONTAP 9 8以降では、デフォルトの階層化スキャンを待たずにいつでも階層化スキャン要求をトリガーできます。

手順

1. 移行と階層化を要求するには、 `volume object-store`コマンドにオプションを指定し `trigger`ます。

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

FabricPoolミラーを管理します。

ONTAP FabricPoolミラーの詳細

災害発生時にデータストア内のデータへのアクセスを確保し、データストアの交換を可能にするために、2つ目のデータストアを追加してFabricPoolミラーを構成し、2つのデータストアにデータを同期的に階層化することができます。新規または既存のFabricPool構成に2つ目のデータストアを追加したり、ミラーのステータスを監視したり、FabricPoolミラーの詳細を表示したり、ミラーを昇格させたり、ミラーを削除したりできます。ONTAP 9.7以降が実行されている必要があります。

ONTAP FabricPoolミラーの作成

FabricPool ミラーを作成するには、 2 つのオブジェクトストアを 1 つの FabricPool に接続します。FabricPool ミラーを作成するには、既存の単一のオブジェクトストア FabricPool 構成に 2 つ目のオブジェクトストアを接続するか、新しい単一のオブジェクトストア FabricPool 構成を作成してから 2 つ目のオブジェクトストアを接続します。MetroCluster 構成上に FabricPool ミラーを作成することもできます。

開始する前に

- コマンドを使用して、2つのオブジェクトストアを作成しておく必要があります `storage aggregate object-store config`。
- MetroCluster 構成上に FabricPool ミラーを作成する場合の要件は次のとおりです。
  - MetroCluster のセットアップと設定が完了している必要があります
  - 選択したクラスタにオブジェクトストア設定を作成しておく必要があります。

    MetroCluster 構成の両方のクラスタに FabricPool ミラーを作成する場合は、両方のクラスタにオブジェクトストア設定を作成しておく必要があります。

  - MetroCluster 構成にオンプレミスのオブジェクトストアを使用しない場合は、次のいずれかのシナリオに該当する必要があります。
    - オブジェクトストアは異なるアベイラビリティゾーンにあります
    - オブジェクトストアは、複数のアベイラビリティゾーンにオブジェクトのコピーを保持するように設定されます

      "MetroCluster構成でのFabricPool用オブジェクトストアのセットアップ"

タスクの内容

FabricPool ミラーには、プライマリオブジェクトストアとは別のオブジェクトストアを使用する必要があります。

FabricPool ミラーを作成する手順は、 MetroCluster 構成と MetroCluster 以外の構成で同じです。

手順

1. 既存のFabricPool設定を使用しない場合は、コマンドを使用してローカル階層にオブジェクトストアを接続して新しい設定を作成し `storage aggregate object-store attach`ます。

   この例では、オブジェクトストアをローカル階層に接続して新しいFabricPoolを作成します。

   ```
   cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
   my-store-1
   ```

2. コマンドを使用して、ローカル階層に2つ目のオブジェクトストアを接続し `storage aggregate object-store mirror`ます。

   この例では、2つ目のオブジェクトストアをローカル階層に接続してFabricPoolミラーを作成します。

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

関連情報

- "ストレージ集約オブジェクトストアアタッチ"
- "ストレージ集約オブジェクトストア構成"
- "ストレージ集約オブジェクトストアミラー"

ONTAP FabricPoolミラーの詳細を表示します。

FabricPool ミラーの詳細を表示して、設定に含まれているオブジェクトストアや、オブジェクトストアミラーがプライマリオブジェクトストアと同期されているかどうかを確認できます。

ステップ

1. コマンドを使用して、FabricPoolミラーに関する情報を表示します `storage aggregate object-store show`。

   次の例は、 FabricPool ミラーのプライマリオブジェクトストアとミラーオブジェクトストアの詳細を表示します。

```
cluster1::> storage aggregate object-store show
```

```
Aggregate      Object Store Name Availability    Mirror Type
-------------- ----------------- -------------   ----------
aggr1          my-store-1        available       primary
               my-store-2        available       mirror
```

   次の例は、再同期処理によってミラーがデグレード状態になっているかどうかを含む、 FabricPool ミラーに関する詳細を表示します。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-store-1        primary           -
               my-store-2        mirror          false
```

関連情報

- "ストレージ集約オブジェクトストア表示"

ONTAP FabricPoolミラーの昇格

オブジェクトストアミラーを昇格してプライマリオブジェクトストアとして再割り当てすることができます。オブジェクトストアミラーがプライマリになると、元のプライマリは自動的にミラーになります。

開始する前に

- FabricPool ミラーが同期されている必要があります
- オブジェクトストアが動作している必要があります

タスクの内容

元のオブジェクトストアを別のクラウドプロバイダのオブジェクトストアに置き換えることができます。たとえば、元のミラーが AWS オブジェクトストアである場合に Azure オブジェクトストアに置き換えることができます。

手順

1. コマンドを使用して、FabricPoolミラーが同期されていることを確認します `storage aggregate object-store show-resync-status`。FabricPool ミラーが同期されている場合はエントリは表示されません。ミラーが同期されていない場合は、再同期が完了するまで待ちます。

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

```
                                          Complete
Aggregate    Primary       Mirror         Percentage
---------    -----------   ----------     ----------
aggr1        my-store-1     my-store-2      40%
```

2. コマンドを使用して、オブジェクトストアミラーを昇格し `storage aggregate object-store modify -aggregate`ます。

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-store-2 -mirror-type primary
```

関連情報

- "ストレージ集約オブジェクトストア変更"
- "ストレージ集約オブジェクトストアの再同期ステータスの表示"

ONTAP FabricPoolミラーの削除

オブジェクトストアをレプリケートする必要がなくなった場合は、 FabricPool ミラーを

削除できます。

開始する前に

プライマリオブジェクトストアが動作している必要があります。動作していないとコマンドは失敗します。

ステップ

1. コマンドを使用して、FabricPoolのオブジェクトストアミラーを削除します `storage aggregate object-store unmirror -aggregate`。

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

関連情報

- "ストレージ集約オブジェクトストアミラー解除"

既存のオブジェクトストアを**ONTAP FabricPool**ミラーに置き換える

FabricPool ミラーテクノロジを使用して、あるオブジェクトストアを別のオブジェクトストアに置き換えることができます。新しいオブジェクトストアは、元のオブジェクトストアと同じクラウドプロバイダを使用する必要はありません。

タスクの内容

元のオブジェクトストアを、別のクラウドプロバイダを使用するオブジェクトストアに置き換えることができます。たとえば、 AWS をクラウドプロバイダとして使用しているオブジェクトストアが Azure を使用するオブジェクトストアに置き換えることも、その逆も可能です。ただし、オブジェクトサイズは新しいオブジェクトストアと元のオブジェクトストアで同じである必要があります。

手順

1. コマンドを使用して、既存のFabricPoolに新しいオブジェクトストアを追加し、FabricPoolミラーを作成し `storage aggregate object-store mirror`ます。

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. コマンドを使用して、ミラー再同期ステータスを監視し `storage aggregate object-store show-resync-status`ます。

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                                  Complete
Aggregate    Primary          Mirror          Percentage
---------    -----------      ----------      ----------
aggr1        my-AWS-store     my-AZURE-store      40%
```

3. コマンドを使用して、ミラーが同期されていることを確認します `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded`。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. コマンドを使用して、プライマリオブジェクトストアをミラーオブジェクトストアとスワップします `storage aggregate object-store modify`。

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. コマンドを使用して、FabricPoolミラーに関する詳細を表示します `storage aggregate object-store show -fields mirror-type,is-mirror-degraded`。

   この例は、 FabricPool ミラーに関する情報を表示したもので、ミラーがデグレード状態（同期されていない状態）になっているかどうかも含まれます。

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. コマンドを使用して、FabricPoolミラーを削除します `storage aggregate object-store unmirror`。

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. コマンドを使用して、FabricPoolが単一のオブジェクトストア設定に戻ったことを確認します `storage aggregate object-store show -fields mirror-type,is-mirror-degraded`。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

関連情報

- "ストレージ集約オブジェクトストアミラー"
- "ストレージ集約オブジェクトストア変更"
- "ストレージ集約オブジェクトストアの再同期ステータスの表示"
- "ストレージ集約オブジェクトストア表示"
- "ストレージ集約オブジェクトストアミラー解除"

ONTAP MetroCluster構成でのFabricPoolミラーの交換

MetroCluster ミラーのオブジェクトストアの 1 つが破棄された場合、または FabricPool 構成で完全に使用できなくなった場合、オブジェクトストアがまだミラーでない場合はミラーにして、破損したオブジェクトストアを FabricPool ミラーから削除します。 次に、新しいオブジェクトストアミラーを FabricPool に追加します。

手順

1. 破損したオブジェクトストアがまだミラーでない場合は、コマンドを使用してオブジェクトストアをミラーにします `storage aggregate object-store modify`。

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mcc1_ostore1 -mirror-type mirror
```

2. コマンドを使用して、FabricPoolからオブジェクトストアミラーを削除します `storage aggregate object-store unmirror`。

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mcc1_ostore1
```

3. ミラーデータストアを削除したあとに、オプションを指定して `-force-tiering-on-metrocluster true`を使用すると、プライマリデータストアで階層化を強制的に再開でき `storage aggregate object-store modify`ます。

   ミラーがないと、 MetroCluster 構成のレプリケーション要件が満たされません。

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. コマンドを使用して、置き換え用のオブジェクトストアを作成し `storage aggregate object-store config create`ます。

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. コマンドを使用して、FabricPoolミラーにオブジェクトストアミラーを追加します `storage aggregate object-store mirror`。

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. コマンドを使用して、オブジェクトストアの情報を表示します `storage aggregate object-store show`。

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary           -
               mcc1_ostore3-mc    mirror          true
```

7. コマンドを使用して、ミラー再同期ステータスを監視し `storage aggregate object-store show-resync-status`ます。

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                                    Complete
Aggregate    Primary         Mirror           Percentage
---------    -----------     ----------       ----------
aggr1        mcc1_ostore1-mc mcc1_ostore3-mc    40%
```

関連情報

- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストアミラー"
- "ストレージ集約オブジェクトストア変更"
- "ストレージ集約オブジェクトストア表示"
- "ストレージ集約オブジェクトストアの再同期ステータスの表示"
- "ストレージ集約オブジェクトストアミラー解除"

FabricPoolリソースを管理するためのONTAPコマンド

FabricPoolのオブジェクトストアを管理するには、コマンドを使用し`storage aggregate object-store`ます。FabricPoolのアグリゲートを管理するには、コマンドを使用し`storage aggregate`ます。FabricPoolのボリュームを管理するには、コマンドを使用し`volume`ます。

状況	使用するコマンド
オブジェクトストアの設定を定義して、ONTAPからアクセスできるようにする	`storage aggregate object-store config create`
オブジェクトストア設定の属性を変更する	`storage aggregate object-store config modify`
既存のオブジェクトストア設定の名前を変更する	`storage aggregate object-store config rename`
オブジェクトストアの設定を削除する	`storage aggregate object-store config delete`
オブジェクトストア設定のリストを表示する	`storage aggregate object-store config show`
新規または既存のFabricPoolにミラーとして2つ目のオブジェクトストアを接続する	`storage aggregate object-store mirror`（admin権限レベルでパラメータと`-name`パラメータを指定） `-aggregate`

既存のFabricPoolミラーからオブジェクトストアミラーを削除する	`storage aggregate object-store unmirror`（admin権限レベルでパラメータと `-name` パラメータを指定） `-aggregate`
FabricPoolミラー再同期ステータスを監視する	`storage aggregate object-store show-resync-status`
FabricPoolミラーの詳細を表示します。	`storage aggregate object-store show`
FabricPoolミラー構成でオブジェクトストアミラーを昇格してプライマリオブジェクトストアと置き換える	`storage aggregate object-store modify`（admin権限レベルでパラメータを指定） `-aggregate`
オブジェクトストアをアグリゲートに接続せずにオブジェクトストアのレイテンシとパフォーマンスをテストする	`storage aggregate object-store profiler start`（advanced権限レベルでパラメータと `-node` パラメータを指定） `-object-store-name`
オブジェクトストアプロファイラのステータスを監視する	`storage aggregate object-store profiler show`（advanced権限レベルでパラメータと `-node` パラメータを指定） `-object-store-name`
実行中のオブジェクトストアプロファイラを中止する	`storage aggregate object-store profiler abort`（advanced権限レベルでパラメータと `-node` パラメータを指定） `-object-store-name`
FabricPoolを使用するためにオブジェクトストアをアグリゲートに接続する	`storage aggregate object-store attach`
FabricPoolを使用するために、FlexGroupボリュームが含まれるアグリゲートにオブジェクトストアを接続する	`storage aggregate object-store attach` を使用して `allow-flexgroup true`
FabricPool対応アグリゲートに接続されているオブジェクトストアの詳細を表示する	`storage aggregate object-store show`
階層化スキャンで使用されるアグリゲートのスペース不足しきい値を表示する	`storage aggregate object-store show`（advanced権限レベルでパラメータを指定） `-fields tiering-fullness-threshold`
FabricPool対応アグリゲートに接続されているオブジェクトストアのスペース使用量を表示する	`storage aggregate object-store show-space`

FabricPoolに使用されていないアグリゲートでInactive Data Reportingを有効にする	`storage aggregate modify`パラメータを指定した場合 `-is-inactive-data-reporting-enabled true`
アグリゲートでアクセス頻度の低いデータのレポートが有効になっているかどうかを表示する	`storage aggregate show`パラメータを指定した場合 `-fields is-inactive-data-reporting-enabled`
アグリゲート内のコールドユーザデータの量に関する情報を表示する	`storage aggregate show-space`パラメータを指定した場合 `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent`
次の項目を指定して、FabricPool用のボリュームを作成します。 • 階層化ポリシー • 階層化の最小クーリング期間（`snapshot-only`または`auto`階層化ポリシー）	`volume create` • パラメータを使用して `-tiering-policy`、階層化ポリシーを指定します。 • 階層化の最小クーリング期間を指定するには、advanced権限レベルでパラメータを使用し`-tiering-minimum-cooling-days`ます。
FabricPoolのボリュームを変更し、次の項目を変更します。 • 階層化ポリシー • 階層化の最小クーリング期間（`snapshot-only`または`auto`階層化ポリシー）	`volume modify` • パラメータを使用して `-tiering-policy`、階層化ポリシーを指定します。 • 階層化の最小クーリング期間を指定するには、advanced権限レベルでパラメータを使用し`-tiering-minimum-cooling-days`ます。
ボリュームに関連するFabricPool情報を表示します。これには次のような情報が含まれます。 • 階層化の最小クーリング期間 • コールドユーザデータの量	`volume show` • 階層化の最小クーリング期間を表示するには、advanced権限レベルでパラメータを使用し`-fields tiering-minimum-cooling-days`ます。 • コールドユーザデータの量を表示するには、パラメータを使用し`-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent`ます。
FabricPoolとの間でボリュームを移動する	`volume move start`オプションのパラメータを使用して `-tiering-policy`、ボリュームの階層化ポリシーを指定します。
FabricPoolの参照されていないスペースを再生するしきい値（デフラグしきい値）を変更する	`storage aggregate object-store modify`（advanced権限レベルでパラメータを指定）`-unreclaimed-space-threshold`

階層化スキャンがFabricPoolのデータの階層化を開始する前に、アグリゲートの使用率のしきい値を変更する FabricPoolは、ローカル階層の容量が98%に達するまで、コールドデータをクラウド階層に階層化し続けます。	`storage aggregate object-store modify`（advanced権限レベルでパラメータを指定）`-tiering-fullness-threshold`
FabricPoolで参照されていないスペースを再生するしきい値を表示する	`storage aggregate object-store show`または `storage aggregate object-store show-space`コマンド（advanced権限レベルでパラメータを指定） `-unreclaimed-space-threshold`

関連情報

- "storage aggregate modify"
- "ストレージ集約オブジェクト"
- "ストレージアグリゲートショースペース"

SVMのデータ移動

SVMのデータ移動の概要

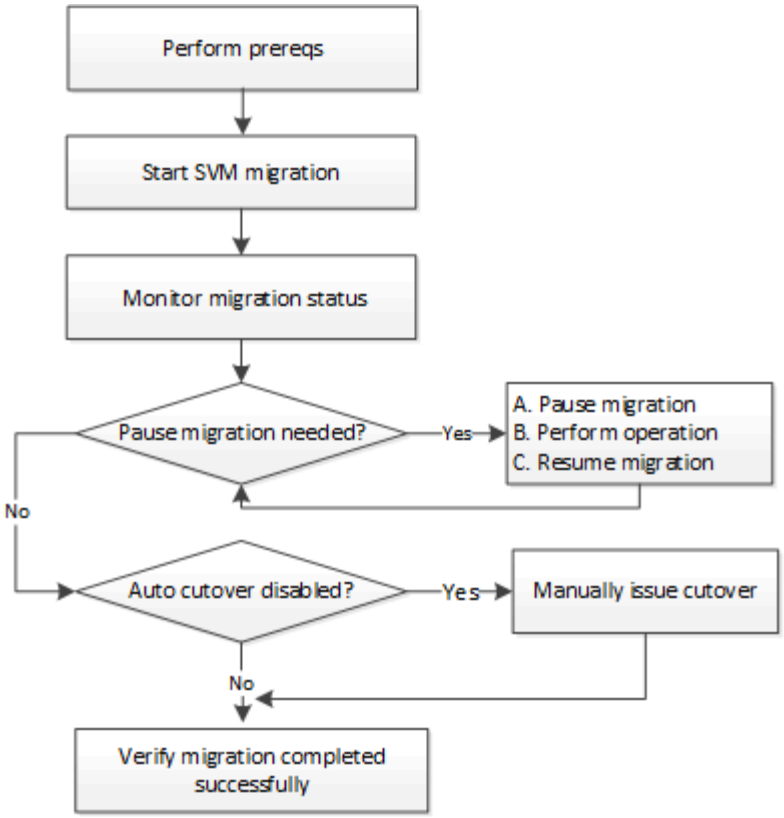
ONTAP 9 .10.1以降では、ONTAP CLIを使用して、容量とロードバランシングを管理したり、機器のアップグレードやデータセンターの統合を有効にしたりするために、SVMをシステムを停止することなくソースクラスタからデスティネーションクラスタに再配置できます。

この無停止のSVM再配置機能は、ONTAP 9 .10.1および9.11.1のAFFプラットフォームでサポートされます。ONTAP 9 12.1以降では、この機能はFASプラットフォームとAFFプラットフォームの両方、およびハイブリッドアグリゲートでサポートされます。

SVMの名前とUUIDは移行後も変更されず、データLIF名、IPアドレス、およびオブジェクト名（ボリューム名など）も変更されません。SVM内のオブジェクトのUUIDは異なります。

SVM移行ワークフロー

次の図は、SVMの移行の一般的なワークフローを示しています。SVMの移行はデスティネーションクラスタから開始します。移行はソースとデスティネーションのどちらからでも監視できます。手動カットオーバーと自動カットオーバーのどちらも実行できます。自動カットオーバーはデフォルトで実行されます。



SVM移行プラットフォームのサポート

コントローラファミリー	サポートされるONTAPのバージョン
AFF Aシリーズ	ONTAP 9.10.1以降
AFF Cシリーズ	ONTAP 9.12.1パッチ4以降
FAS	ONTAP 9.12.1以降

AFFクラスタからハイブリッドアグリゲートを使用するFASクラスタに移行する場合、ボリュームの自動配置で同様のアグリゲートの一致が試行されます。たとえば、ソースクラスタにボリュームが60個ある場合、ボリュームの配置では、ボリュームを配置するデスティネーションにAFFアグリゲートが検索されます。AFFアグリゲートに十分なスペースがない場合、ボリュームはフラッシュディスク以外のアグリゲートに配置されます。

ONTAPのバージョン別の拡張性サポート

ONTAPのバージョン	ソースとデスティネーションのHAペア
ONTAP 9 .14.1	12
ONTAP 9 .13.1	6
ONTAP 9 .11.1	3
ONTAP 9 10.1	1

ソースクラスタとデスティネーションクラスタ間の**TCP**ラウンドトリップタイム（**RTT**）に関するネットワークインフラのパフォーマンス要件

クラスタにインストールされているONTAPのバージョンに応じて、ソースクラスタとデスティネーションクラスタを接続するネットワークの最大応答時間を次に示します。

ONTAPのバージョン	最大RTT
ONTAP 9.12.1以降	10ミリ秒
ONTAP 9.11.1以前	2ミリ秒

SVMあたりのサポートされる最大ボリューム数

ソース	デスティネーション	ONTAP 9 .14.1	ONTAP 9 .13.1	ONTAP 9 12.1	ONTAP 9.11.1以前
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	N/A
FAS	AFF	80	80	80	N/A
AFF	FAS	80	80	80	N/A

前提条件

SVMの移行を開始する前に、次の前提条件を満たしている必要があります。

- クラスタ管理者である必要があります。
- "ソースクラスタとデスティネーションクラスタが相互にピア関係にある必要があります"です。
- ソースクラスタとデスティネーションクラスタでSnapMirrorが同期されている必要があり"インストールされたライセンス"ます。このライセンスはに含まれてい"ONTAP One"ます。
- ソースクラスタのすべてのノードでONTAP 9 .10.1以降が実行されている必要があります。特定のONTAPアレイコントローラのサポートについては、を参照してください"Hardware Universe"。
- ソースクラスタ内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。
- デスティネーションクラスタ内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。
- デスティネーションクラスタのONTAPのバージョンは、ソースクラスタと同じか、新しいメジャーバージョンが2つ以下である必要があります。
- ソースクラスタとデスティネーションクラスタで、データLIFへのアクセス用に同じIPサブネットがサポートされている必要があります。
- ソースSVMに含まれているボリュームの数がよりも少ない必要がありこのリリースでサポートされるデータボリュームの最大数ます。
- ボリュームを配置するための十分なスペースが宛先に必要です。
- ソース SVM に暗号化されたボリュームがある場合は、オンボード キー マネージャまたは外部キー管理をデスティネーションのクラスタ レベルで設定する必要があります。
  - この場合、ソースのSVMレベルで設定されたキーマネージャはデスティネーションに移行されません。デスティネーションではクラスタレベルのキーマネージャが使用されます。

- ソースに暗号化されたボリュームがあり、 NetApp Aggregate Encryption (NAE) 用に構成されている場合は、宛先も NAE 用に構成する必要があります。
- MetroCluster以外の構成とMetroCluster構成の間、または2つのMetroCluster構成の間でSVMを移行する場合は、構成が次の要件を満たしていることを確認します。
  - ソースとデスティネーションのMetroClusterクラスタは「normal」状態です。そのため、スイッチオーバーモードや「waiting-for-switchback」状態になることはできません。
  - ソースとデスティネーションのMetroClusterクラスタでFCからIPへの移行やハードウェアの更新を実行中ではありません。
  - ソース クラスタと宛先クラスタの両方でONTAP 9.16.1 以降が実行されている必要があります。
  - ソースがMetroClusterクラスタの場合、SVMのサブタイプは「sync-source」です（「sync-destination」ではありません）。

> デスティネーションがMetroClusterクラスタの場合、デスティネーションに作成されるSVMは常に「sync-source」になります。デスティネーションがMetroCluster以外のクラスタの場合、SVMサブタイプは常に「default」です。

ベストプラクティス

SVM移行を実行するときは、CPUワークロードが実行されるように、ソースクラスタとデスティネーションクラスタの両方にCPUヘッドルームを30%確保しておくことを推奨します。

SVMの処理

SVMの移行と競合する可能性がある以下の処理が実行中でないことを確認する必要があります。

- フェイルオーバー処理
- wafliron
- フィンガープリント処理
- ボリュームの移動、リホスト、クローニング、作成、変換、または分析

サポート対象の機能とサポート対象外の機能

次の表に、SVMのデータ移動でサポートされるONTAP機能とサポートが利用可能なONTAPリリースを示します。

SVM移行におけるソースとデスティネーション間のONTAPのバージョンの相互運用性については、を参照してください"SnapMirror関係に互換性があるONTAPのバージョン"。

機能	最初にサポートされたリリース	コメント
自律型ランサムウェア対策	ONTAP 9 12.1	
Cloud Volumes ONTAP	サポート対象外	

外部キー管理ツール	ONTAP 9 .11.1	
FabricPool	サポート対象外	
ファンアウト関係（移行するソースにSnapMirrorソースボリュームと複数のデスティネーションがある）	ONTAP 9 .11.1	
FC SAN	サポート対象外	
Flash Pool	ONTAP 9 12.1	
FlexCacheホリユウム	サポート対象外	
FlexGroup	サポート対象外	
IPSecポリシー	サポート対象外	
IPv6 LIF	サポート対象外	
iSCSI SAN	サポート対象外	
ジョブスケジュールのレプリケーション	ONTAP 9 .11.1	ONTAP 9 .10.1では、移行時にジョブスケジュールはレプリケートされないため、デスティネーションで手動で作成する必要があります。ONTAP 9 .11.1以降では、ソースで使用されるジョブスケジュールが移行時に自動的にレプリケートされます。
負荷共有ミラー	サポート対象外	

MetroCluster SVM	ONTAP 9 .16.1	ONTAP 9.16.1以降では、次のMetroCluster SVM移行がサポートされます。 • MetroCluster以外の構成とMetroCluster IP構成の間でのSVMの移行 • 2つのMetroCluster IP構成間でのSVMの移行 • MetroCluster FC構成とMetroCluster IP構成間でのSVMの移行 注: SVM の移行をサポートするには、ソース クラスタと宛先クラスタの両方でONTAP 9.16.1 以降が実行されている必要があります。 MetroCluster SVMの次の移行は、すべてのバージョンのONTAPでサポートされるわけではありません。 • 2つのMetroCluster FC構成間でのSVMの移行 • MetroCluster以外の構成とMetroCluster FC構成間でのSVMの移行 参照前提条件 MetroCluster構成で SVM を移行します。
NetAppアグリゲート暗号化（NAE）	ONTAP 9 .11.1	NAEボリュームは、サポートするデスティネーションのNAEに配置する必要があります。使用可能なNAEデスティネーションがない場合、移行処理は失敗します。
NDMP構成	サポート対象外	
NetAppボリューム暗号化（NVE）	ONTAP 9 10.1	NVEボリュームは、デスティネーションにNVEボリュームとしてマイグレートされます。
NFSトSMBカンサロク	ONTAP 9 .13.1	ⓘ 監査を有効にしたオンプレミスのSVM移行の場合は、ソースSVMで監査を無効にしてから移行を実行する必要があります。 SVM移行前： • "デスティネーションクラスタで監査ログリダイレクトを有効にする必要がある"です。 • "ソースSVMからの監査ログデスティネーションパスがデスティネーションクラスタに作成されている必要があります。"です。
NFS v3、NFS v4.1、NFS v4.2	ONTAP 9 10.1	

NFS v4.0	ONTAP 9 12.1	
pNFSを使用したNFSv4.1	ONTAP 9 .14.1	
NVMe over Fabric	サポート対象外	
ソースクラスタでCommon Criteriaモードを有効にしたオンボードキーマネージャ（OKM）	サポート対象外	
qtree	ONTAP 9 .14.1	
クォータ	ONTAP 9 .14.1	
S3	サポート対象外	
SMBプロトコル	ONTAP 9 12.1	SMBの移行にはシステムの停止が伴い、移行後にクライアントの更新が必要になります。
SnapMirrorのクラウド関係	ONTAP 9 12.1	ONTAP 9 12.1以降では、SnapMirrorクラウド関係が確立されたオンプレミスのSVMを移行する場合、デスティネーションクラスタにがインストールされており、クラウドにミラーリングされるボリューム内の容量の移動に対応できる十分な容量がデスティネーションクラスタに"SnapMirrorクラウドライセンス"必要です。
SnapMirror非同期デスティネーション	ONTAP 9 12.1	

SnapMirror非同期ソース	ONTAP 9 .11.1	• FlexVol SnapMirror関係では、ほとんどの移行中も転送を通常どおり継続できます。 • 実行中の転送はカットオーバー中にキャンセルされ、カットオーバー中に新しい転送は失敗し、移行が完了するまで再開できません。 • 移行中にキャンセルされた、または実行されなかったスケジュールされた転送は、移行完了後に自動的には開始されません。 SnapMirrorソースを移行した場合、ONTAPでは、SnapMirrorの更新が実行されるまで、移行後のボリュームの削除は禁止されません。これは、移動されたSnapMirrorソースボリュームのSnapMirror関連情報を確認できるのは、移動が完了して最初の更新が実行されたあとに限られるためです。
SMTape設定	サポート対象外	
SnapLock	サポート対象外	
SnapMirrorアクティブ同期	サポート対象外	
SnapMirror SVMピア関係	ONTAP 9 12.1	
SnapMirror SVMディザスタリカバリ	サポート対象外	
SnapMirror同期	サポート対象外	
スナップショット	ONTAP 9 10.1	
改ざん防止スナップショットロック	ONTAP 9 .14.1	改ざん防止スナップショットロックは、SnapLockと同等ではありません。SnapLock Enterpriseとの SnapLock Complianceはサポートされていません。
仮想IP LIF / BGP	サポート対象外	
Virtual Storage Console 7.0以降	サポート対象外	
ホリユウムクロン	サポート対象外	

vStorage	サポート対象外	vStorageが有効な場合、移行は許可されません。移行を実行するには、vStorageオプションを無効にしてから、移行の完了後に再度有効にします。

移行中にサポートされる処理

次の表は、移行中のSVMにおけるボリュームの各種処理がサポートされるかどうかを、移行状態別に示したものです。

ボリューム操作	SVMの移行状態		
	* 実行中 *	一時停止	* カットオーバー *
作成	不可	許容	サポート対象外
削除	不可	許容	サポート対象外
ファイルシステム分析の無効化	許容	許容	サポート対象外
ファイルシステム分析の有効化	不可	許容	サポート対象外
変更	許容	許容	サポート対象外
オフライン/オンライン	不可	許容	サポート対象外
移動/リホスト	不可	許容	サポート対象外
qtreeの作成/変更	不可	許容	サポート対象外
クォータの作成/変更	不可	許容	サポート対象外
名前変更	不可	許容	サポート対象外
サイズ変更	許容	許容	サポート対象外
制限	不可	許容	サポート対象外
Snapshot属性の変更	許容	許容	サポート対象外
Snapshotの自動削除の変更	許容	許容	サポート対象外
Snapshotの作成	許容	許容	サポート対象外
Snapshotの削除	許容	許容	サポート対象外
Snapshotからファイルをリストア	許容	許容	サポート対象外

SVMの移行

SVMの移行が完了すると、クライアントはデスティネーションクラスタに自動的にカットオーバーされ、不要なSVMはソースクラスタから削除されます。自動カットオーバーとソースの自動クリーンアップはデフォルトで有効になっています。必要に応じて、クライアントの自動カットオーバーを無効にしてカットオーバーが発生する前に移行を一時停止したり、ソースSVMの自動クリーンアップを無効にしたりできます。

- オプションを使用すると `-auto-cutover false`、クライアントの自動カットオーバーが通常どおり実行されたときに移動を一時停止し、あとで手動でカットオーバーを実行できます。

  SVM移行後のクライアントの手動カットオーバー

- advanced権限オプションを使用すると、カットオーバー後にソースSVMの削除を無効にし、カットオーバー後にソースのクリーンアップを手動で実行できます `-auto-source-cleanup false`。

  カットオーバー後のソースSVMの手動削除

自動カットオーバーを有効にして**SVM**を移行する

デフォルトでは、クライアントは移行の完了時に自動的にデスティネーションクラスタにカットオーバーされ、不要なSVMはソースクラスタから削除されます。

手順

1. デスティネーションクラスタから、移行の事前確認を実行します。

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. デスティネーションクラスタから、SVMの移行を開始します。

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name
   ```

3. 移行ステータスを確認します。

   ```
   dest_cluster> vserver migrate show
   ```

   SVMの移行が完了すると、ステータスにmigrate-completeと表示されます。

自動クライアントカットオーバーを無効にして**SVM**を移行する

auto-cutover falseオプションを使用すると、クライアントの自動カットオーバーが正常に実行されたときに移行を一時停止し、あとで手動でカットオーバーを実行できます。を参照して SVM移行後のクライアントの手動カットオーバー

手順

1. デスティネーションクラスタから、移行の事前確認を実行します。

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. デスティネーションクラスタから、SVMの移行を開始します。

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-cutover false
   ```

3. 移行ステータスを確認します。

   `dest_cluster> vserver migrate show`SVM移行が非同期データ転送を完了し、カットオーバー処理の準備が完了すると、ステータスに「カットオーバー準備完了」と表示されます。

ソースのクリーンアップを無効にして**SVM**を移行する

advanced権限-auto-source-cleanup falseオプションを使用すると、カットオーバー後にソースSVMの削除を無効にし、カットオーバー後にソースのクリーンアップを手動でトリガーできます。を参照して ソースSVMを手動で削除する

手順

1. デスティネーションクラスタから、移行の事前確認を実行します。

   ```
   dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. デスティネーションクラスタから、SVMの移行を開始します。

   ```
   dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-source-cleanup false
   ```

3. 移行ステータスを確認します。

   ```
   dest_cluster*> vserver migrate show
   ```

   SVM移行のカットオーバーが完了し、ソースクラスタからSVMを削除できる状態になると、ステータスにready-for-source-cleanupと表示されます。

ボリューム移行の監視

コマンドを使用してSVMの移行全体を監視するだけでなく `vserver migrate show` 、SVMに含まれるボリュームの移行ステータスも監視できます。

手順

1. ボリュームの移行ステータスを確認します。

   ```
   dest_clust> vserver migrate show-volume
   ```

SVM 移行を一時停止して再開します

移行のカットオーバーを開始する前に、SVMの移行を一時停止できます。コマンドを使用して、SVMの移行を一時停止できます `vserver migrate pause`。

移行を一時停止

コマンドを使用すると、クライアントカットオーバーを開始する前にSVMの移行を一時停止できます `vserver migrate pause`。

移行操作の実行中は、一部の設定変更が制限されます。ただし、ONTAP 9 12.1以降では、移行を一時停止して一部の制限された設定および一部の失敗した状態を修正することで、障害の原因となった可能性のある設定の問題を修正できます。SVMの移行を一時停止するときに解決できる失敗状態には、次のようなものがあります。

- `setup-configuration-failed`
- `migrate-failed`

手順

1. デスティネーションクラスタから、移行を一時停止します。

```
vserver migrate pause -vserver <vserver name>
```

移行を再開する

一時停止したSVMの移行を再開する準備ができたら、またはSVMの移行が失敗した場合は、コマンドを使用できます `vserver migrate resume`。

手順

1. デスティネーションクラスタで次の手順を実行します。
   a. SVMの移行を再開します。

```
vserver migrate resume
```

   b. SVMの移行が再開されたことを確認し、進捗状況を監視します。

```
vserver migrate show
```

SVMの移行をキャンセルする

SVMの移行が完了する前にキャンセルする必要がある場合は、 `vserver migrate abort`指示。SVM移行をキャンセルできるのは、処理が一時停止状態または障害状態にある場合だけです。ステータスが「カットオーバー開始」の場合、またはカットオーバーが完了した後は、SVM の移行をキャンセルできません。は使用できません `abort`SVM 移行の進行中のオプション。

手順

1. 移行ステータスを確認します。

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. 移行をキャンセルします。

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

3. キャンセル処理の進捗を確認します。

```
dest_cluster> vserver migrate show
```

キャンセル処理の実行中は、移行ステータスにmigrate-abortingと表示されます。キャンセル処理が完了すると、移行ステータスには何も表示されません。

クライアントの手動カットオーバー

デフォルトでは、デスティネーションクラスタへのクライアントカットオーバーは、SVM移行が「ready-for-cutover」状態になったあとに自動的に実行されます。クライアントの自動カットオーバーを無効にする場合は、クライアントのカットオーバーを手動で実行する必要があります。

手順

1. クライアントカットオーバーを手動で実行します。

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. カットオーバー処理のステータスを確認します。

```
dest_cluster> vserver migrate show
```

クライアントのカットオーバー後にソース**SVM**を手動で削除する

ソースのクリーンアップを無効にしてSVMの移行を実行した場合は、クライアントのカットオーバーの完了後にソースSVMを手動で削除できます。

手順

1. ソースのクリーンアップの準備が完了していることを確認します。

```
dest_cluster> vserver migrate show
```

2. ソースをクリーンアップします。

```
dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
```

HAペアの管理

ONTAPクラスタにおける**HA**ペア管理について学ぶ

クラスタノードは、フォールトトレランスとノンストップオペレーションを実現するためにハイアベイラビリティ（HA）ペアで構成されます。ノードに障害が発生した場合や定期的なメンテナンスのためにノードを停止する必要がある場合は、パートナーがストレージをテイクオーバーしてデータの提供を継続できます。ノードがオンラインに戻ったら、パートナーはストレージをギブバックします。

HAペアコントローラ構成は、対応するFAS / AFFストレージコントローラ（ローカルノードとパートナーノード）のペアで構成されます。これらの各ノードは、もう一方のディスクシェルフに接続されます。HAペアの一方のノードでエラーが発生してデータの処理が停止すると、障害が発生したパートナーのステータスが検出

され、そのコントローラからすべてのData Processingがテイクオーバーされます。

_Takeover は、ノードがパートナーのストレージの制御を引き継ぐプロセスです。

giveback は、ストレージがパートナーに返されるプロセスです。

デフォルトでは、次のいずれかの状況で自動的にテイクオーバーが実行されます。

- ノードでソフトウェアまたはシステムの障害が発生し、パニックが発生した場合。HAペアコントローラは、対応するパートナーノードに自動的にフェイルオーバーされます。パートナーがパニック状態から回復してブートされると、ノードで自動的にギブバックが実行され、パートナーは通常動作に戻ります。
- ノードでシステム障害が発生し、そのノードをリブートできない。たとえば、停電が原因でノードに障害が発生した場合、HAペアコントローラがパートナーノードに自動的にフェイルオーバーされ、稼働しているストレージコントローラからデータが提供されます。

> ノードのストレージへの電源も同時に喪失した場合は、標準テイクオーバーは実行できません。

- ノードのパートナーからハートビート メッセージが届かない場合。この状況は、パートナーでハードウェアまたはソフトウェア障害（インターコネクト障害など）が発生し、パニック状態にはならなかったものの、正常に機能しなくなった場合に発生します。
- パラメータまたは `-inhibit-takeover true`パラメータを使用せずに一方のノードを停止した場合 `-f`

> クラスタHAが有効な2ノードクラスタで、パラメータを使用してノードを停止またはリブート `-inhibit-takeover true`すると、クラスタHAを無効にしてからオンラインのままにするノードにイプシロンを割り当てないかぎり、両方のノードでデータの提供が停止します。

- パラメータを使用せずに一方のノードをリブートした場合 `-inhibit-takeover true`（ `-onboot`コマンドのパラメータは `storage failover`デフォルトで有効になっています）。
- リモート管理デバイス（サービスプロセッサ）でパートナーノードの障害が検出された場合。これは、ハードウェアアシストテイクオーバーを無効にした場合は該当しません。

コマンドを使用してテイクオーバーを手動で開始することもできます `storage failover takeover`。

クラスタの耐障害性と診断の強化

ONTAP 9.9.1以降では、耐障害性と診断機能が次のように追加され、クラスタの運用が改善されています。

- ポートの監視と回避：2ノードスイッチレスクラスタ構成では、全体的なパケット損失（接続の損失）が発生するポートを回避します。ONTAP 9 8.1以前では、この機能はスイッチ経由の構成でのみ使用できました。
- ノードの自動フェイルオーバー：クラスタネットワーク経由でデータを提供できないノードは、ディスクを所有しないでください。代わりに、パートナーが正常に稼働している場合は、そのHAパートナーがテイクオーバーします。
- 接続の問題を分析するコマンド：次のコマンドを使用して、パケット損失が発生しているクラスタパスを表示します。 `network interface check cluster-connectivity show`

  の詳細については `network interface check cluster-connectivity show`、を"ONTAPコマン

ド リファレンス"参照してください。

ONTAP クラスタにおけるハードウェアアシストテイクオーバーについて学ぶ

デフォルトで有効になっているハードウェアアシストテイクオーバー機能を使用すると、ノードのリモート管理デバイス（サービスプロセッサ）を使用してテイクオーバー処理にかかる時間を短縮できます。

リモート管理デバイスは障害を検出すると、パートナーのハートビートが停止したことをONTAPが認識するのを待たずに、すぐにテイクオーバーを開始します。この機能を有効にせずに障害が発生した場合、パートナーはノードからハートビートが送信されなくなったことを認識するまで待機し、ハートビートが失われたことを確認してからテイクオーバーを開始します。

ハードウェアアシストテイクオーバー機能では、この待機時間を回避するために次のプロセスが使用されます。

1. リモート管理デバイスは、特定のタイプの障害についてローカルシステムを監視します。
2. 障害が検出されると、リモート管理デバイスはすぐにパートナーノードにアラートを送信します。
3. アラートを受け取ったパートナーはテイクオーバーを開始します。

ハードウェアアシストテイクオーバーをトリガーするシステムイベント

リモート管理デバイス（サービスプロセッサ）から受信したアラートのタイプによっては、パートナーノードでテイクオーバーが生成されることがあります。

アラート	テイクオーバーが開始されるか	説明
abnormal_reboot	いいえ	ノードの異常リブートが発生しました。
l2_watchdog_reset	○	システムウォッチドッグハードウェアがL2リセットを検出しました。リモート管理デバイスでシステムCPUから応答がないことが検出され、システムがリセットされました。
ハートビート損失	いいえ	リモート管理デバイスがノードからハートビートメッセージを受信しなくなりました。このアラートは、HAペアのノード間のハートビートメッセージではなく、ノードとローカルのリモート管理デバイス間のハートビートメッセージです。
定期的なメッセージ	いいえ	通常のハードウェアアシストテイクオーバー処理中は、定期的なメッセージが送信されます。
power_cycle_via_sp	○	リモート管理デバイスがシステムの電源を入れ直した。
パワーロス	○	ノードで電源喪失が発生しました。リモート管理デバイスには、電源喪失後も短時間電力を維持する電源装置が搭載されているため、パートナーに電力喪失を報告できます。
power_off_via_sp	○	リモート管理デバイスの電源がオフになっている。

reset_via_sp	○	リモート管理デバイスによってシステムがリセットされました。
テスト	いいえ	ハードウェアアシストテイクオーバー処理を確認するために送信されるテストメッセージです。

関連情報

"ハードウェアアシスト（HWassist）テイクオーバー-解決ガイド"

ONTAP クラスタの自動テイクオーバーとギブバックについて学ぶ

自動テイクオーバー処理と自動ギブバック処理を組み合わせて使用することで、クライアントの停止を短くしたり回避したりできます。

デフォルトでは、HAペアの一方のノードでパニック、リブート、または停止が発生すると、パートナーノードが自動的にテイクオーバーし、該当するノードのリブート時にストレージを戻します。その後、HAペアは通常の動作状態に戻ります。

また、いずれかのノードが応答しなくなった場合にも自動テイクオーバーが実行される可能性があります。

自動ギブバックはデフォルトで実行されます。ギブバックによるクライアントへの影響を制御する場合は、自動ギブバックを無効にしてコマンドを使用し `storage failover modify -auto-giveback false -node <node>`ます。自動ギブバックは、トリガーされた状況に関係なく実行されます。パートナーノードでは、コマンドのパラメータ `storage failover modify`で制御される一定の時間待機します `-delay- seconds`。デフォルトの遅延は600秒です。

このプロセスにより、次の処理に必要な時間を含む1回の長時間の停止を回避できます。

- テイクオーバー処理
- テイクオーバーされたノードをブートしてギブバック可能な状態にします。
- ギブバック処理

ルート以外のいずれかのアグリゲートで自動ギブバックが失敗した場合、自動的に2回ギブバックが試行されます。

> テイクオーバープロセスでは、パートナーノードがギブバック可能な状態になる前に自動ギブバックプロセスが開始されます。自動ギブバックプロセスの制限時間が経過してもパートナーノードの準備が完了していない場合は、タイマーが再開されます。そのため、パートナーノードが準備完了してから実際にギブバックが実行されるまでの時間が、自動ギブバックの時間よりも短くなる可能性があります。

テイクオーバー時の動作

パートナーをテイクオーバーするノードは、パートナーのアグリゲートとボリュームのデータの提供と更新を継続します。

テイクオーバープロセスでは次の手順が実行されます。

1. ユーザが開始したネゴシエートテイクオーバーの場合は、パートナーノードからテイクオーバーを実行中のノードに集約データが移動されます。各アグリゲート（ルートアグリゲートを除く）の現在の所有者が

テイクオーバーノードに変わったときに、短時間の停止が発生します。ただし、アグリゲートの再配置を伴わないテイクオーバーに比べると短時間で済みます。

> パニック時のネゴシエートテイクオーバーは実行できません。パニックに関連しない障害が原因でテイクオーバーが発生する可能性があります。ノードとそのパートナー間の通信が失われると、障害が発生します（ハートビート損失とも呼ばれます）。障害が原因でテイクオーバーが発生した場合は、パートナーノードがハートビートの損失を検出するために時間がかかるため、停止時間が長くなる可能性があります。

- 進捗状況はコマンドを使用して監視できます `storage failover show-takeover`。
- コマンドでパラメータを `storage failover takeover`使用すると、このテイクオーバーインスタンスの実行中にアグリゲートの再配置を実行しないことができます `-bypass-optimization`。

  計画的テイクオーバー処理では、クライアントの停止を最小限にするため、アグリゲートが順に再配置されます。アグリゲートの再配置を省略すると、計画的テイクオーバー時のクライアントの停止時間が長くなります。

2. ユーザが開始したネゴシエートテイクオーバーの場合は、ターゲットノードが正常にシャットダウンされ、そのあとにルートアグリゲートと最初の手順で再配置されなかったアグリゲートのテイクオーバーが実行されます。
3. LIFのフェイルオーバールールに基づいて、ターゲットノードからテイクオーバーノード、またはクラスタ内の他のノードにデータLIF（論理インターフェイス）が移行されます。コマンドでパラメータを `storage failover takeover`使用すると、`LIF`の移行を回避できます `-skip-lif-migration`。ユーザが開始したテイクオーバーの場合、ストレージのテイクオーバーの開始前にデータLIFが移行されます。パニックまたは障害が発生した場合、構成によっては、ストレージとともに、またはテイクオーバーの完了後にデータLIFが移行される可能性があります。
4. テイクオーバーの発生時に既存のSMBセッションが切断されます。

> SMBプロトコルの性質上、すべてのSMBセッションが中断されます（Continuous Availabilityプロパティが設定された共有に接続しているSMB 3.0セッションを除く）。SMB 1.0およびSMB 2.xセッションでは、テイクオーバー後に開いているファイルハンドルを再接続できません。そのため、テイクオーバーの際に停止が発生し、一部のデータが失われる可能性があります。

5. 継続的な可用性が有効になっている共有に対するSMB 3.0セッションは、テイクオーバー後に切断された共有に再接続できます。サイトでMicrosoft Hyper-VへのSMB 3.0接続を使用していて、関連付けられている共有で継続的な可用性プロパティが有効になっている場合、テイクオーバーはそれらのセッションで無停止で実行されます。

テイクオーバーを実行中のノードがパニック状態になった場合の動作

テイクオーバーを実行中のノードが、テイクオーバーを開始してから60秒以内にパニック状態になると、次のような状況が発生します。

- パニックが発生したノードがリブートします。
- リブート後、ノードは自己リカバリ処理を実行し、テイクオーバーモードではなくなります。
- フェイルオーバーが無効になります。
- パートナーの一部のアグリゲートをまだ所有している場合は、ストレージフェイルオーバーを有効にしたあとに、コマンドを使用してそれらのアグリゲートをパートナーに戻します `storage failover`

giveback。

ギブバック時の動作

問題が解決されたとき、パートナーノードがブートしたとき、またはギブバックが開始されたときに、ローカルノードからパートナーノードに所有権が戻されます。

通常のギブバック処理では次のプロセスが実行されます。ここでは、ノードAがノードBをテイクオーバーしたものとします。ノードBの問題は解決されており、データの提供を再開できる状態になっています。

1. ノードBの問題が解決され、次のメッセージが表示されます。 `Waiting for giveback`
2. コマンドまたは自動ギブバック（設定されている場合）でギブバックが開始され `storage failover giveback`ます。これにより、ノードBのアグリゲートおよびボリュームの所有権をノードAからノードBに戻すプロセスが開始されます。
3. ノードAからルートアグリゲートの制御が最初に返されます。
4. ノードBを通常の動作状態でブートするプロセスが完了します。
5. ノードBのブートプロセスでルート以外のアグリゲートを受け取れる状態になった時点で、すぐに他のアグリゲートの所有権が1つずつ戻され、ギブバックが完了します。ギブバックの進捗は、コマンドを使用して監視できます `storage failover show-giveback`。

> `storage failover show-giveback`このコマンドでは、ストレージフェイルオーバーのギブバック処理中に発生するすべての処理に関する情報が表示されるわけではありません（また、それを意図したものでもありません）。コマンドを使用すると、ノードの現在のフェイルオーバーステータスに関するその他の詳細情報（ノードが完全に機能しているか、テイクオーバーが可能か、ギブバックが完了したかなど）を表示できます `storage failover show`。

各アグリゲートのI/Oは、そのアグリゲートのギブバックが完了したあとに再開されるため、全体的な停止時間が短縮されます。

HAポリシーとそのテイクオーバーとギブバックへの影響

ONTAPは、CFO（コントローラフェイルオーバー）およびSFO（ストレージフェイルオーバー）のHAポリシーをアグリゲートに自動的に割り当てます。このポリシーは、アグリゲートとそのボリュームに対するストレージフェイルオーバー処理の実行方法を決定します。

CFOとSFOの2つのオプションによって、ONTAPがストレージフェイルオーバーおよびギブバック処理で使用するアグリゲートの制御順序が決まります。

CFOおよびSFOという用語は、ストレージフェイルオーバー（テイクオーバーとギブバック）処理を表すこともありますが、実際にはアグリゲートに割り当てられるHAポリシーを表しています。たとえば、SFOアグリゲートやCFOアグリゲートという表現は、単にアグリゲートに割り当てられたHAポリシーを表しています。

HAポリシーは、テイクオーバー処理とギブバック処理に次のように影響します。

- ONTAPシステムで作成されたアグリゲート（ルートボリュームを含むルートアグリゲートを除く）には、SFOのHAポリシーが割り当てられます。手動で開始されたテイクオーバーでは、テイクオーバー前にSFO（ルート以外）アグリゲートをパートナーに順次再配置することで、パフォーマンスが最適化されます。ギブバック処理では、テイクオーバーされたシステムがブートして管理アプリケーションがオンラ

インになり、ノードがアグリゲートを受け取れる状態になってから、アグリゲートが順番にギブバックされます。

- アグリゲートの再配置処理では、アグリゲートのディスク所有権が再割り当てされ、ノードからパートナーに制御が移るため、SFOのHAポリシーが設定されたアグリゲートのみが再配置の対象となります。
- ルートアグリゲートには常にCFOのHAポリシーが割り当てられ、ギブバック処理の開始時にギブバックされます。これは、テイクオーバーされたシステムをブートできるようにするために必要です。他のすべてのアグリゲートは、テイクオーバーされたシステムのブートプロセスが完了して管理アプリケーションがオンラインになり、ノードがアグリゲートを受け取れる状態になったあと、順番にギブバックされます。

アグリゲートのHAポリシーをSFOからCFOに変更する処理はメンテナンスモードの処理です。カスタマーサポート担当者から指示がないかぎり、この設定を変更しないでください。

バックグラウンド更新がテイクオーバーとギブバックに与える影響

ディスクファームウェアのバックグラウンド更新によるHAペアのテイクオーバー、ギブバック、およびアグリゲートの再配置の処理に対する影響は、処理がどのように開始されたかによって異なります。

ディスクファームウェアのバックグラウンド更新がテイクオーバー、ギブバック、およびアグリゲートの再配置に与える影響を次に示します。

- いずれかのノードのディスクでディスクファームウェアのバックグラウンド更新が発生した場合、手動で開始したテイクオーバー処理は、そのディスクでディスクファームウェアの更新が完了するまで保留されます。ディスクファームウェアのバックグラウンド更新が120秒経っても完了しないと、テイクオーバー処理は中止され、ディスクファームウェアの更新の完了後に手動で再開する必要があります。コマンドのパラメータ `storage failover takeover`をに設定し `true`てテイクオーバーを開始した `-bypass-optimization`場合は、デスティネーションノードでディスクファームウェアのバックグラウンド更新を実行していても、テイクオーバーには影響しません。
- ソース（テイクオーバー）ノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、コマンドのパラメータを `storage failover takeover`に設定して `immediate`手動で開始したテイクオーバー `-options`処理はすぐに開始されます。
- ノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、そのノードがパニック状態になると、パニック状態になったノードのテイクオーバーがただちに開始されます。
- いずれかのノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、データアグリゲートのギブバックは、そのディスクでディスクファームウェアの更新が完了するまで保留されます。
- ディスクファームウェアのバックグラウンド更新が120秒経っても完了しないと、ギブバック処理は中止され、ディスクファームウェアの更新の完了後に手動で再開する必要があります。
- いずれかのノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、アグリゲートの再配置処理は、そのディスクでディスクファームウェアの更新が完了するまで保留されます。ディスクファームウェアのバックグラウンド更新が120秒経っても完了しないと、アグリゲートの再配置処理は中止され、ディスクファームウェアの更新の完了後に手動で再開する必要があります。コマンドの `storage aggregate relocation`をに設定し `true`てアグリゲートの再配置を開始した場合 `-override-destination-checks`は、デスティネーションノードでディスクファームウェアのバックグラウンド更新を実行していても、アグリゲートの再配置には影響しません。

関連情報

- "ストレージアグリゲートの再配置"

- "storage failover giveback"
- "storage failover modify"
- "storage failover show-giveback"
- "storage failover takeover"

ONTAP自動テイクオーバーコマンド

自動テイクオーバーは、サポートされるすべてのNetApp FAS、AFF、およびASAプラットフォームでデフォルトで有効になります。デフォルトの動作を変更し、パートナーノードがリブート、パニック、または停止したときに自動テイクオーバーを実行するタイミングを制御しなければならない場合があります。

テイクオーバーを自動で実行するパートナーノードの状況	使用するコマンド
リブートまたは停止	`storage failover modify -node nodename -onreboot true`
パニック	`storage failover modify -node nodename -onpanic true`

テイクオーバー機能が無効な場合にEメール通知を有効にする

テイクオーバー機能が無効になった場合に通知を受け取るようにするには、 EMS メッセージ「 takeover impossible 」の自動 E メール通知を有効にするようにシステムを設定します。

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

関連情報

- "storage failover modify"

ONTAP自動ギブバックコマンド

デフォルトでは、オフラインのノードがオンラインに戻ったときにテイクオーバーパートナーノードからストレージが自動的にギブバックされるため、ハイアベイラビリティペア関係がリストアされます。ほとんどの場合、これが望ましい動作です。ギブバックの前にテイクオーバーの原因を調査するなどの目的で自動ギブバックを無効にする必要がある場合は、デフォルト以外の設定の動作について把握しておく必要があります。

状況	使用するコマンド
自動ギブバックを有効にします。テイクオーバーされたノードがブートしてWaiting for giveback状態になり、[Delay before Auto giveback]の期間が過ぎた時点でギブバックが実行されるようにします。 デフォルト設定はtrueです。	`storage failover modify -node` *`nodename`* `-auto-giveback true`
自動ギブバックを無効にするデフォルト設定はtrueです。 *注：*このパラメータをfalseに設定しても、パニック時のテイクオーバー後の自動ギブバックは無効になりません。パニック時のテイクオーバー後の自動ギブバックは、パラメータをfalseに設定して無効にする必要があります。 `-auto-giveback-after -panic`	`storage failover modify -node` *`nodename`* `-auto-giveback false`
パニック時のテイクオーバー後の自動ギブバックを無効にします（この設定はデフォルトで有効になっています）。	`storage failover modify -node` *`nodename`* `-auto-giveback-after-panic false`
自動ギブバックを指定した秒数だけ待機します（デフォルトは600）。このオプションでは、ノードがテイクオーバーされてから自動ギブバックが実行されるまでの最小時間を指定します。	`storage failover modify -node` *`nodename`* `-delay-seconds` *`seconds`*

storage failover modifyコマンドの種類による自動ギブバックへの影響

自動ギブバックが実行されるかどうかは、storage failover modifyコマンドのパラメータの設定によって異なります。

次の表に、パニック時以外のテイクオーバーイベントに適用されるコマンドパラメータのデフォルト設定を示し `storage failover modify`ます。

パラメータ	デフォルト設定
`-auto-giveback` *`true`*	*`false`*`
`true`	`-delay-seconds` *`integer`* `(seconds)`
600	`-onreboot` *`true`*
`false``	*`true`*

次の表に、パラメータと `-auto-giveback`パラメータの組み合わせについて、パニック時以外のテイクオーバー時の自動ギブバックの処理を示し `-onreboot`ます。

`storage failover modify`使用するパラメータ	テイクオーバーの原因	自動ギブバックの実行

`-onreboot true`
 	
`-auto-giveback true`
	rebootコマンド	○

haltコマンド、またはサービスプロセッサから実行された電源再投入処理	○	`-onreboot true`
		
		`-auto-giveback false`

rebootコマンド	○	haltコマンド、またはサービスプロセッサから実行された電源再投入処理

いいえ	`-onreboot false`
	
	`-auto-giveback true`
		rebootコマンド

該当しない場合はテイクオーバーは実行されません	haltコマンド、またはサービスプロセッサから実行された電源再投入処理	○

`-onreboot false`
 	
`-auto-giveback false`
	rebootコマンド	いいえ

パラメータは、 `-auto-giveback`パニックおよびその他すべての自動テイクオーバー後のギブバックを制御します。 `-onreboot`パラメータがに設定され `true`ている場合にリブートが原因でテイクオーバーが発生すると、パラメータがに設定されている `true`かどうかに関係なく、常に自動ギブバックが実行され `-auto-giveback`ます。

パラメータは、 `-onreboot`ONTAPから実行したリブートおよびhaltコマンドに適用されます。 `-onreboot`パラメータをfalseに設定すると、ノードのリブート時にテイクオーバーが実行されません。そのため、パラメータがtrueに設定されているかどうかに関係なく自動ギブバックは実行されません `-auto-giveback`。クライアントのアクセスが中断します。

パニック時に適用される自動ギブバック パラメータの組み合わせとその影響

次の表に、パニック時に適用されるコマンドパラメータを示し `storage failover modify`ます。

パラメータ	デフォルト設定
`-onpanic _true	false_`
`true`	`-auto-giveback-after-panic _true
false_` （権限： advanced ）	`true`

`-auto-giveback _true	false_`

次の表に、コマンドのパラメータの組み合わせについて、パニック時の自動ギブバックへの影響を示し `storage failover modify`ます。

`storage failover`使用するパラメータ	パニック発生後の自動ギブバックの実行
`-onpanic true -auto-giveback true -auto-giveback-after-panic true`	○
`-onpanic true -auto-giveback true -auto-giveback-after-panic false`	○
`-onpanic true -auto-giveback false -auto-giveback-after-panic true`	○
`-onpanic true -auto-giveback false -auto-giveback-after-panic false`	いいえ
`-onpanic false`がに設定されて `false`いる場合 `-onpanic`、または `-auto-giveback-after-panic`に設定されている値に関係なく、テイクオーバー/ギブバックは実行されません。 `-auto-giveback`	いいえ

パニックに関連しない障害が原因でテイクオーバーが発生する可能性があります。a_failure_は、ノードとそのパートナー間の通信が失われたときに実行されます。これは、_ハートビートlost_とも呼ばれます。障害が原因でテイクオーバーが発生した場合、ギブバックはではなくパラメータで `-auto-giveback-after-panic parameter`制御されます `-onfailure`。

ノードがパニック状態になると、そのノードのパートナーノードにパニックパケットが送信されます。何らかの理由でパートナーノードにパニックパケットが受信されなかった場合、パニックは誤って障害と解釈される可能性があります。パニックパケットを受信しないと、パートナーノードは通信が失われたことだけを認識し、パニックが発生したことを認識しません。この場合、通信の喪失はパニックではなく障害としてパートナーノードで処理され、ギブバックは（ではなく）パラメータで制御され `-onfailure`ます `-auto-giveback-after-panic parameter`。

の詳細については `storage failover modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 手動テイクオーバーコマンド

パートナーでメンテナンスが必要な場合やその他の同様の状況では、テイクオーバーを手動で実行できます。テイクオーバーの実行に使用するコマンドは、パートナーの状態に応じて異なります。

状況	使用するコマンド
パートナーノードをテイクオーバーする	`storage failover takeover`
テイクオーバーを実行中のノードにパートナーのアグリゲートを移動するまでのテイクオーバーの進捗を監視する	`storage failover show-takeover`
クラスタ内のすべてのノードのストレージフェイルオーバーステータスを表示する	`storage failover show`
LIFを移行せずにパートナーノードをテイクオーバーする	`storage failover takeover -skip-lif-migration-before-takeover true`
ディスクが一致していなくてもパートナーノードをテイクオーバーする	`storage failover takeover -allow-disk-inventory-mismatch true`
ONTAP バージョンが一致していない場合でもパートナーノードをテイクオーバーする * 注： * このオプションは、無停止の ONTAP アップグレードプロセスでのみ使用されます。	`storage failover takeover -option allow-version-mismatch`
アグリゲートの再配置を実行せずにパートナーノードをテイクオーバーする	`storage failover takeover -bypass-optimization true`
パートナーがストレージリソースを正常に終了する前にパートナーノードをテイクオーバーする	`storage failover takeover -option immediate`

> immediateオプションを指定してstorage failoverコマンドを実行する前に、次のコマンドを使用して別のノードにデータLIFを移行する必要があります。 `network interface migrate-all -node node`
>
> の詳細については `network interface migrate-all`、を"ONTAPコマンド リファレンス"参照してください。
>
> 先にデータLIFを移行せずにコマンドを指定すると、オプションを指定し `storage failover takeover -option immediate`なくてもノードからのデータLIFの移行が大幅に遅れます `skip-lif-migration-before-takeover`。
>
> 同様に、 immediate オプションを指定した場合は、 bypass - optimization オプションを *false* に設定しても、ネゴシエートテイクオーバーの最適化が省略されます。

テイクオーバーを手動で開始する場合のイプシロンの移動

手動で開始したテイクオーバーによってストレージシステムの1つのノードで予期しないノード障害が発生し、クラスタ全体のクォーラムが失われる可能性がある場合は、イプシロンを移動する必要があります。

タスクの内容

計画的なメンテナンスを実行するには、HAペアの一方のノードをテイクオーバーする必要があります。残りのノードでクライアントデータが計画外に停止しないように、クラスタ全体のクォーラムを維持する必要があります。場合によっては、テイクオーバーの実行時にクラスタで予期しないノード障害が発生し、クラスタ全体のクォーラムが失われることがあります。

これは、テイクオーバーするノードにイプシロンが設定されている場合や、イプシロンが設定されたノードが正常な状態でない場合に発生します。クラスタの耐障害性を高めるには、テイクオーバーするノード以外の正

常なノードにイプシロンを移動します。通常はHAパートナーです。

クォーラムの投票に参加するのは、対象となる正常なノードだけです。クラスタ全体のクォーラムを維持するには、対象となる、オンラインかつ正常なノードの半数を超える投票が必要です。オンラインのノード数が偶数のクラスタの場合は、クォーラムを維持するために、イプシロンと呼ばれる投票加重がいずれかのノードに追加で割り当てられます。

> クラスタ形成の投票はコマンドを使用して変更でき `cluster modify -eligibility false`ますが、ノード構成をリストアする場合やノードのメンテナンスが長時間かかる場合を除き、この設定は避けてください。クラスタ参加資格を無効に設定すると、参加資格をリセットしてリブートするまで、そのノードはSANデータを提供しなくなります。ノードにクラスタ参加資格がないと、そのノードへのNASデータアクセスにも影響する可能性があります。

手順

1. クラスタの状態を確認し、テイクオーバーするノード以外の正常なノードにイプシロンが設定されていることを確認します。

   a. advanced モードのプロンプト（ * > ）が表示されたら、次のコマンドを入力して advanced 権限レベルに切り替えます。

      ```
      set -privilege advanced
      ```

   b. イプシロンが設定されているノードを特定します。

      ```
      cluster show
      ```

      次の例では、Node1にイプシロンが設定されています。

ノード	健全性	シヨウケン	イプシロン
ノード 1 ：ノード 2	正しいです	正しいです	true false

      テイクオーバーするノードにイプシロンが設定されていない場合は、手順4に進みます。

   の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。

2. テイクオーバーするノードからイプシロンを削除します。

   ```
   cluster modify -node Node1 -epsilon false
   ```

3. パートナーノード（この例ではNode2）にイプシロンを割り当てます。

   ```
   cluster modify -node Node2 -epsilon true
   ```

4. テイクオーバー処理を実行します。

   ```
   storage failover takeover -ofnode node_name
   ```

5. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

関連情報

- "storage failover show"
- "storage failover takeover"

ONTAP 手動ギブバックコマンド

パートナーノードのプロセスを終了する標準ギブバック、または強制ギブバックを実行できます。

ギブバックを実行する前に、テイクオーバーされたシステムから障害が発生したドライブを取り外す必要があります（を参照）"ディスクとアグリゲートの管理"。

ギブバックが中断された場合

ギブバックプロセス中にテイクオーバーノードで障害や停電が発生すると、そのプロセスは停止し、障害が修復されるか電源が復旧するまでテイクオーバーノードはテイクオーバーモードに戻ります。

ただし、これは障害が発生したギブバックの段階によって異なります。（ルートアグリゲートのギブバック後に）部分的なギブバック状態の間に障害や停電が発生した場合、ノードはテイクオーバーモードに戻りません。代わりに、部分的なギブバックモードに戻ります。この場合、プロセスを完了するには、ギブバック処理をもう一度実行します。

ギブバックが拒否された場合

ギブバックが拒否された場合は、EMSメッセージを確認して原因を特定する必要があります。理由に応じて、拒否を無視しても問題がないかどうかを判断できます。

`storage failover show-giveback`ギブバックの進捗が表示されます。ギブバックを拒否したサブシステムがある場合はそのサブシステムも表示されます。ソフトな拒否は無視できますが、ハードな拒否は、強制した場合でも無視できません。次の表に、無視すべきでないソフトな拒否と推奨される対処方法を示します。

次のコマンドを使用して、ギブバックの拒否に関するEMSの詳細を確認できます。

```
event log show -node * -event gb*
```

の詳細については `event log show`、を"ONTAPコマンド リファレンス"参照してください。

ルートアグリゲートのギブバック

次の拒否は、アグリゲートの再配置処理には適用されません。

拒否しているサブシステムモジュールです	回避策

vFiler_low_level	拒否の原因となっているSMBセッションを終了するか、開いているセッションを確立したSMBアプリケーションをシャットダウンします。 この拒否を無視すると、SMBを使用しているアプリケーションが原因によって突然切断され、データが失われる可能性があります。
ディスクチェック	ギブバックを実行する前に、障害が発生したかバイパスされたディスクをすべて取り外します。ディスクの完全消去を実行中の場合は、処理が完了するまで待ちます。 この拒否を無視すると、リザベーションの競合やディスクにアクセスできないことが原因でアグリゲートやボリュームがオフラインになり、システムが停止する可能性があります。

SFOアグリゲートのギブバック

次の拒否は、アグリゲートの再配置処理には適用されません。

拒否しているサブシステムモジュールです	回避策
ロックマネージャ	ファイルを開いているSMBアプリケーションを正常にシャットダウンするか、それらのボリュームを別のアグリゲートに移動します。 この拒否を無視すると、SMBロック状態が失われ、システムが停止してデータが失われます。
ロックマネージャNDO	ロックがミラーされるまで待ちます。 この拒否を無視すると、Microsoft Hyper-V仮想マシンが停止します。
RAID	EMSメッセージを確認して拒否の原因を特定します。 nvfileが原因で拒否された場合は、オフラインのボリュームとアグリゲートをオンラインにします。 ディスクの追加処理またはディスク所有権の再割り当て処理を実行中の場合は、処理が完了するまで待ちます。 アグリゲート名またはUUIDの競合が原因で拒否された場合は、問題をトラブルシューティングして解決します。 ミラーの再同期、ミラーの検証、またはディスクのオフライン化が原因で拒否された場合は無視してかまいません。ギブバック後に処理が再開されます。

ディスクインベントリ	トラブルシューティングを行い、問題の原因を特定して解決します。 移行中のアグリゲートに属するディスクをデスティネーションノードで認識できないことがあります。 ディスクにアクセスできないと、アグリゲートまたはボリュームにアクセスできない可能性があります。
ボリューム移動処理	トラブルシューティングを行い、問題の原因を特定して解決します。 この拒否は、重要なカットオーバーフェーズ中にボリューム移動処理が中止されるのを防ぎます。カットオーバー中にジョブが中止されると、ボリュームにアクセスできなくなる可能性があります。

手動ギブバックの実行用コマンド

HA ペアのノードで、メンテナンスが完了したあとやテイクオーバーの原因となった問題を解決したあとに元の所有者にストレージを戻すには、手動でギブバックを開始します。

状況	使用するコマンド
パートナーノードにストレージをギブバックします	`storage failover giveback -ofnode` *`nodename`*
パートナーがギブバック待機モードになっていなくてもストレージをギブバックします	`storage failover giveback -ofnode` *`nodename`* `-require-partner-waiting false` このオプションは、長時間クライアントが停止しても問題がない場合にのみ使用してください。
ギブバック処理がプロセスで拒否されてもストレージをギブバックする（強制的にギブバックを実行する）	`storage failover giveback -ofnode` *`nodename`* `-override-vetoes true` このオプションを使用すると、長時間クライアントが停止したり、ギブバック後にアグリゲートやボリュームがオンラインにならなくなったりする可能性があります。
CFOアグリゲート（ルートアグリゲート）のみをギブバックする	`storage failover giveback -ofnode` *`nodename`* `-only-cfo-aggregates true`
givebackコマンドの実行後にギブバックの進捗を監視する	`storage failover show-giveback`

関連情報

- "storage failover giveback"
- "storage failover show-giveback"

ONTAP クラスタでのテイクオーバーとギブバックのテスト

HAペアについてのすべての設定が完了したら、テイクオーバー処理やギブバック処理の際に両方のノードのストレージに中断なくアクセスできることを確認する必要があります。テイクオーバープロセス中も、通常はパートナーノードから提供されるデータはローカル（テイクオーバー）ノードから引き続き提供されます。ギブバック時には、パートナーのストレージの制御と提供がパートナーノードに戻る必要があります。

手順

1. HAインターコネクトケーブルのケーブル接続を調べて、しっかりと接続されていることを確認します。
2. ライセンスされたプロトコルごとに、両方のノードでファイルを作成および取得できることを確認します。
3. 次のコマンドを入力します。

   ```
   storage failover takeover -ofnode partnernode
   ```

   の詳細については `storage failover takeover`、を"ONTAPコマンド リファレンス"参照してください。

4. 次のいずれかのコマンドを入力して、テイクオーバーが実行されたことを確認します。

   ```
   storage failover show-takeover
   ```

   ```
   storage failover show
   ```

   `storage failover`コマンドの `-auto-giveback`オプションを有効にした場合は、次の手順を実行します。

ノード	パートナー	テイクオーバーが可能か	State 概要の略
ノード1	ノード2	-	ギブバックを待っています
ノード2	ノード1	正しくない	テイクオーバーの発生後、 number of seconds で示された秒数以内に自動ギブバックが開始されます

   `storage failover`コマンドの `-auto-giveback`オプションを無効にした場合は、次の手順を実行します。

ノード	パートナー	テイクオーバーが可能か	State 概要の略

ノード1	ノード2	-	ギブバックを待っています
ノード2	ノード1	正しくない	テイクオーバー中です

5. パートナーノード（ノード2）に属するディスクのうち、テイクオーバーノード（ノード1）で検出できるすべてのディスクを表示します。

   ```
   storage disk show -home node2 -ownership
   ```

   次のコマンドは、ノード2に属するディスクのうち、ノード1で検出できるすべてのディスクを表示します。
   ```
   cluster::> storage disk show -home node2 -ownership
   ```

ディスク	アグリゲート	ホーム	所有者	DR ホーム	ホーム ID	所有者 ID	DR ホーム ID	予約者	プール
1.0.2	-	ノード2	ノード2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	ノード2	ノード2	-	4078312453	4078312453	-	4078312452	Pool0

6. テイクオーバーノード（ノード1）でパートナーノード（ノード2）のアグリゲートを制御していることを確認します。

   ```
   aggr show -fields home-id,home-name,is-home
   ```

アグリゲート	home-id	Home - 名前 h	is-fhome
aggr0_1	2014942045	node1	正しい
aggr0_2	4078312453	ノード2	正しくない
aggr1_1	2014942045	node1	正しい
aggr1_2	4078312453	ノード2	正しくない

   テイクオーバー時、パートナーノードのアグリゲートの「 is-home 」の値が false になります。

7. 「 Waiting for giveback' 」メッセージが表示されたら、パートナー・ノードのデータ・サービスをギブバックします。

   ```
   storage failover giveback -ofnode partnernode
   ```

8. 次のいずれかのコマンドを入力して、ギブバック処理の進捗を監視します。

   ```
   storage failover show-giveback
   ```

   ```
   storage failover show
   ```

9. ギブバックが正常に完了したことを示すメッセージが表示されたかどうかに応じて、次の手順に進みます。

テイクオーバーおよびギブバックの結果	そしたら…。
正常に完了しました	パートナーノードで手順2~8を繰り返します。
不合格	テイクオーバーまたはギブバックの失敗を修正してから、この手順を繰り返します。

関連情報

- "storage disk show"
- "storage failover giveback"
- "storage failover show"
- "storage failover show-giveback"

HAペアを監視するためのONTAPコマンド

ONTAPコマンドを使用して、HAペアのステータスを監視できます。テイクオーバーが発生した場合は、その原因を確認することもできます。

をオンにする場合は	使用するコマンド
フェイルオーバーの有効 / 無効と発生の有無、または現在フェイルオーバーを実行できない理由	`storage failover show`
ストレージフェイルオーバーの HA モード設定が有効になっているノードを表示するストレージフェイルオーバー（ HA ペア）構成に含めるには、値を HA に設定する必要があります。	`storage failover show -fields mode`
ハードウェアアシストテイクオーバーが有効かどうか	`storage failover hwassist show`
これまでに発生したハードウェアアシストテイクオーバーイベントの履歴	`storage failover hwassist stats show`
テイクオーバー処理（パートナーのアグリゲートをテイクオーバーを実行中のノードに移動）の進捗状況	`storage failover show-takeover`
ギブバック処理（アグリゲートをパートナーノードに戻す）の進捗	`storage failover show-giveback`
テイクオーバーまたはギブバックの処理中にアグリゲートがホームであるかどうか	`aggregate show -fields home-id,owner-id,home-name,owner-name,is-home`
クラスタHAが有効になっているかどうか（2ノードクラスタの場合のみ）	`cluster ha show`
HAペアのコンポーネントのHAの状態（HAの状態を使用するシステム）	`ha-config show`これはメンテナンスモードのコマンドです。

storage failover show-typeコマンドで表示されるノードの状態

次に、コマンドで表示されるノードの状態を示し `storage failover show`ます。

ノードの状態	説明
partner_name に接続されています。自動テイクオーバーは無効になっています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーの自動テイクオーバーは無効になっています。
partner_name で待機しているパートナーのスペアディスクのギブバックが保留中です。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。パートナーへのSFOアグリゲートのギブバックは完了しますが、パートナーのスペアディスクはまだローカルノードで所有されています。 • 詳細については、コマンドを実行して `storage failover show-giveback`ください。
partner_name を待機していますパートナーロックの同期を待っています。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。パートナーロックの同期が実行されるのを待っています。
partner_name を待機していますローカルノードでクラスタのアプリケーションがオンラインになるのを待っています。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。クラスタのアプリケーションがオンラインになるのを待っています。
テイクオーバーがスケジュールされました。target node relocating its SFO aggregates（テイクオーバーの準備中）。	テイクオーバーの処理が開始されました。テイクオーバーの準備として、ターゲットノードでSFOアグリゲートの所有権を切り替えています。
テイクオーバーがスケジュールされました。テイクオーバーの準備として、ターゲットノードでSFOアグリゲートが再配置されました。	テイクオーバーの処理が開始されました。テイクオーバーの準備として、ターゲットノードでSFOアグリゲートの所有権が切り替えられました。
テイクオーバーのスケジュール：ローカルノードでディスクファームウェアのバックグラウンド更新を無効にするのを待っています。ノードでファームウェアの更新を実行中です。	テイクオーバーの処理が開始されました。ローカルノードでのディスクファームウェアのバックグラウンド更新が完了するのを待っています。
テイクオーバーの準備としてテイクオーバーするノードへの SFO アグリゲートの再配置	テイクオーバーの準備として、ローカルノードでテイクオーバーするノードに SFO アグリゲートの所有権を切り替えています。
テイクオーバーするノードに SFO アグリゲートを再配置しました。テイクオーバーするノードのテイクオーバーを待機しています。	ローカルノードからテイクオーバーするノードへの SFO アグリゲートの所有権の切り替えが完了しました。テイクオーバーするノードによるテイクオーバーを待っています。

SFO アグリゲートを partner_name に再配置していますローカルノードでのディスクファームウェアのバックグラウンド更新の無効化を待機しています。ノードでファームウェアの更新を実行中です。	ローカルノードからテイクオーバーするノードへの SFO アグリゲートの所有権の切り替えを実行中です。ローカルノードでのディスクファームウェアのバックグラウンド更新が完了するのを待っています。
SFO アグリゲートを partner_name に再配置していますpartner_nameでのディスクファームウェアのバックグラウンド更新の無効化を待機しています。ノードでファームウェアの更新を実行中です。	ローカルノードからテイクオーバーするノードへの SFO アグリゲートの所有権の切り替えを実行中です。パートナーノードでのディスクファームウェアのバックグラウンド更新が完了するのを待っています。
partner_name に接続されています。前回のテイクオーバーの試行が理由で中止されました。ローカルノードがパートナーのSFOアグリゲートの一部を所有します。パラメータをtrueに設定してパートナーのテイクオーバーを再実行し `-bypass-optimization`、残りのアグリゲートをテイクオーバーするか、パートナーのギブバックを実行して再配置されたアグリゲートを戻します。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。前回のテイクオーバーの試行がreasonに表示された理由により中止されました。パートナーの一部のSFOアグリゲートがローカルノードに所有されている。 • 残りのSFOアグリゲートをテイクオーバーするには、-bypass-optimizationパラメータをtrueに設定してパートナーノードのテイクオーバーを再実行します。再配置されたアグリゲートを戻すには、パートナーのギブバックを実行します。
partner_name に接続されています。前回のテイクオーバーの試行が中止されました。ローカルノードがパートナーのSFOアグリゲートの一部を所有します。パラメータをtrueに設定してパートナーのテイクオーバーを再実行し `-bypass-optimization`、残りのアグリゲートをテイクオーバーするか、パートナーのギブバックを実行して再配置されたアグリゲートを戻します。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。前回のテイクオーバーの試行が中止されました。パートナーの一部のSFOアグリゲートがローカル ノードで所有されています。 • 残りのSFOアグリゲートをテイクオーバーするには、-bypass-optimizationパラメータをtrueに設定してパートナーノードのテイクオーバーを再実行します。再配置されたアグリゲートを戻すには、パートナーのギブバックを実行します。
partner_name を待機しています前回のテイクオーバーの試行が理由で中止されました。ローカルノードがパートナーのSFOアグリゲートの一部を所有します。「-bypass-optimization」パラメータをtrueに設定してパートナーのテイクオーバーを再実行し、残りのアグリゲートをテイクオーバーするか、パートナーのギブバックを実行して再配置されたアグリゲートを戻します。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。前回のテイクオーバーの試行がreasonに表示された理由により中止されました。パートナーの一部のSFOアグリゲートがローカルノードに所有されている。 • 残りのSFOアグリゲートをテイクオーバーするには、-bypass-optimizationパラメータをtrueに設定してパートナーノードのテイクオーバーを再実行します。再配置されたアグリゲートを戻すには、パートナーのギブバックを実行します。

partner_name を待機しています前回のテイクオーバーの試行が中止されました。ローカルノードがパートナーのSFOアグリゲートの一部を所有します。「-bypass-optimization」パラメータをtrueに設定してパートナーのテイクオーバーを再実行し、残りのアグリゲートをテイクオーバーするか、パートナーのギブバックを実行して再配置されたアグリゲートを戻します。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。前回のテイクオーバーの試行が中止されました。パートナーの一部のSFOアグリゲートがローカル ノードで所有されています。 • 残りのSFOアグリゲートをテイクオーバーするには、-bypass-optimizationパラメータをtrueに設定してパートナーノードのテイクオーバーを再実行します。再配置されたアグリゲートを戻すには、パートナーのギブバックを実行します。
partner_name に接続されています。ローカルノードでディスクファームウェアのバックグラウンド更新（BDFU）を無効にできなかったため、前回のテイクオーバーの試行が中止されました。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。ローカルノードでのディスクファームウェアのバックグラウンド更新が無効になっていないため、前回のテイクオーバーの試行が中止されました。
partner_name に接続されています。前回のテイクオーバーの試行が理由で中止されました。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。前回のテイクオーバーの試行がreasonに表示された理由により中止されました。
partner_name を待機しています前回のテイクオーバーの試行が理由で中止されました。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。前回のテイクオーバーの試行がreasonに表示された理由により中止されました。
partner_name に接続されています。partner_nameによる前回のテイクオーバーの試行は、理由により中止されました。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーノードによる前回のテイクオーバーの試行がreasonに表示された理由により中止されました。
partner_name に接続されています。partner_nameによる前回のテイクオーバーの試行が中止されました。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーノードによる前回のテイクオーバーの試行が中止されました。
partner_name を待機していますpartner_nameによる前回のテイクオーバーの試行は、理由により中止されました。	ローカルノードとパートナーノードの間で、 HA インターコネクトを介して情報を交換できません。パートナーノードによる前回のテイクオーバーの試行がreasonに表示された理由により中止されました。
前回のギブバックがモジュールで失敗しました：module name 。秒数で自動ギブバックが開始されます。	前回のギブバックの試行が module_name で示されたモジュールで失敗しました。秒数で自動ギブバックが開始されます。 • 詳細については、コマンドを実行して `storage failover show-giveback`ください。

コントローラの無停止アップグレード手順の一環として、ノードがパートナーのアグリゲートを所有します。	コントローラの無停止アップグレードを実行中の手順があるため、パートナーのアグリゲートがノードで所有されています。
partner_name に接続されています。クラスタ内の別のノードに属するアグリゲートがノードで所有されています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。クラスタ内の別のノードに属するアグリゲートがノードで所有されている。
partner_name に接続されています。パートナーロックの同期を待っています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーロックの同期が完了するのを待っています。
partner_name に接続されています。ローカルノードでクラスタのアプリケーションがオンラインになるのを待っています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。ローカルノードでクラスタのアプリケーションがオンラインになるのを待っています。
非 HA モードでは、 NVRAM をすべて使用するにはリブートしてください。	ストレージフェイルオーバーを実行できません。HAモードオプションはnon_haに設定されています。 • ノードのNVRAMをすべて使用できるようにするには、ノードをリブートする必要があります。
非HAモード。ノードをリブートしてHAをアクティブ化します。	ストレージフェイルオーバーを実行できません。 • HA機能を有効にするには、ノードをリブートする必要があります。
非HAモード。	ストレージフェイルオーバーを実行できません。HAモードオプションはnon_haに設定されています。 • HA機能を有効にするには、HAペアの両方のノードでコマンドを実行してからノードをリブートする必要があり `storage failover modify -mode ha -node nodename`ます。

関連情報

- "ONTAPコマンド リファレンス"
- "cluster ha show"
- "ストレージフェイルオーバー hwassist"
- "storage failover modify"
- "storage failover show"
- "storage failover show-giveback"

ストレージフェイルオーバーを有効または無効にするONTAPコマンド

ストレージフェイルオーバー機能を有効または無効にするには、次のコマンドを使用します。

状況	使用するコマンド
テイクオーバーを有効化	`storage failover modify -enabled true -node` *`nodename`*
テイクオーバーを無効化	`storage failover modify -enabled false -node` *`nodename`*

ストレージフェイルオーバーは、メンテナンス手順の一環として必要な場合にのみ無効にしてください。

関連情報

- "storage failover modify"

2ノードクラスタでテイクオーバーを開始せずにONTAPノードを停止または再起動する

2ノードクラスタのノードをテイクオーバーなしで停止またはリブートするノードまたはシェルフでハードウェアの特定のメンテナンスを実施し、パートナーノードの稼働状態を維持してダウンタイムを制限する場合や、手動テイクオーバーを実行できない問題が発生してパートナーノードのアグリゲートを稼働させてデータを提供し続ける場合は、また、テクニカルサポートが問題のトラブルシューティングを支援している場合は、その一環としてこの手順の実行を求められることがあります。

タスクの内容

- テイクオーバーを禁止する前に（パラメータを使用して `-inhibit-takeover true`）、クラスタHAを無効にします。

- 2ノードクラスタでは、クラスタHAによって、一方のノードで障害が発生してもクラスタが無効になることはありません。ただし、パラメータを使用する前にクラスタHAを無効にしないと、 `-inhibit-takeover true`両方のノードがデータの提供を停止します。
- クラスタHAを無効にする前にノードを停止またはリブートしようとすると、ONTAPによって警告が表示され、クラスタHAを無効にするように指示されます。

- オンラインのままにするパートナーノードにLIF（論理インターフェイス）を移行します。
- 停止またはリブートするノードにアグリゲートを保持する場合は、オンラインのままにするノードにアグリゲートを移動します。

手順

1. 両方のノードが正常であることを確認します。
   `cluster show`

   両方のノードについて、 `true`列にと表示され `Health`ます。

```
cluster::> cluster show
Node          Health  Eligibility
------------ ------- ------------
node1         true     true
node2         true     true
```

の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。

2. 停止またはリブートするノードからすべてのLIFをパートナーノードに移行します。
`network interface migrate-all -node node_name`

   の詳細については `network interface migrate-all`、を"ONTAPコマンド リファレンス"参照してください。

3. ノードを停止またはリブートするときにオンラインのままにしておくアグリゲートがある場合は、それらのアグリゲートをパートナーノードに再配置します。それ以外の場合は、次の手順に進みます。

   a. 停止またはリブートするノード上のアグリゲートを表示します。
   `storage aggregates show -node node_name`

   たとえば、node1は停止またはリブートするノードです。

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1       2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
            4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

   b. アグリゲートをパートナーノードに移動します。
   `storage aggregate relocation start -node node_name -destination node_name -aggregate-list aggregate_name`

たとえば、アグリゲートaggr1、aggr2、およびtest2_aggrをnode1からnode2に移動します。

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr
```

4. クラスタHAを無効にします。
   `cluster ha modify -configured false`

   HAが無効になっていることを示す出力が表示されます。 `Notice: HA is disabled`

   この処理では、ストレージフェイルオーバーは無効になりません。

5. 該当するコマンドを使用して、ターゲットノードを停止またはリブートし、テイクオーバーを禁止します。
   - `system node halt -node node_name -inhibit-takeover true`
   - `system node reboot -node node_name -inhibit-takeover true`

   コマンド出力に、続行するかどうかを確認する警告が表示されます。と入力します。 `y`

6. オンラインのノードが健全な状態（パートナーが停止している状態）であることを確認します。
   `cluster show`

   オンラインノードの場合は、 `true`列にと表示され `Health`ます。

   コマンドの出力に、クラスタHAが構成されていないことを示す警告が表示されます。この警告は無視してかまいません。

7. ノードの停止またはリブートに必要な操作を実行します。
8. オフラインになったノードをLoaderプロンプトからブートします。
   `boot_ontap`
9. 両方のノードが正常であることを確認します。
   `cluster show`

   両方のノードについて、 `true`列にと表示され `Health`ます。

   コマンドの出力に、クラスタHAが構成されていないことを示す警告が表示されます。この警告は無視してかまいません。

10. クラスタHAを再度有効にします。
    `cluster ha modify -configured true`
11. 前の手順でパートナーノードにアグリゲートを再配置した場合は、アグリゲートをホームノードに戻します。それ以外の場合は、次の手順に進みます。
    `storage aggregate relocation start -node node_name -destination node_name
    -aggregate-list aggregate_name`

    たとえば、アグリゲートaggr1、aggr2、およびtest2_aggrをノードnode2からノードnode1に移動します。

```
storage aggregate relocation start -node node2 -destination node1 -aggregate
-list aggr1,aggr2,test2_aggr
```

12. LIFをそれぞれのホームポートにリバートします。

    a. ホームにないLIFを表示します。
    `network interface show -is-home false`

    の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

    b. 停止したノードから移行されなかったホーム以外のLIFがある場合は、リバート前にLIFを安全に移動できることを確認します。

    c. 安全な場合は、すべてのLIFをホームにリバートします。 `network interface revert *`+の詳細について `network interface revert`は、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "クラスタHA modify"
- "storage aggregate relocation start"

System ManagerによるREST API管理

System ManagerによるREST API管理

REST APIログには、System ManagerからONTAPに対して発行されたAPI呼び出しが記録されます。このログを使用して、ONTAPのさまざまな管理タスクを実行するために必要な呼び出しの性質と順序を把握できます。

System ManagerでのREST APIとAPIログの使用方法

System ManagerからONTAPに対してREST API呼び出しを実行する方法はいくつかあります。

System ManagerからAPI呼び出しが実行されるタイミング

ここでは、System ManagerがONTAP REST API呼び出しを実行するタイミングの最も重要な例を示します。

ページの自動更新

ダッシュボードページなどに表示されている情報を更新するために、API呼び出しがバックグラウンドで自動的に実行されます。

ユーザによる表示操作

System ManagerのUIから特定のストレージリソースまたは一連のリソースを表示すると、API呼び出しが実行されます。

ユーザによる更新操作

API呼び出しは、System Manager UIからONTAPリソースを追加、変更、または削除するときに実行されます。

ログエントリをクリックして、API呼び出しを手動で再実行することもできます。これにより、呼び出しからのJSON出力の生データが表示されます。

詳細情報

- "ONTAP 9自動化のドキュメント"

REST APIログへのアクセス

System Managerで実行されたONTAP REST API呼び出しのレコードが記録されたログにアクセスできます。ログを表示するときに、API呼び出しを再実行して出力を確認することもできます。

手順

1. ページ上部のをクリック してREST APIログを表示します。

   最新のエントリがページの下部に表示されます。

2. 左側の*[ダッシュボード]*をクリックし、ページをリフレッシュするために実行されたAPI呼び出し用の新しいエントリを確認します。
3. をクリックし、[qtree]*をクリックします。

   qtreeのリストを取得するための特定のAPI呼び出しがSystem Managerで実行されます。

4. 次の形式のAPI呼び出しについて説明するログエントリを探します。

   `GET /api/storage/qtrees`

   エントリには、などの追加のHTTPクエリパラメータが含まれています。 `max_records`

5. ログエントリをクリックしてGET API呼び出しを再実行し、JSON出力を表示します。

   例

```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
```

```
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
00a0986abd71/1"
        }
      }
    },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```

ボリューム管理

System ManagerによるボリュームとLUNの管理

ONTAP System Manager によるボリューム管理の概要について学習します

System.7以降では、ONTAP 9 Managerを使用して、FlexVolボリュームやLUN、qtree、Storage Efficiency、クォータなどの論理ストレージを管理できます。

従来のSystem Manager（ONTAP 9.7以前でのみ使用可能）を使用している場合は、 "論理ストレージを管理する"

ボリュームの管理

System ManagerでONTAPボリュームを管理する

System Managerでボリュームのリストを表示したら、さまざまな操作を実行してボリュームを管理できます。

次のボリュームを含む一部のボリュームタイプは、System Managerでは使用できません。

- Vol0
- DELおよびTMPタイプのボリューム
- FlexGroup構成要素
- MetroCluster構成でレプリケートされたボリューム

手順

1. System Manager で、 * Storage > Volumes （ボリューム） * をクリックします。

   ボリュームのリストが表示されます。

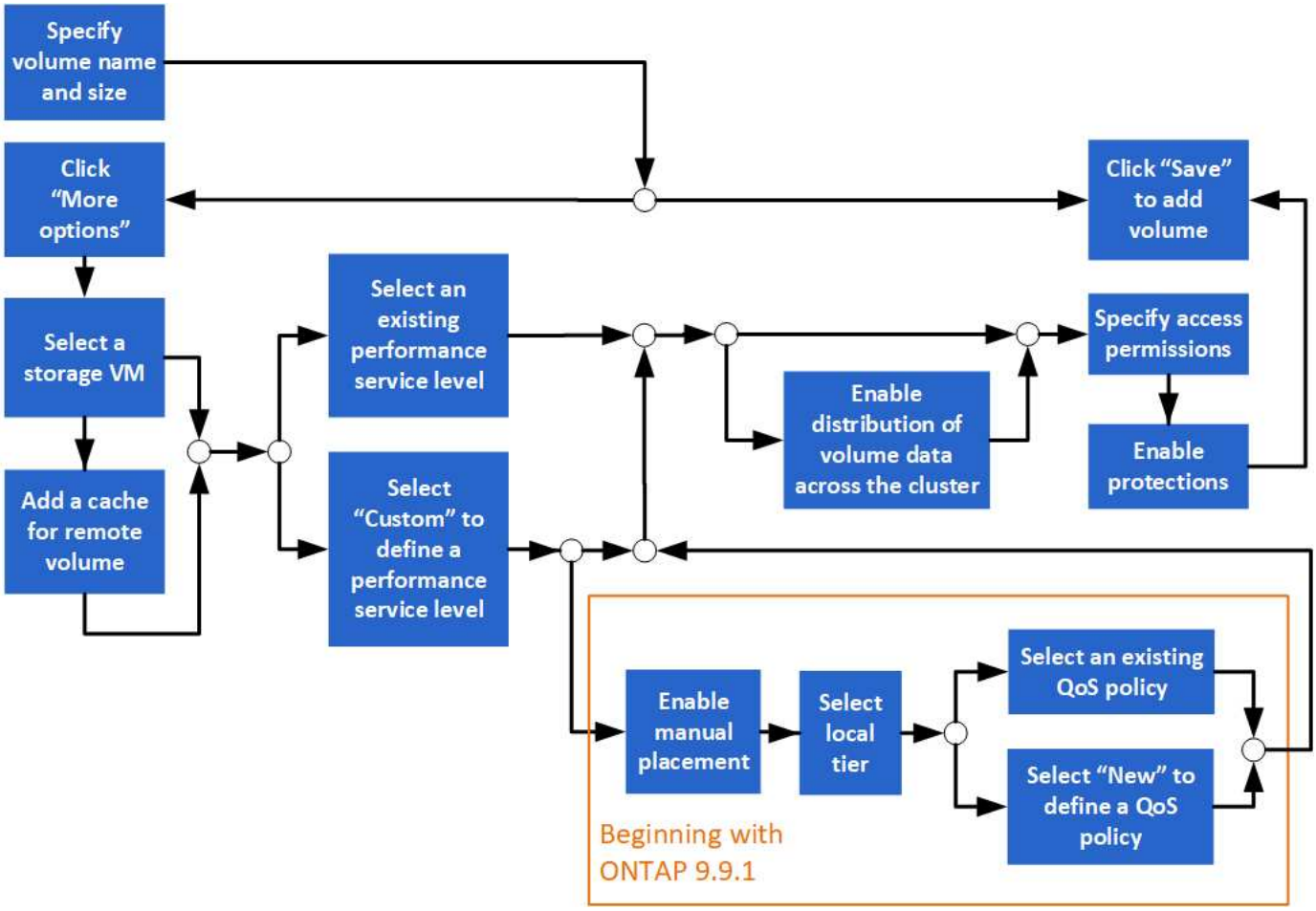
2. 次の操作を実行できます。

このタスクを実行します。	対処方法
ボリュームの追加	をクリックします。 + Add を参照して "ボリュームの追加"

複数のボリュームを管理	ボリュームの横にあるチェックボックスをオンにします。 • をクリックし Delete て、選択したボリュームを削除します。 • をクリックし Protect て、選択したボリュームに保護ポリシーを割り当てます。 • 選択したすべてのボリュームに対して実行する次のいずれかの操作をクリック More アイコン"]して選択します。 ◦ クォータの有効化 ◦ オフラインカ ◦ 移動 ◦ 削除したボリュームを表示
1 つのボリュームを管理します	ボリュームの横にあるをクリックし、次のいずれかの操作を実行します。 • 編集 • サイズ変更（ONTAP 9 .10.1以降。オンラインボリュームとDP FlexVolボリュームのみ） • 削除 • クローン • オフラインにする（またはオンラインにする） • クォータの有効化（またはクォータの無効化） • エクスポートポリシーの編集 • マウントパスの編集 • 移動 • クラウド階層の設定の編集 • 保護する
ボリュームの名前を変更します	概要ページでボリュームの名前を変更できます。 ボリューム名の横にあるをクリックし、ボリュームの名前を変更します。

ボリュームの追加

ボリュームを作成し、NFSサービスまたはSMBサービス用に設定されている既存のStorage VMに追加できます。



開始する前に

- NFSまたはSMBサービス用に設定されているStorage VMがクラスタに存在している必要があります。
- ONTAP 9.13.1以降では、新しいボリュームに対して容量分析とアクティビティ追跡をデフォルトで有効にすることができます。System Managerでは、クラスタレベルまたはStorage VMレベルでデフォルト設定を管理できます。詳細については、を参照してください "ファイルシステム分析を有効にする"。

手順

1. [ストレージ] > [ボリューム] に移動します。
2. を選択します + Add 。
3. ボリュームの名前とサイズを指定します。
4. 次のいずれかの手順を実行します。

選択するボタン	実行する処理
* 保存 *	ボリュームは、システムのデフォルト設定を使用して作成および追加されます。追加の手順は必要ありません。
* その他のオプション *	に進み、[step5]ボリュームの仕様を定義します。

5. [[step5 、 Step 5]] ボリュームの名前とサイズを指定した場合は、それらが表示されます。それ以外の場合は、名前とサイズを入力します。
6. プルダウンリストからStorage VMを選択します。

NFSプロトコルが設定されているStorage VMだけが表示されます。NFSプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

7. リモートボリュームのキャッシュを追加するには、 * リモートボリュームのキャッシュを追加 * を選択し、次の値を指定します。
   - クラスタを選択します。
   - Storage VMを選択してください。
   - キャッシュボリュームにするボリュームを選択します。
8. ストレージと最適化 * セクションで、次の値を指定します。
   a. ボリュームの容量はすでに表示されていますが、変更は可能です。
   b. [パフォーマンスサービスレベル *] フィールドで、サービスレベルを選択します。

選択するサービスレベル	発生する処理
「最高レベル」、「パフォーマンス」、「バリュー」などの既存のサービスレベル。 システムプラットフォームに有効なサービスレベル（AFF、FASなど）のみが表示されます。	ローカル階層が自動的に選択されます。に進みます[step9]。
カスタム	新しいサービスレベルの定義に進みます[step8c]。

   c. [[step8c、手順8c]] ONTAP 9.9.1以降では、System Managerを使用して、ボリュームを配置するローカル階層を手動で選択できます（サービスレベルが「カスタム」を選択している場合）。

> このオプションは、リモートボリュームのキャッシュとして * 追加を選択した場合、または * ボリュームデータをクラスタに分散した場合には使用できません * （以下を参照）。

この選択をすると…	実行する手順
* 手動配置 *	手動配置が有効になっています。*Distribute volume data across the cluster * selection （ * ボリュームデータのクラスタへの分散）が無効になっています（以下を参照）。に進み、Step 8dプロセスを完了します。
選択なし	手動配置が有効になっていません。ローカル階層が自動的に選択されます。に進みます[step9]。

   a. プルダウンメニューからローカル階層を選択します。
   b. QoSポリシーを選択します。

      [Existing]を選択して既存のポリシーのリストから選択するか、[New]を選択して新しいポリシーの仕様を入力します。

9. [[step9 、 Step 9] * Optimization options * セクションで、ボリュームデータをクラスタ全体に分散するかどうかを決定します。

この選択をすると…	発生する処理
* ボリュームデータをクラスタ全体に分散 *	追加するボリュームがFlexGroupボリュームになります。このオプションは、以前に * 手動配置 * を選択した場合は使用できません。
選択なし	追加するボリュームは、デフォルトでFlexVol volumeになります。

10. アクセス権限 * セクションで、ボリュームを構成するプロトコルのアクセス権限を指定します。

    ONTAP 9 .11.1以降では、新しいボリュームはデフォルトで共有できません。デフォルトのアクセス権限を指定するには、次のチェックボックスをオンにします。

    - **NGS**経由でエクスポート: `default`ユーザーにデータへのフルアクセスを許可するエクスポート ポリシー。
    - * SMB/CIFSで共有*：名前が自動生成されて編集可能な共有を作成します。、権限レベルを指定することもできます。

11. 「 * 保護」セクションで、ボリュームの保護を指定します。
    - ONTAP 9.12.1 以降では、デフォルトを使用するのではなく、[スナップショットを有効にする (ローカル)] を選択し、スナップショット ポリシーを選択できます。
    - SnapMirror を有効にする（ローカルまたはリモート） * を選択する場合は、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。

12. [保存（ Save ）] を選択します。

    ボリュームが作成され、クラスタとStorage VMに追加されます。

    このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

ボリュームへのタグの割り当て

ONTAP 9 14.1以降では、System Managerを使用してボリュームにタグを割り当て、プロジェクトやコストセンターなどのオブジェクトをカテゴリに属するオブジェクトとして識別することができます。

タスクの内容

ボリュームにタグを割り当てることができます。まず、タグを定義して追加する必要があります。その後、タグを編集または削除することもできます。

タグは、ボリュームの作成時に追加することも、あとから追加することもできます。

タグを定義するには、キーを指定し、"`key:value`"の形式で値を関連付けます。たとえば、「`dept:engineering`」や「`location:san-jose`」などです。

タグを作成するときは、次の点を考慮する必要があります。

- キーの長さは1文字以上で、nullにすることはできません。値にはnullを指定できます。

- キーは、値をカンマで区切って複数の値とペアにすることができます（例："`location:san-jose, Toronto"'）。
- タグは複数のリソースに使用できます。
- キーの先頭は小文字にする必要があります。
- ボリュームに割り当てられているタグは、ボリュームを削除すると削除されます。
- ボリュームがリカバリキューからリカバリされた場合、タグはリカバリされません。
- タグは、ボリュームを移動またはクローニングしても保持されます。
- ディザスタリカバリ関係でStorage VMに割り当てられたタグは、パートナーサイトのボリュームにレプリケートされます。

手順

タグを管理するには、次の手順を実行します。

1. System Managerで、*[ボリューム]*をクリックし、タグを追加するボリュームを選択します。

   タグは* Tags *セクションに表示されます。

2. [タグの管理]*をクリックして、既存のタグを変更するか、新しいタグを追加します。

   タグを追加、編集、または削除できます。

実行する処理	実行する手順
タグの追加	a. [タグの追加]*をクリックします。 b. キーとその値を指定します（複数の値はカンマで区切ります）。 c. [保存（ Save ）] をクリックします。
タグの編集	a. 「* Key 」および「 Values（オプション）*」フィールドの内容を変更します。 b. [保存（ Save ）] をクリックします。
タグの削除	a. 削除するタグの横にあるをクリックし ます。

削除したボリュームのリカバリ

FlexVolを誤って削除した場合は、System Managerを使用してリカバリできます。ONTAP 9 .8以降では、System Managerを使用してFlexGroupボリュームをリカバリすることもできます。ボリュームをパージして完全に削除することもできます。

ボリュームの保持期限はStorage VMレベルで設定できます。デフォルトでは、ボリュームの保持期間は12時間に設定されています。

削除したボリュームの選択

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. [詳細] 、 [削除されたボリュームを表示する *] の順にクリックし
3. ボリュームを選択し、ボリュームをリカバリするか完全に削除する操作をクリックします。

ボリューム構成のリセット

ボリュームを削除すると、そのボリュームに関連付けられている構成が削除されます。ボリュームをリカバリしても、すべての構成がリセットされるわけではありません。ボリュームのリカバリ後に次のタスクを手動で実行して、ボリュームを元の状態に戻します。

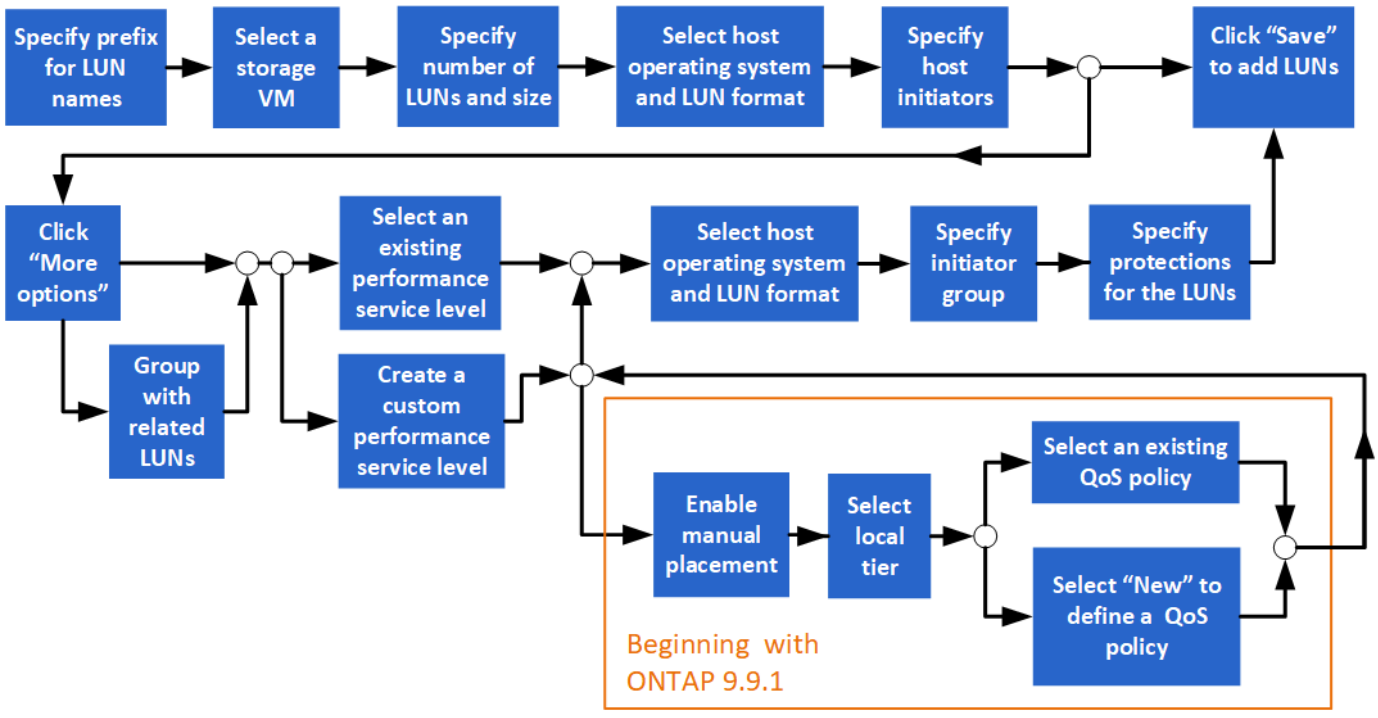
手順

1. ボリュームの名前を変更します。
2. ジャンクションパスを設定（NAS）
3. ボリューム内のLUNのマッピングを作成します（SAN）。
4. Snapshotポリシーとエクスポートポリシーをボリュームに関連付けます。
5. ボリュームの新しいクォータポリシールールを追加します。
6. ボリュームのQoSポリシーを追加します。

ONTAP System ManagerでLUNを管理する

LUNを作成して、SANプロトコルが設定された既存のStorage VMに追加できます。LUNをグループ化したり、名前を変更したりすることもできます。

LUNの追加



開始する前に

SANサービス用に設定されているStorage VMがクラスタに存在している必要があります。

手順

1. [* ストレージ] > [LUN] に移動します。
2. をクリックします。 + Add
3. 各LUN名の先頭に使用するプレフィックスを指定します。（LUNを1つだけ作成する場合は、LUN名を入力します）。
4. プルダウンリストからStorage VMを選択します。

   SANプロトコル用に設定されているStorage VMのみが表示されます。SAN プロトコル用に設定されている Storage VM が 1 つしかない場合、「 * Storage VM * 」フィールドは表示されません。

5. 作成するLUNの数と各LUNのサイズを指定します。
6. ホストオペレーティングシステムとLUNの形式をプルダウンリストから選択します。
7. ホストイニシエータを入力し、カンマで区切ります。
8. 次のいずれかを実行します。

クリックするボタン	実行する処理
* 保存 *	入力した仕様でLUNが作成されます。その他の仕様には、システムのデフォルトが使用されます。追加の手順は必要ありません。
* その他のオプション *	に進み、[step9-define-add-specs]LUNの追加仕様を定義します。

9. [[step9-define-add-specs、Step 9]：以前にLUNプレフィックスを入力した場合はすでにLUNプレフィックスが表示されますが、変更することができます。それ以外の場合は、プレフィックスを入力します。
10. プルダウンリストからStorage VMを選択します。

    SANプロトコル用に設定されているStorage VMのみが表示されます。SAN プロトコル用に設定されている Storage VM が 1 つしかない場合、「 * Storage VM * 」フィールドは表示されません。

11. LUNをグループ化する方法を決定します。

この選択をすると…	発生する処理
* 関連する LUN* でグループ化します	これらのLUNは、Storage VM上の既存ボリューム上の関連するLUNとグループ化されます。
選択なし	LUNは「container」というボリュームにグループ化されます。

12. ストレージと最適化 * セクションで、次の値を指定します。
    a. 以前に入力したLUNの数と容量はすでに表示されていますが、変更することもできます。それ以外の場合は、値を入力します。
    b. [パフォーマンスサービスレベル *] フィールドで、サービスレベルを選択します。

選択するサービスレベル	発生する処理

「最高レベル」、「パフォーマンス」、「バリュー」などの既存のサービスレベル。 システムプラットフォームに有効なサービスレベル（AFF、FASなど）のみが表示されます。	ローカル階層が自動的に選択されます。に進みます[step13]。
カスタム	新しいサービスレベルの定義に進みます[step12c]。

c. [[step12c、手順12c]] ONTAP 9.9.1以降では、System Managerを使用して、作成するLUNを配置するローカル階層を手動で選択できます（「カスタム」サービスレベルを選択した場合）。

この選択をすると…	実行する手順
* 手動配置 *	手動配置が有効になっています。に進み、Step 12Dプロセスを完了します。
選択なし	手動選択は有効になっていません。ローカル階層が自動的に選択されます。に進みます[step13]。

d. プルダウンメニューからローカル階層を選択します。

e. QoSポリシーを選択します。

[Existing]を選択して既存のポリシーのリストから選択するか、[New]を選択して新しいポリシーの仕様を入力します。

13. [[step13 、 Step 13]] 「 * Host Information * 」セクションには、ホストオペレーティングシステムと LUN 形式はすでに表示されていますが、変更することができます。

14. [* Host Mapping] で、 LUN のイニシエータのタイプを選択します。
    - * 既存のイニシエータグループ * ：表示されるリストからイニシエータグループを選択します。
    - * 既存のイニシエータグループを使用する新しいイニシエータグループ * ：新しいグループの名前を指定し、新しいグループの作成に使用するグループを選択します。
    - * ホストイニシエータ * ：新しいイニシエータグループから名前を指定し、 * + イニシエータの追加 * をクリックしてイニシエータをグループに追加します。

15. 「 * Protection * 」セクションで、 LUN の保護を指定します。

SnapMirror を有効にする（ローカルまたはリモート） * を選択する場合は、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。

16. [保存（ Save ）] をクリックします。

LUNが作成され、クラスタとStorage VMに追加されます。

これらのLUNの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

LUNの名前を変更する

概要ページでLUNの名前を変更できます。

手順

1. System Managerで、*[LUN]*をクリックします。
2. 名前を変更するLUNの名前の横にあるをクリックし、LUN名を変更します。
3. [保存（ Save ）] をクリックします。

ONTAP System Managerでストレージを拡張

System Managerを使用してボリュームまたはLUNのサイズを拡張し、ホストで使用できるスペースを増やすことができます。LUNのサイズは、LUNが含まれるボリュームのサイズを超えることはできません。

ONTAP 9.12.1以降では、ボリュームの新しい容量を入力すると、*[ボリュームのサイズ変更]*ウィンドウに、ボリュームのサイズ変更によるデータスペースとSnapshotリザーブへの影響が表示されます。

- [ボリュームのサイズを拡張する]
- LUNのサイズを拡張する

また、既存のボリュームにLUNを追加することもできます。ONTAP 9.8 以降で System Manager を使用する場合、プロセスは異なります。

- 既存のボリュームへのLUNの追加（ONTAP 9.8）
- 既存のボリュームへのLUNの追加（ONTAP 9.7）

ボリュームのサイズを拡張する

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. サイズを拡張するボリュームの名前にカーソルを合わせます。
3. をクリックします。
4. 「 * 編集 * 」を選択します。
5. 容量の値を増やします。
6. [Existing（既存）]および[New（新規）]のデータスペースとSnapshotリザーブの詳細を確認します。

LUNのサイズを拡張する

手順

1. [*Storage] > [LUNs] をクリックします。
2. サイズを拡張するLUNの名前にカーソルを合わせます。
3. をクリックします。
4. 「 * 編集 * 」を選択します。

5. 容量の値を増やします。

既存のボリュームへの**LUN**の追加（**ONTAP 9.8**）

ONTAP 9 8以降では、System Managerを使用して、すでにLUNが1つ以上ある既存のボリュームにLUNを追加できます。

手順

1. [*Storage] > [LUNs] をクリックします。
2. [* 追加 +*] をクリックします。
3. [Add LUNs] ウィンドウのフィールドに値を入力します。
4. [* その他のオプション *] を選択します。
5. 「 Group with related LUN* 」チェックボックスを選択します。
6. ドロップダウンフィールドで、別のLUNを追加するボリューム上のLUNを選択します。
7. 残りのフィールドに入力します。* Host Mapping * の場合は、次のいずれかのオプションボタンをクリックします。
   - * 既存のイニシエータグループ * を使用すると、リストから既存のグループを選択できます。
   - * 新しいイニシエータグループ * を指定すると、フィールドに新しいグループを入力できます。

既存のボリュームへの**LUN**の追加（**ONTAP 9.7**）

ONTAP 9 .7でSystem Managerを使用して既存のボリュームにLUNを追加するには、先にクラシックビューに切り替えてください。

手順

1. ONTAP 9.7でSystem Managerにログインします。
2. [クラシック表示（ Classical View ）] をクリックする。
3. Storage > LUNs > Create * を選択します
4. LUNを作成するための詳細を指定してください。
5. LUNを追加する既存のボリュームまたはqtreeを指定します。

ONTAP System Manager による圧縮、コンパクション、重複排除を使用してストレージ スペースを節約します。

AFF以外のクラスタのボリュームでは、重複排除、データ圧縮、およびデータコンパクションを一緒に、または個別に実行して、最適なスペース削減効果を得ることができます。

- 重複排除は、重複するデータブロックを排除します。
- データ圧縮は、データブロックを圧縮して、必要な物理ストレージの量を削減します。
- データコンパクションでは、より少ないスペースにより多くのデータが格納され、ストレージ効率が向上します。

これらのタスクは、 AFF以外のクラスタ上のボリュームでサポートされています。インライン重複排除やインライン圧縮などのすべてのインラインストレージ効率化機能は、 AFFボリュームではデフォルトで有効になっています。

手順

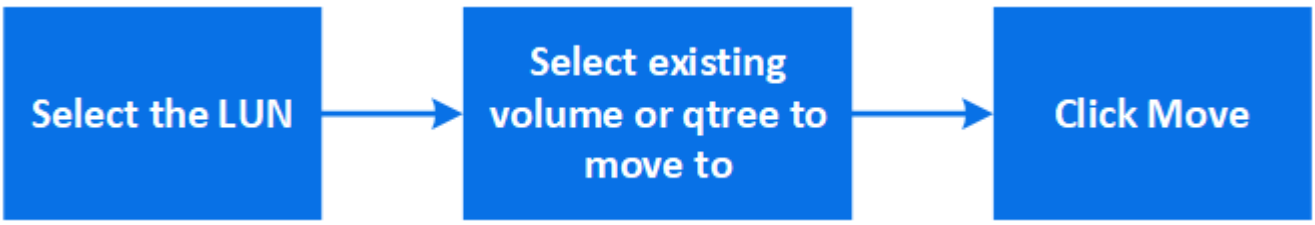
1. [ストレージ]>[ボリューム]*をクリックします。
2. ストレージを保存するボリュームの名前の横にあるをクリックします。
3. をクリックし、[Storage Efficiency]*までスクロールします。
4. オプション：バックグラウンド重複排除を有効にする場合は、チェックボックスがオンになっていることを確認します。
5. オプション：バックグラウンド圧縮を有効にする場合は、ストレージ効率化ポリシーを指定し、チェックボックスがオンになっていることを確認します。
6. オプション：インライン圧縮を有効にする場合は、チェックボックスがオンになっていることを確認します。

ONTAP System Managerを使用してLUNを移動することで負荷を分散します

LUNをStorage VM内の別のボリュームに移動して負荷を分散したり、上位のパフォーマンスサービスレベルのボリュームに移動してパフォーマンスを向上させたりできます。

移動の制限

- 同じボリューム内のqtreeにLUNを移動することはできません。
- CLIを使用してファイルから作成したLUNは、System Managerでは移動できません。
- データを提供しているオンラインのLUNは移動できません。
- デスティネーションボリュームに割り当てられているスペースにLUNを格納できない場合は、LUNを移動できません（ボリュームで自動拡張が有効になっている場合も同様）。
- SnapLockボリュームのLUNはSystem Managerでは移動できません。



をクリック"]

手順

1. [*Storage] > [LUNs] をクリックします。
2. 移動する LUN を選択し、 * Move * をクリックします。
3. LUNの移動先の既存のボリュームを選択します。ボリュームにqtreeが含まれている場合は、qtreeを選択します。

移動処理の実行中、LUNは元のボリュームとデスティネーションボリュームの両方に表示されます。

ONTAP System Managerを使用してボリュームを別の階層に移動することで負荷を分散します

ONTAP 9.9.1 以降では、アクティブおよび非アクティブなデータ ストレージの分析に基づいてボリュームを移動できます。 ONTAP 9.8 では、System Manager を使用してボリュームを別の階層に移動し、負荷を分散することもできます。

詳細については、以下を参照してください。 "ファイルシステム分析の概要" 。

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. 移動する 1 つ以上のボリュームを選択し、 * 移動 * をクリックします。
3. ボリュームの移動先となる既存の階層（アグリゲート）を選択します。

Ansible Playbook を使用して、ONTAP System Manager でボリュームまたは LUN を追加または編集します。

9.1以降では、ONTAP 9 ManagerでAnsible Playbookを使用して、ボリュームまたはLUNを追加または編集できます。

この機能を使用すると、ボリュームまたはLUNを追加または編集するときに、同じ構成を複数回使用したり、同じ構成をわずかに変更して使用したりできます。

Ansible Playbookを有効または無効にする

System ManagerでAnsible Playbookの使用を有効または無効にすることができます。

手順

1. System Managerで、クラスタ設定ページのUI設定に移動します。
   - クラスタ > 設定 *
2. [*UI 設定 *] で、スライダスイッチを [有効] または [無効] に変更します。

ボリューム構成をAnsible Playbookに保存

ボリュームの構成を作成または変更するときに、構成をAnsible Playbookファイルとして保存できます。

手順

1. ボリュームを追加または編集します。
   - 音量 > 追加 * （または * 音量 > 編集 * ）
2. ボリュームの設定値を指定または編集します。
3. 「 * Save to Ansible Playbook * 」を選択して、構成を Ansible Playbook ファイルに保存してください。

次のファイルを含むzipファイルがダウンロードされます。

- **variable.yaml**：ボリュームを追加または編集するために入力または変更した値。
- **volumeAdd.yaml**（または **volumeEdit.yaml**）：ファイルから入力を読み取るときに値を作成または変更するために必要なテストケース `variable.yaml`。

LUN構成をAnsible Playbookに保存

LUNの構成を作成または変更するときに、構成をAnsible Playbookファイルとして保存できます。

手順

1. LUNを追加または編集します。
   - lun> 追加 * （または * lun > 編集 * ）
2. LUNの設定値を指定または編集します。
3. Ansible Playbook に保存 * を選択して、構成を Ansible Playbook ファイルに保存：

   次のファイルを含むzipファイルがダウンロードされます。

   - **variable.yaml**：LUNを追加または編集するために入力または変更した値。
   - **lunAdd.yaml**（または **lunEdit.yaml**）：ファイルから入力を読み取るときに値を作成または変更するために必要なテストケース `variable.yaml`。

グローバル検索結果からAnsible Playbookファイルをダウンロード

グローバル検索を実行するときに、Ansible Playbookファイルをダウンロードできます。

手順

1. 検索フィールドに「ボリューム」または「LUN」または「Playbook」と入力します。
2. 検索結果として、「ボリューム管理 (Ansible Playbook)」または「LUN 管理 (Ansible Playbook)」を見つけます。
3. をクリックし てAnsible Playbookファイルをダウンロードします。

Ansible Playbookファイルの操作

Ansible Playbookファイルを変更して実行することで、ボリュームとLUNの構成を指定できます。

タスクの内容

操作 (「追加」または「編集」) を実行するには、次の 2 つのファイルを使用します。

状況	使用する変数ファイル	使用する実行ファイル
ボリュームの追加	`volumeAdd-varible.yaml`	`valueAdd.yaml`
ボリュームの編集	`volumeEdit-variable.yaml`	`volumeEdit.yaml`
LUNを追加する	`lunAdd-variable.yaml`	`lunAdd.yaml`
LUNの編集	`lunEdit-variable.yaml`	`lunEdit.yaml`

手順

1. 変数ファイルを変更します。

   ファイルには、ボリュームまたはLUNの設定に使用するさまざまな値が含まれています。

   - 値を変更しない場合は、コメントを付けたままにします。
   - 値を変更する場合は、コメントを削除します。

2. 関連付けられた実行ファイルを実行します。

   実行ファイルには、変数ファイルから入力を読み取るときに値を作成または変更するために必要なテストケースが含まれています。

3. ユーザのログインクレデンシャルを入力します。

ONTAP System Managerでストレージ効率ポリシーを管理する

ONTAP 9 8以降では、System Managerを使用して、FASシステムでStorage VMの効率化ポリシーを有効化、無効化、追加、編集、削除できます。

この機能はAFFシステムでは使用できません。

手順

1. Storage > Storage VM* を選択します
2. 効率化ポリシーを管理するStorage VMを選択します。
3. タブで、[効率化ポリシー]*セクションを選択します → 。そのStorage VMの効率化ポリシーが表示されます。

次のタスクを実行できます。

- * 効率化ポリシーを有効または無効にするには、 Status 列の切り替えボタンをクリックします。
- * Add * をクリックして効率化ポリシーを追加します。
- *編集*効率化ポリシー。ポリシー名の右にあるをクリックし、*編集*を選択します。 ⋮
- *削除*効率化ポリシーを選択するには、ポリシー名の右にあるをクリックして ⋮ *削除*を選択します。

効率化ポリシーのリスト

- * 自動 *

  重複排除をバックグラウンドで継続的に実行するように指定します。このポリシーは、新しく作成したすべてのボリューム、およびアップグレードしたボリュームのうち、バックグラウンド重複排除の対象として手動で設定されていないボリュームに対して設定されます。ポリシーをデフォルトまたはその他のポリシーに変更すると' autoポリシーは無効になります

  ボリュームがAFF以外のシステムからAFF システムに移動した場合、デスティネーションノードで「auto」ポリシーがデフォルトで有効になります。ボリュームがAFF ノードからAFF以外のノードに移動すると、デフォルトでデスティネーションノードの「auto」ポリシーが「inline-only」ポリシーに置き換えられます。

- * ポリシー *

  効率化ポリシーの名前を指定します。

- * ステータス *

  効率化ポリシーのステータスを指定します。ステータスは、次のいずれかになります。

  - 有効

    効率化ポリシーを重複排除処理に割り当てることができることを示します。

  - 無効にする

    効率化ポリシーが無効であることを示します。[ステータス]ドロップダウンメニューを使用してポリシーを有効にし、あとで重複排除処理に割り当てることができます。

- * 実行者 *

  ストレージ効率化ポリシーをスケジュールに基づいて実行するか、しきい値（変更ログのしきい値）に基づいて実行するかを指定します。

- * QoS ポリシー *

  ストレージ効率化ポリシーのQoSタイプを指定します。QoSタイプは次のいずれかになります。

  - 背景

    QoSポリシーをバックグラウンドで実行するように指定します。これにより、クライアント処理へのパフォーマンスの影響を軽減できます。

  - ベストエフォート

    QoSポリシーをベストエフォートベースで実行するように指定します。これにより、システムリソースの利用率を最大限に高めることができます。

- * 最大実行時間 *

  効率化ポリシーの最大実行時間を指定します。この値を指定しない場合、処理が完了するまで効率化ポリシーが実行されます。

詳細領域

効率化ポリシーのリストの下の領域には、選択した効率化ポリシーに関する追加情報が表示されます。これには、スケジュールベースのポリシーの場合はスケジュールの名前と詳細、しきい値ベースのポリシーの場合はしきい値などの情報が含まれます。

ONTAP System Managerでクォータを使用してリソースを管理する

System.7以降では、ONTAP 9 Managerを使用して使用クォータを設定および管理できます。

ONTAP CLIを使用して使用クォータを設定および管理する場合は、を参照してください"Logical Storage Managementの略"。

ONTAP 9 .7以前の従来のOnCommand System Managerを使用して使用クォータを設定および管理している場合は、ご使用のリリースに対応する次の資料を参照してください。

- "ONTAP 9.7および9.6のドキュメント"
- "ONTAP 9.5ドキュメント"
- "ONTAP 9.4ドキュメント"
- "ONTAP 9.3ドキュメント"

クォータの概要

クォータを使用すると、ユーザ、グループ、またはqtreeによって使用されるディスクスペースやファイル数を制限したり、追跡したりできます。クォータは、特定のボリュームまたはqtreeに適用されます。

クォータを使用すると、ボリューム内のリソース使用量を追跡および制限したり、リソース使用量が特定のレベルに達したときに通知したりできます。

クォータには、ソフトクォータとハードクォータがあります。ソフトクォータでは、指定された制限を超えるとONTAPによって通知が送信されますが、ハードクォータでは、指定された制限を超えると書き込み処理が失敗します。

ONTAP System Managerでクォータを設定してリソースの使用を制限する

クォータを追加して、クォータターゲットが使用できるディスクスペースの量を制限します。

クォータにはハードリミットとソフトリミットを設定できます。

ハードクォータはシステムリソースにハードリミットを適用します。この制限を超えることになる処理はすべて失敗します。ソフトクォータは、リソース使用量が一定のレベルに達すると警告メッセージを送信しますが、データアクセス処理には影響しないため、クォータを超過する前に適切に対処できます。

手順

1. [ストレージ]>[クォータ]*をクリックします。
2. [追加]*をクリックします。

ONTAP System Manager でテストするためのボリュームと LUN のクローンを作成する

ボリュームやLUNをクローニングして、テスト用の書き込み可能な一時的なコピーを作成できます。クローンには、データの現在のポイントインタイムの状態が反映されます。クローンを使用すると、追加のユーザに本番環境のデータへのアクセスを許可することなく、データへのアクセスを許可することもできます。

開始する前に

ストレージシステムにFlexCloneライセンスがインストールされている必要があります "インストール済み"。

ボリュームのクローニング

次の手順で、ボリュームのクローンを作成します。

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. クローニングするボリュームの名前の横にあるをクリックします ⋮ 。
3. リストから * Clone * を選択します。
4. クローンの名前を指定し、その他のオプションを選択します。
5. * Clone * をクリックし、ボリュームのリストにボリュームクローンが表示されていることを確認します。

また、ボリュームの詳細を表示したときに表示される「 * Overview * 」からボリュームをクローニングすることもできます。

LUNのクローニング

アクティブボリューム内のLUNをクローニングして、LUNのコピーを作成できます。これらのFlexClone LUNは、アクティブボリューム内の元のLUNの読み書き可能なコピーです。

スペースリザーブFlexClone LUNには、親のスペースリザーブLUNと同じ量のスペースが必要です。FlexClone LUNのスペースをリザーブしない場合は、FlexClone LUNに対する変更に対応できるだけの十分なスペースがボリュームにあることを確認する必要があります。

> この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"データのクローンを作成します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

例 **11.** 手順

System Manager

1. [*Storage] > [LUNs] をクリックします。
2. クローニングするLUNの名前の横にあるをクリックします ⋮ 。
3. リストから * Clone * を選択します。
4. クローンの名前を指定し、その他のオプションを選択します。
5. [* Clone*] をクリックし、 LUN のリストに LUN クローンが表示されていることを確認します。

また、 LUN の詳細を表示したときに表示される「 * Overview * 」から LUN のクローンを作成することもできます。

LUNクローンを作成すると、スペースが必要になったときのクローンの削除がSystem Managerで自動的に有効になります。

CLI

1. クローンを作成する前に、LUNがigroupにマッピングされていないこと、または書き込まれていないことを確認します。
2. コマンドを使用し `lun show`て、LUNが存在することを確認します。

   ```
   lun show -vserver vs1
   ```

   ```
   Vserver  Path               State     Mapped    Type      Size
   -------- ----------------- --------- --------- -------- -------
   vs1      /vol/vol1/lun1    online   unmapped  windows  47.07MB
   ```

3. コマンドを使用し `volume file clone create`て、FlexClone LUNを作成します。

   ```
   volume file clone create -vserver vs1 -volume vol1 -source-path lun1
   -destination-path/lun1_clone
   ```

   FlexClone LUNを自動削除できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してボリュームにこのFlexClone LUNを作成する場合は、すべてのFlexClone LUNに対して自動削除を有効にする必要があります。

4. コマンドを使用し `lun show`て、LUNが作成されたことを確認します。

   ```
   lun show -vserver vs1
   ```

   ```
   Vserver  Path                      State    Mapped   Type      Size
   -------- ------------------------ -------- -------- -------- ------
   vs1      /vol/volX/lun1           online   unmapped windows  47.07MB
   vs1      /vol/volX/lun1_clone     online   unmapped windows  47.07MB
   ```

ONTAP System Managerで情報を検索、フィルタリング、並べ替える

System Managerでは、さまざまな操作、オブジェクト、および情報トピックを検索できます。また、テーブルデータで特定のエントリを検索することもできます。

System Managerでは、次の2種類の検索を実行できます。

- [グローバル検索]

  各ページの上部にあるフィールドに検索引数を入力すると、System Managerはインターフェイス全体で一致するものを検索します。その後、結果をソートおよびフィルタできます。

  ONTAP 9 .12.1以降では、NetAppサポートサイトの検索結果も表示され、関連するサポート情報へのリンクが表示されます。

- [表-グリッド検索]

  ONTAP 9 .8以降では、表グリッドの上部にあるフィールドに検索引数を入力すると、その表の列と行だけが検索されて一致するものが検索されます。

グローバル検索

System Managerの各ページの上部にあるグローバル検索フィールドを使用して、さまざまなオブジェクトやインターフェイスでの操作を検索できます。たとえば、さまざまなオブジェクトの名前、ナビゲータ列（左側）のページ、「ボリュームの追加」や「ライセンスの追加」などのさまざまな操作項目、外部のヘルプトピックへのリンクなどを検索できます。結果をフィルタリングしてソートすることもできます。

> より正確な結果を得るには、ログインしてから1分後、オブジェクトを作成、変更、または削除してから5分後に、検索、フィルタ、ソートを実行してください。

検索結果の取得

検索では大文字と小文字は区別されません。さまざまなテキスト文字列を入力して、必要なページ、アクション、または情報トピックを検索できます。最大20件の結果が表示されます。検索結果がさらに見つかった場合は、 * Show More * をクリックしてすべての結果を表示できます。次に、一般的な検索例を示します。

検索のタイプ	検索文字列の例	検索結果の例
オブジェクト名	vol_	Storage VM の vol_lun_dest ： svm0 （ボリューム） /vol/ vol … est1/lun Storage VM ： svm0 （ LUN ） svm0 ： vol_lun_dest1 ロール： Destination （関係）
インターフェイス内の場所	ボリューム	ボリュームの追加 (アクション) 保護–概要 (ページ) 削除されたボリュームのリカバリ (ヘルプ)
アクション別	追加	ボリュームの追加（アクション）ネットワーク–概要（ページ）ボリュームと LUN の拡張（ヘルプ）

ヘルプコンテンツ	SAN	ストレージ–概要（ページ） SAN の概要（ヘルプ）データベース用の SAN ストレージのプロビジョニング（ヘルプ）

NetAppサポートサイトでのグローバル検索結果

ONTAP 9 12.1以降では、Active IQデジタルアドバイザ（デジタルアドバイザとも呼ばれます）に登録されているユーザに対して、System Managerの製品情報など、NetAppサポートサイトの情報へのリンクを提供する別の列が表示されます。

検索結果には次の情報が含まれます。

- * HTML、PDF、EPUB、またはその他の形式でドキュメントにリンクする情報のタイトル*。
- コンテンツタイプ。製品ドキュメントトピック、KnowledgeBase記事、または別の種類の情報のいずれであるかを識別します。
- *コンテンツのサマリー概要 *。
- *最初に公開された日付。
- *更新日*最終更新日。

次の操作を実行できます。

アクション	結果
ONTAP System Manager*をクリックし、検索フィールドにテキストを入力します。	検索結果には、System Managerに関するNetApp Support Site 情報が含まれます。
[すべての製品]をクリックし、検索フィールドにテキストを入力します。	検索結果には、System Managerだけでなく、すべてのネットアップ製品のNetApp Support Site 情報も含まれます。
検索結果をクリックします。	NetApp Support Site の情報は、別のブラウザウィンドウまたはタブに表示されます。
「その他の結果を見る」をクリックします。	10件を超える結果がある場合は、10番目の結果の後に[さらに結果を表示（See more results）]をクリックして、さらに結果を表示できます。[さらに結果を表示（See more results）]をクリックするたびに、可能な場合は別の10件の結果が表示されます。
リンクをコピーします。	リンクがクリップボードにコピーされます。ファイルまたはブラウザウィンドウにリンクを貼り付けることができます。
をクリックします	結果が表示されるパネルはピンで固定され、別のパネルで作業しても表示されたままになります。
をクリックします。 ×	結果パネルはピン固定されず、閉じられます。

検索結果のフィルタリング

次の例に示すように、フィルタを使用して結果を絞り込むことができます。

フィルタ	構文	検索文字列の例
オブジェクトタイプ別	<type>：<objectName>	ボリューム：vol_2
オブジェクトサイズ別	<type><size-symbol><number><units>	LUN < 500MB
破損ディスク	「壊れたディスク」または「不健全なディスク」	正常でないディスク
ネットワークインターフェイス	<IP address>	172.22.108.21

検索結果のソート

すべての検索結果を表示すると、アルファベット順にソートされます。結果をソートするには、をクリック Filter し、結果のソート方法を選択します。

表-グリッド検索

ONTAP 9 .8以降では、情報が表グリッド形式で表示されるたびに、検索ボタンが表の上部に表示されます。

- 検索 * をクリックすると、検索引数を入力できるテキストフィールドが表示されます。System Manager では、テーブル全体が検索され、指定した検索引数に一致するテキストを含む行のみが表示されます。

アスタリスク（ * ）を「ワイルドカード」文字として使用し、文字の代わりに使用できます。たとえば、を検索する `vol*`と、次のような行が表示される場合があります。

- vol_122_D9
- vol_lun_dest1
- vol2866
- volspec1
- volum_dest_765
- ボリューム
- volume_new4
- volume9987

CLIを使用した論理ストレージ管理

CLIを使用した論理ストレージ管理の概要

ONTAP CLIを使用すると、FlexVolボリュームの作成と管理、FlexCloneテクノロジを使用したボリューム、ファイル、LUNの効率的なコピーの作成、qtreeとクォータの作成、重複排除や圧縮などの効率化機能の管理を行うことができます。

これらの手順は、次の状況で使用する必要があります。

- ONTAP FlexVol volumeの機能とStorage Efficiency機能の範囲について理解する必要がある。
- System Managerや自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

ボリュームの作成と管理

ボリュームの作成

コマンドを使用すると、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create`。

タスクの内容

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームの作成時に指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、コマンドを使用して、SVMネームスペースでボリュームを_mount_theにする必要があります `volume mount`。

開始する前に

- 新しいボリュームの SVM とそのボリュームにストレージを提供するアグリゲートが、すでに存在している必要があります。
- SVM に関連付けられているアグリゲートのリストがある場合は、アグリゲートがそのリストに含まれている必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. ボリュームを作成します。

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user
   user_name_or_number -group group_name_or_number -junction-path junction_path
   [-policy export_policy_name]
   ```

   > `-security style` `-user`、、 `-group`、、 `-junction-path`の `-policy`各オプションは、NASネームスペース専用です。

   の選択肢は `-junction-path`次のとおりです。

   - ルートの直下。例： `/new_vol`

     新しいボリュームを作成し、 SVM のルートボリュームに直接マウントされるように指定することができます。

- 既存のディレクトリの下（例： `/existing_dir/new_vol`

  新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

たとえば、新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は `/new_dir/new_vol`、SVMのルートボリュームにジャンクションされている新しい親ボリュームを最初に作成する必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドは、SVMとアグリゲートに `aggr1`users1という名前の新しいボリュームを作成し `vs1.example.com`ます。新しいボリュームは、で使用でき `/users`ます。ボリュームのサイズは750GBで、ボリュームギャランティのタイプはvolume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

次のコマンドでは、「 home4` 」という名前の新しいボリュームを SVM 「 vs1.example.com`" 」およびアグリゲート「 aggr1 」に作成します。ディレクトリは `/eng/`vs1 SVMのネームスペース内にすでに存在し、新しいボリュームがで使用可能になります `/eng/home。これがネームスペースのホームディレクトリになります。 `/eng/`ボリュームのサイズは750GBで、ボリュームギャランティのタイプは（デフォルト）です `volume。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- -------  -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

ONTAPで大容量ファイルと大容量ファイルのサポートを有効にする

ONTAP 9.12.1 P2以降では、新しいボリュームを作成したり既存のボリュームを変更したりして、サポートされる最大ボリュームサイズを300TB、最大サイズを60PB、最大ファイル（LUN）サイズを128TBに変更したりできます"FlexGroupボリューム"。

開始する前に

- ONTAP 9 .12.1 P2以降がクラスタにインストールされている。
- SnapMirror関係にあるソースクラスタで大容量ボリュームのサポートを有効にする場合は、ソースボリュームをホストするクラスタとデスティネーションボリュームをホストするクラスタにONTAP 9 .12.1 P2以降がインストールされている必要があります。
- クラスタ管理者またはSVM管理者である。
- この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

新しいボリュームを作成する

ステップ

1. 大容量ボリュームでファイルのサポートが有効になっているボリュームを作成します。

```
volume create -vserver <svm_name> -volume <volume_name> -aggregate
<aggregate_name> -is-large-size-enabled true
```

例

次の例は、大容量ボリュームとファイルサイズのサポートを有効にして新しいボリュームを作成します。

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large
-size-enabled true
```

既存のボリュームを変更する

ステップ

1. ボリュームを変更して、大容量ボリュームとファイルのサポートを有効にします。

```
volume modify -vserver <svm_name> -volume <volume_name> -is-large-size
-enabled true
```

例

次の例は、大容量のボリュームとファイルサイズをサポートするように既存のボリュームを変更します。

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

2. ボリュームを再マウントして新しい設定をアクティブ化します。

```
volume unmount -vserver <svm_name> -volume <volume_name>
```

```
volume mount -vserver <svm_name> -volume <volume_name>
```

関連情報

- "ONTAP NFSボリュームを作成する"
- "ONTAPコマンド リファレンス"

SANホリユウム

SANボリュームプロビジョニングの概要

ONTAPには、SANボリュームプロビジョニングの基本的なオプションがいくつかあります。各オプションでは、ONTAPブロック共有テクノロジに必要なボリュームスペースとスペースを、それぞれ異なる方法で管理します。環境に最適なオプションを選択できるように、各プロビジョニングオプションの仕組みを理解しておく必要があります。

SAN LUNとNAS共有を同じFlexVol volumeに配置することは推奨されません。SAN LUNとNAS共有用に別 々 のFlexVolをプロビジョニングする必要があります。これにより、管理とレプリケーションの展開が簡素化されます。また、Active IQ Unified Manager（旧OnCommand Unified Manager）でのFlexVolボリュームのサポート方法も並行しています。

ボリュームのシンプロビジョニング

シンプロビジョニング ボリュームは、作成時に追加のスペースが確保されません。ボリュームにデータが書き込まれるときに、書き込み処理に対応するために必要なアグリゲート内のストレージをボリュームが要求します。シンプロビジョニング ボリュームを使用する場合はアグリゲートをオーバーコミットできますが、アグリゲートの空きスペースが不足すると、必要なスペースをボリュームが確保できなくなる可能性があります。

シンプロビジョニングFlexVol volumeを作成するには、そのオプションをに `none`設定し `-space-guarantee`ます。

ボリュームのシックプロビジョニング

シックプロビジョニングは、ボリューム内のブロックにいつでも書き込むことができるように、作成時にアグリゲートから十分なストレージが確保されます。シックプロビジョニングを利用するようにボリュームを設定した場合は、ONTAPの任意のStorage Efficiency機能（圧縮や重複排除など）を使用して、さらに大容量のストレージ要件にも事前に対応できます。

シックプロビジョニングFlexVol volumeを作成するには、その（サービスレベル目標）オプションをに `thick`設定し `-space-slo`ます。

ボリュームのセミシックプロビジョニング

セミシックプロビジョニングを使用するボリュームを作成すると、ONTAPはボリュームサイズに対応するためにアグリゲートからストレージスペースを確保します。ブロック共有テクノロジでブロックが使用されているためにボリュームの空きスペースが不足している場合、ONTAPは保護データオブジェクト（Snapshot、FlexCloneファイルおよびLUN）を削除して保持しているスペースを解放します。上書きに必要なスペースを確保できる速度でONTAPが保護データオブジェクトを削除できるかぎり、書き込み処理は引き続き成功します。これは「ベストエフォート」書き込み保証と呼ばれます。

セミシックプロビジョニングを使用するボリュームでは、Storage Efficiencyテクノロジ（重複排除、圧縮、コンパクションなど）を使用できません。

セミシックプロビジョニングFlexVol volumeを作成するには、その（サービスレベル目標）オプションをに`semi-thick`設定し`-space-slo`ます。

スペースリザーブファイルおよびスペースリザーブ**LUN**での使用

スペースリザーブファイルまたはスペースリザーブLUNは、ストレージの作成時にストレージが割り当てられるファイルまたはLUNです。ネットアップではこれまで、スペース・リザベーションが無効になっているLUN （スペース・リザーブなしの LUN ）を「シン・プロビジョニング LUN 」と呼んできました。

スペースリザーブなしのファイルは、一般に「シンプロビジョニングされたファイル」とは呼ばれません。

次の表に、スペースリザーブファイルおよびスペースリザーブLUNで使用できる3つのボリュームプロビジョニングオプションの主な違いを示します。

ボリュームのプロビジョニング	**LUN/file** のスペースリザベーション	上書き	保護データ [2]	ストレージ効率 [3]
シック	サポート対象	保証された ^1	保証	サポート対象
シン	効果なし	なし	保証	サポート対象
セミシック	サポート対象	ベストエフォート ^1 ^	ベストエフォート	サポート対象外

- メモ *

1. 上書きを保証したり、ベストエフォートで上書きを保証できるようにするには、LUNまたはファイルでスペースリザベーションが有効になっている必要があります。
2. 保護データには、Snapshot、自動削除の対象としてマークされたFlexCloneファイルおよびLUN（バックアップクローン）が含まれます。
3. Storage Efficiencyには、重複排除、圧縮、自動削除の対象としてマークされていないFlexCloneファイルとLUN（アクティブクローン）、およびFlexCloneサブファイル（コピーオフロードに使用）が含まれます。

SCSIシンプロビジョニングLUNのサポート

ONTAPは、T10 SCSIシンプロビジョニングLUNとNetAppシンプロビジョニングLUNをサポートしています。T10 SCSIシンプロビジョニングを使用すると、ホストアプリケーションは、ブロック環境向けのLUNのスペース再生機能やスペース監視機能などのSCSI機能をサポートできます。T10 SCSIシンプロビジョニングがSCSIホストソフトウェアでサポートされている必要があります。

LUNのT10シンプロビジョニングのサポートを有効または無効にするには、ONTAP設定を使用し `space-allocation`ます。ONTAPの設定を使用し `space-allocation enable`て、LUNでT10 SCSIシンプロビジョニングを有効にします。

その `[-space-allocation {enabled|disabled}]`コマンドの"ONTAPコマンド リファレンス" T10 シン プロビジョニングのサポートを有効/無効にする方法、および LUN で T10 SCSI シン プロビジョニングを有効にする方法については、さらに詳しい情報があります。

ボリュームプロビジョニングオプションの設定

スペース要件に応じて、シンプロビジョニング、シックプロビジョニング、またはセミシックプロビジョニング用にボリュームを設定できます。

タスクの内容

このオプションをに `thick`設定する `-space-slo`と、次の処理が実行されます。

- ボリューム全体がアグリゲートに事前に割り当てられます。コマンドまたは `volume modify`コマンドを使用してボリュームのオプションを設定する `-space-guarantee`ことはできません `volume create`。
- 上書きに必要なスペースの100%がリザーブされます。コマンドを使用してボリュームのオプションを設定する `-fractional-reserve`ことはできません。 `volume modify`

このオプションをに `semi-thick`設定する `-space-slo`と、次の処理が実行されます。

- ボリューム全体がアグリゲートに事前に割り当てられます。コマンドまたは `volume modify`コマンドを使用してボリュームのオプションを設定する `-space-guarantee`ことはできません `volume create`。
- スペースは上書き用にリザーブされません。コマンドを使用して、ボリュームのオプションを設定 `-fractional-reserve`できます `volume modify`。
- Snapshotの自動削除が有効になります。

ステップ

1. ボリュームのプロビジョニングオプションを設定します。

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
   ```

   AFFシステムおよびAFF以外のDPボリュームでは、この `-space-guarantee`オプションのデフォルトはです `none`。それ以外の場合は、デフォルトでになり `volume`ます。既存のFlexVolボリュームの場合は、コマンドを使用し `volume modify`てプロビジョニングオプションを設定します。

   次のコマンドを使うと、 SVM vs1 上の vol1 にシンプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

次のコマンドを使うと、 SVM vs1 上の vol1 にシックプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

次のコマンドを使うと、 SVM vs1 上の vol1 にセミシックプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

関連情報

- "ボリュームの作成"
- "ボリュームの変更"

ONTAPでのボリュームまたはアグリゲートのスペース使用量を確認する

ONTAPである機能を有効にすると、想定よりも多くのスペースが消費されることがあります。ONTAPでは、消費されるスペースを、ボリューム、アグリゲート内のボリュームのフットプリント、およびアグリゲートの3つの観点から判断できます。

スペース割り当ての表示

ボリューム、アグリゲート、またはその両方でのスペース消費またはスペース不足により、ボリュームのスペースが不足することがあります。スペース使用量の機能別の内訳をさまざまな観点から確認することで、調整や無効化が必要な機能や、その他の対処（アグリゲートやボリュームのサイズ拡張など）を講じておくべきかどうかを判断できます。

スペース使用量は、以下の観点から詳細に確認できます。

- ボリュームのスペース使用量

  Snapshotによる使用量など、ボリューム内のスペース使用量の詳細が表示されます。

  コマンドを使用し `volume show-space`て、ボリュームのスペース使用量を確認します。

  の詳細については `volume show-space`、を"ONTAPコマンド リファレンス"参照してください。

  ONTAP 9 14.1以降では、が有効になっているボリュームについて、温度に基づくStorage Efficiency（TSSE）コマンドによって報告されるボリュームで使用されているスペース量 `volume show-space -physical used`には、TSSEによって実現されるスペース削減量が含まれます。

- アグリゲート内のボリュームの占有量

ボリュームのメタデータも含め、アグリゲートで各ボリュームが使用しているスペースの量に関する詳細を把握できます。

コマンドを使用して `volume show-footprint`、アグリゲートに対するボリュームの占有量を確認します。

の詳細については `volume show-footprint`、を"ONTAPコマンド リファレンス"参照してください。

- アグリゲートのスペース使用量

  アグリゲートに含まれるすべてのボリュームのボリューム占有量、アグリゲートSnapshot用にリザーブされたスペース、およびその他のアグリゲートメタデータの合計が表示されます。

  WAFLでは、アグリゲート レベルのメタデータおよびパフォーマンス用に総ディスク スペースの10%が予約されます。アグリゲート内のボリュームを維持するためのスペースはWAFLリザーブから使用され、変更することはできません。

  ONTAP 9.12.1以降では、30TBを超えるアグリゲートのWAFLリザーブが、AFFプラットフォームおよびFAS500fプラットフォームの10%から5%に削減されました。ONTAP 9.14.1以降では、これと同じ削減効果がすべてのFASプラットフォームのアグリゲートに適用されるため、アグリゲートの使用可能スペースが5%増加します。

  コマンドを使用し `storage aggregate show-space`て、アグリゲートのスペース使用量を確認します。

  の詳細については `storage aggregate show-space`、を"ONTAPコマンド リファレンス"参照してください。

テープバックアップや重複排除などの特定の機能では、ボリュームとアグリゲートの両方から直接メタデータ用のスペースが使用されます。これらの機能では、ボリュームとボリュームのフットプリントの観点でスペース使用量が異なります。

ボリュームメタデータとデータ指標のレポート

これまで、いくつかのボリュームスペース指標では、消費された合計データ量がメタデータとユーザデータの2つの指標の組み合わせとして報告されてきました。ONTAP 9 .15.1以降では、メタデータとユーザデータのメトリックが別 々 にレポートされます。これをサポートするために、2つの新しいメタデータカウンタが導入されました。

- 合計-メタデータ

  このカウンタは、ボリューム内のメタデータの合計サイズを表示します。アグリゲートに格納されているボリュームメタデータは含まれません。レポートそれは別 々 にユーザーによって割り当てられた論理データを決定するのに役立ちます。

- メタデータ容量の合計

  ボリュームに格納されているメタデータとアグリゲートに格納されているボリュームメタデータの合計です。アグリゲート内のボリュームのメタデータフットプリントの合計が表示されます。それを別 々 に報告することは、ユーザーによって割り当てられた物理データを決定するのに役立ちます。

また、いくつかの既存のカウンタが更新され、メタデータコンポーネントが削除されてユーザデータのみが表示されるようになりました。

- ユーザデータ
- ボリュームのデータ容量

これらの変更により、ユーザによって消費されるデータを、より正確に確認できるようになります。これには、より正確にチャージバックを決定できることなど、いくつかのメリットがあります。

関連情報

- "NetAppナレッジベース: スペースの使用状況"
- "ONTAP 9にアップグレードすることで、ストレージ容量の5%を解放できます。12.1"

SnapshotとLUNの自動削除を有効にしてスペースを管理

SnapshotおよびFlexClone LUNを自動的に削除するポリシーを定義して有効にすることができます。SnapshotとFlexClone LUNを自動的に削除すると、スペース使用量の管理に役立ちます。

タスクの内容

読み書き可能ボリュームのSnapshotや読み書き可能な親ボリュームのFlexClone LUNを自動的に削除できます。読み取り専用ボリューム（SnapMirrorデスティネーションボリュームなど）のSnapshotの自動削除は設定できません。

ステップ

1. コマンドを使用して、Snapshotの自動削除ポリシーを定義して有効にします `volume snapshot autodelete modify`。

   ニーズに合わせたポリシーの詳細と定義については、を"ONTAPコマンド リファレンス"参照して `volume snapshot autodelete modify`ください。

   次のコマンドは、Storage Virtual Machine（SVM）vs0.example.comに属するボリュームvol3に対して、Snapshotの自動削除を有効にし、トリガーをに設定します `snap_reserve`。

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger snap_reserve
   ```

   次のコマンドは、Storage Virtual Machine（SVM）vs0.example.comに属するボリュームvol3に対して、Snapshotと対象としてマークされたFlexClone LUNの自動削除を有効にします。

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger volume -commitment try -delete-order
   oldest_first -destroy-list lun_clone,file_clone
   ```

アグリゲートレベルのSnapshotは、ボリュームレベルのSnapshotとは動作が異なり、ONTAPによって自動的に管理されます。アグリゲートSnapshotを削除するオプションは常に有効になっており、スペース使用量の管理に役立ちます。

アグリゲートに対してtriggerパラメータがに設定されている場合、`snap_reserve`Snapshotはリザーブされているスペースが容量のしきい値を超えるまで維持されます。したがって、triggerパラメータがに設定されていない場合でも、`snap_reserve`Snapshotは自動的に削除されるため、コマンドでSnapshotに使用されているスペースはと表示され `0`ます。また、アグリゲートでSnapshotによって使用されるスペースは空きスペースとみなされ、コマンドのavailable spaceパラメータに含まれます。

ボリュームがフルになったときに自動的にスペースを確保するように設定する

FlexVol では、 ONTAP がフルに近くなったときに、さまざまな方法でボリュームの空きスペースを自動的に増やすことができます。ONTAP で使用できる方法、およびアプリケーションとストレージアーキテクチャの要件に応じた順序を選択します。

タスクの内容

ONTAP では、ボリュームがフルになったときに、次のいずれかまたは両方の方法を使用して空きスペースを自動的に増やすことができます。

- ボリュームのサイズを増やす（ *autogrow* ）。

  この方法は、ボリュームの包含アグリゲートに、より大容量のボリュームに対応できる十分なスペースがある場合に便利です。ボリュームの最大サイズは ONTAP で設定できます。この拡張は、ボリュームに書き込まれるデータの量に基づいて、現在の使用済みスペースの量と設定されているしきい値に基づいて自動的にトリガーされます。

  自動拡張は、Snapshotの作成時にトリガーされません。Snapshotの作成を試みたときに十分なスペースがないと、自動拡張が有効になっていてもSnapshotの作成は失敗します。

- Snapshot、FlexCloneファイル、またはFlexClone LUNを削除します。

  たとえば、クローンボリュームまたはLUN内のSnapshotにリンクされていないSnapshotを自動的に削除するようにONTAPを設定したり、ONTAPで最初に削除するSnapshot（最も古いSnapshotまたは最も新しいSnapshot）を定義したりできます。また、ONTAPがスナップショットの削除を開始するタイミング（ボリュームがフルに近くなったときや、ボリュームのスナップショットリザーブがフルに近くなったときなど）を指定することもできます。

両方 ONTAP の方法を有効にする場合、ボリュームがフルに近くなったときに最初にどちらの方法を試行するかを指定できます。最初の方法でボリュームの追加のスペースが十分に確保されない場合は、次に ONTAP がもう一方の方法を試行します。

デフォルトでは、 ONTAP は最初にボリュームサイズの拡張を試行します。削除したSnapshotはリストアできないため、ほとんどの場合、デフォルトの構成を使用することを推奨します。ただし、可能なかぎりボリュームのサイズを拡張しないようにする必要がある場合は、ボリュームのサイズを拡張する前にSnapshotを削除するようにONTAPを設定できます。

手順

1. ボリュームがフルに近くなったときにONTAPでボリュームサイズの拡張を試行するようにするには、コマ

ンドでモードを指定して `grow`、ボリュームの自動拡張機能を有効にします `volume autosize`。の詳細については `volume autosize`、を"ONTAPコマンド リファレンス"参照してください。

ボリュームが拡張される際には、関連付けられているアグリゲートの空きスペースが使用されることに注意してください。スペースが必要なときは常にボリュームを拡張して対処する場合は、関連付けられているアグリゲートの空きスペースを監視し、必要に応じて追加する必要があります。

2. ボリュームがフルに近くなったときにONTAPでSnapshot、FlexCloneファイル、またはFlexClone LUNを削除する場合は、それらのタイプのオブジェクトの自動削除を有効にします。
3. ボリュームの自動拡張機能と自動削除機能の両方を有効にした場合は、コマンドにオプションを指定して `-space-mgmt-try-first`、ONTAPがボリュームの空きスペースを確保するために最初に実行する方法を選択します。 `volume modify`の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

   最初にボリュームのサイズを拡張することを指定するには（デフォルト）、を使用し `volume_grow`ます。Snapshotの削除を先に指定するには、を使用し `snap_delete`ます。

ボリュームのサイズを自動的に拡張および縮小するように設定する

必要なスペースに応じてFlexVolボリュームを自動的に拡張または縮小するように設定できます。自動拡張を使用すると、ボリュームがスペース不足になるのを防ぐことができます（アグリゲートが追加のスペースを提供できる場合）。自動縮小では、ボリュームが必要以上に大きくなるのを防ぎ、アグリゲートのスペースを解放して他のボリュームで使用できるようにします。

タスクの内容

自動縮小は、変化するスペース需要に対応するために自動拡張と組み合わせてのみ使用でき、単独で使用することはできません。自動縮小を有効にすると、自動拡張と自動縮小の処理が無限に繰り返されるのを防ぐために、ONTAPはボリュームの縮小動作を自動的に管理します。

ボリュームが拡張されると、格納できるファイルの最大数が自動的に増える可能性があります。ボリュームが縮小されても格納できるファイルの最大数は変わらず、ボリュームが縮小前のファイルの最大数に対応するサイズよりも小さくなることはありません。そのため、自動縮小でボリュームを最初のサイズまで縮小できるとは限りません。

デフォルトでは、ボリュームは自動拡張が有効になっているサイズの120%まで拡張できます。ボリュームをそれよりも大きく拡張できるようにする必要がある場合は、それに応じてボリュームの最大サイズを設定する必要があります。

開始する前に

FlexVol volumeがオンラインになっている必要があります。

ステップ

1. ボリュームのサイズを自動的に拡張および縮小するように設定します。

   ```
   volume autosize -vserver SVM_name -volume volume_name -mode grow_shrink
   ```

   次に、test2という名前のボリュームで自動サイズ変更を有効にするコマンドを示します。ボリュームの60%が使用された時点で縮小を開始するように設定します。拡張を開始するタイミングおよびボリュームの最大サイズについてはデフォルト値のままです。

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

自動縮小と**Snapshot**の自動削除の両方を有効にするための要件

自動縮小機能は、特定の設定要件を満たしていれば、Snapshotの自動削除と一緒に使用できます。

自動縮小機能とSnapshotの自動削除機能の両方を有効にする場合は、設定が次の要件を満たしている必要があります。

- Snapshotの削除を試行する前に、ボリュームサイズの拡張を試行するようにONTAPを設定する必要があります（ `-space-mgmt-try-first`オプションをに設定する必要があります `volume_grow`）。
- Snapshotの自動削除のトリガーは、ボリュームがフルである必要があります（ `trigger`パラメータをに設定する必要があります `volume`）。

自動縮小機能と**Snapshot**の削除

自動縮小機能はFlexVol volumeのサイズを縮小するため、ボリュームSnapshotが自動的に削除されるタイミングにも影響します。

自動縮小機能は、次の方法でボリュームSnapshotの自動削除と連動します。

- オートサイズモードとSnapshotの自動削除の両方が有効になっている場合 `grow_shrink`、ボリュームサイズが縮小されるとSnapshotの自動削除がトリガーされることがあります。

  これは、Snapshotリザーブがボリュームサイズの割合（デフォルトは5%）に基づいており、その割合が小さいボリュームサイズに基づいているためです。これにより、スナップショットがリザーブからオーバーフローし、自動的に削除される可能性があります。

- オートサイズモードが有効になっている場合 `grow_shrink`にSnapshotを手動で削除すると、ボリュームの自動縮小がトリガーされることがあります。

FlexVol volumeのスペース不足アラートと過剰割り当てアラートへの対処

ONTAP では、 FlexVol ボリュームがスペース不足になると、該当するボリュームにスペースを追加して対処できるように EMS メッセージが表示されます。アラートの種類とその対処方法を理解しておくと、データの可用性を維持するのに役立ちます。

ボリュームが _full_と みなされるのは、アクティブファイルシステム（ユーザデータ）で使用可能なボリューム内のスペースの割合がしきい値（設定可能）を下回った場合です。ボリュームが過剰割り当ての状態になると、メタデータを格納したり基本的なデータアクセスをサポートしたりするために ONTAP で使用されるスペースが不足した状態になります。他の目的のために確保されているスペースを使用してボリュームを引き続き利用できる場合もありますが、スペースリザベーションやデータの可用性を維持できなくなるリスクがあります。

過剰割り当てには論理的なものと物理的なものがあります。_ 論理的な過剰割り当て _ は、スペースリザベーションなど、以降のスペースコミットメントを受け入れるためにリザーブされたスペースが別の目的に使用されたことを意味します。_ 物理的な過剰割り当て _ は、ボリュームで使用する物理ブロックが不足した状態を示します。この状態のボリュームには、書き込みができなくなったり、オフラインになったりするリスクがあり、これが原因でコントローラが停止してしまう可能性もあります。

ボリュームは、メタデータ用に使用またはリザーブされているスペースによって 100% を超えることがあります。100% を超えているからといって必ずしも過剰割り当ての状態であるとは限りません。qtreeレベルおよびボリュームレベルの共有が同じFlexVolまたはSCVMMプールに存在する場合、qtreeはFlexVol共有上のディレクトリとして表示されます。したがって、誤って削除しないように注意する必要があります。

次の表に、ボリュームのスペース不足アラートと過剰割り当てアラートについて、問題への対処方法と対処しなかった場合のリスクを示します。

アラートの種類	**EMS** レベル	設定可能かどうか	定義	対処方法	対処しなかった場合はリスクがあります
ほぼフルです	デバッグ	Y	ファイルシステムがこのアラートに設定されたしきい値（デフォルトは95%）を超えています。この割合は `Used`、合計からSnapshotリザーブのサイズを引いた値です。	• ボリュームサイズノカクチョウ • ユーザデータを減らす	書き込み処理やデータ可用性に対する影響はまだありません。
フル	デバッグ	Y	ファイルシステムがこのアラートに設定されたしきい値（デフォルトは98%）を超えています。この割合は `Used`、合計からSnapshotリザーブのサイズを引いた値です。	• ボリュームサイズノカクチョウ • ユーザデータを減らす	書き込み処理やデータ可用性に対する影響はまだありませんが、ボリュームは書き込み処理ができなくなるリスクのある段階に近づいています。

アラートの種類	**EMS** レベル	設定可能かどうか	定義	対処方法	対処しなかった場合はリスクがあります
論理的な過剰割り当て	SVC エラーです	n	ファイルシステムがフルの状態で、さらにメタデータ用のボリュームのスペースが不足しています。	• ボリュームサイズノカクチョウ • Snapshotの削除 • ユーザデータを減らす • ファイルまたは LUN のスペースリザベーションを無効にします	リザーブされていないファイルに対する書き込み処理が失敗する可能性があり
物理的な過剰割り当て	ノードエラー	n	ボリュームで書き込み可能な物理ブロックが不足しています。	• ボリュームサイズノカクチョウ • Snapshotの削除 • ユーザデータを減らす	書き込み処理ができなくなり、データの可用性を維持できなくなるリスクがあり、ボリュームがオフラインになる可能性もあります。

あるボリュームで、フルの割合が上下してしきい値にかかるたびに、 EMS メッセージが生成されます。ボリュームのフルレベルがしきい値を下回ると、 `volume ok`EMSメッセージが生成されます。

アグリゲートのスペース不足アラートと過剰割り当てアラートへの対処

ONTAP では、アグリゲートがスペース不足になると、該当するアグリゲートにスペースを追加して対処できるように EMS メッセージが表示されます。アラートの種類とその対処方法を理解しておくと、データの可用性を維持するのに役立ちます。

アグリゲートが _full_と みなされるのは、アグリゲート内のボリュームで使用可能なスペースの割合が事前に定義されたしきい値を下回った場合です。アグリゲートが過剰割り当ての状態になると、メタデータを格納したり基本的なデータアクセスをサポートしたりするために ONTAP で使用されるスペースが不足した状態になります。他の目的のために確保されているスペースを使用してアグリゲートを引き続き利用できる場合もありますが、アグリゲートに関連付けられているボリュームのボリュームギャランティやデータの可用性を維持できなくなるリスクがあります。

過剰割り当てには論理的なものと物理的なものがあります。_ 論理的な過剰割り当て _ は、ボリュームギャランティなどの以降のスペースコミットメントを考慮してリザーブされたスペースが別の目的に使用されていることを示します。_ 物理的な過剰割り当て _ は、アグリゲートで使用する物理ブロックが不足した状態を示します。この状態のアグリゲートには、書き込みができなくなったり、オフラインになったりするリスクがあり、これが原因でコントローラが停止してしまう可能性もあります。

次の表に、アグリゲートのスペース不足アラートと過剰割り当てアラートについて、問題への対処方法と対処しなかった場合のリスクを示します。

アラートの種類	EMSレベル	設定可能かどうか	定義	対処方法	対処しなかった場合はリスクがあります
ほぼフルです	デバッグ	n	ボリュームに割り当てられたスペース量（ギャランティも含む）がこのアラートのしきい値（ 95% ）を超えています。この割合は `Used`、合計からSnapshotリザーブのサイズを引いた値です。	• アグリゲートにストレージを追加しています • ボリュームを縮小するか削除する • スペースが多い別のアグリゲートにボリュームを移動する • ボリュームギャランティの削除（設定）ボリュームギャランティノサクジョ（セッテイ） `none`	書き込み処理やデータ可用性に対する影響はまだありません。
フル	デバッグ	n	ファイルシステムがこのアラートのしきい値（ 98% ）を超えています。この割合は `Used`、合計からSnapshotリザーブのサイズを引いた値です。	• アグリゲートにストレージを追加しています • ボリュームを縮小するか削除する • スペースが多い別のアグリゲートにボリュームを移動する • ボリュームギャランティの削除（設定）ボリュームギャランティノサクジョ（セッテイ） `none`	アグリゲート内のボリュームのボリュームギャランティを維持できなくなったり、ボリュームに対する書き込み処理ができなくなったりするリスクがあります。

アラートの種類	EMSレベル	設定可能かどうか	定義	対処方法	対処しなかった場合はリスクがあります
論理的な過剰割り当て	SVCエラーです	n	ボリューム用にリザーブされたスペースがフルの状態で、さらにメタデータ用のアグリゲートのスペースが不足しています。	• アグリゲートにストレージを追加しています • ボリュームを縮小するか削除する • スペースが多い別のアグリゲートにボリュームを移動する • ボリュームギャランティの削除（設定）ボリュームギャランティノサクジョ（セッテイ） `none`	アグリゲート内のボリュームのボリュームギャランティを維持できなくなったり、ボリュームに対する書き込み処理ができなくなったりするリスクがあります。
物理的な過剰割り当て	ノードエラー	n	アグリゲートで書き込み可能な物理ブロックが不足しています。	• アグリゲートにストレージを追加しています • ボリュームを縮小するか削除する • スペースが多い別のアグリゲートにボリュームを移動する	アグリゲート内のボリュームに対する書き込み処理ができなくなり、データの可用性を維持できなくなるリスクがあり、アグリゲートがオフラインになる可能性もあります。最悪の場合、ノードが停止することもあります。

あるアグリゲートで、フルの割合が上下してしきい値にかかるたびに、 EMS メッセージが生成されます。アグリゲートのフルレベルがしきい値を下回ると、 `aggregate ok`EMSメッセージが生成されます。

フラクショナルリザーブヲセッテイスルサイノコウリョジコウ

フラクショナルリザーブは、 _lun overwrite reserve _ とも呼ばれ、 FlexVol ボリューム内のスペースリザーブ LUN およびファイルのオーバーライトリザーブを無効にすることができます。これにより、ストレージ利用率を最大限に高めることができます。

スペース不足による書き込み処理の失敗が悪影響を及ぼす環境では、この構成で課される可能性のある要件を理解しておく必要があります。

フラクショナルリザーブ設定はパーセンテージで表され、有効な値は `0`と `100`パーセントのみです。フラクショナルリザーブ設定はボリュームの属性です。フラクショナルリザーブを設定して `0`ストレージ利用率を高めます。ただし、ボリュームの空きスペースがなくなると、ボリュームギャランティがに設定されていても、ボリュームに格納されたデータにアクセスするアプリケーションでデータを利用できなくなる可能性が

あります `volume`。ただし、ボリュームを適切に構成して使用すれば、書き込みが失敗する可能性を最小限に抑えることができます。次の要件の_all_が満たされている場合、ONTAPはフラクショナルリザーブがに設定されたボリュームに対して「ベストエフォート」書き込み保証を提供します `0`。

- 重複排除を使用していない
- 圧縮を使用していない
- FlexCloneサブファイルは使用されていません
- すべてのFlexCloneファイルとFlexClone LUNで自動削除が有効になっている

  これはデフォルト設定ではありません。FlexCloneファイルやFlexClone LUNの自動削除は、作成時に設定するか作成後に変更して明示的に有効にする必要があります。

- ODXコピー オフロードとFlexCloneコピー オフロードを使用していない
- ボリュームギャランティがに設定されている `volume`
- ファイルまたはLUNのスペースリザベーション： `enabled`
- ボリュームのSnapshotリザーブの設定： `0`
- ボリュームSnapshotの自動削除は `enabled`、コミットメントレベルが、 `destroy`削除リストが、 `lun_clone,vol_clone,cifs_share,file_clone,sfsr`トリガーが `volume`

  この設定では、必要に応じてFlexCloneファイルとFlexClone LUNも削除されます。

- 上記の要件をすべて満たしていても変更率が高いと、まれにSnapshotの自動削除が遅れてボリュームのスペースが不足することがあります。
- 上記のすべての要件が満たされ、Snapshotが使用されていない場合、ボリューム書き込みでスペースが不足することはありません。

また、必要に応じてボリュームの自動拡張機能を使用することで、ボリュームSnapshotが自動的に削除される可能性を減らすことができます。自動拡張機能を有効にする場合は、関連付けられたアグリゲートの空きスペースを監視する必要があります。アグリゲートの空きスペースがなくなり、ボリュームを拡張できなくなると、ボリュームの空きスペースが不足したときに削除されるSnapshotが増える可能性があります。

上記の設定要件をすべて満たすことができず、ボリュームのスペース不足を防ぐ必要がある場合は、ボリュームのフラクショナルリザーブ設定をに設定する必要があります `100`。これにより、事前に確保する必要がある空きスペースは増えますが、上記のテクノロジを使用する場合でもデータ変更処理が確実に実行されるようになります。

フラクショナル リザーブ設定のデフォルト値と有効値は、ボリュームのギャランティによって異なります。

ボリュームギャランティ	デフォルトのフラクショナルリザーブ	有効な値
ボリューム	100	0、100
なし	0	0、100

ボリュームのファイルと**inode**の使用量を確認する

FlexVolには、格納できるファイルの最大数があります。CLIコマンドを使用して、FlexVolボリュームの（パブリック）inodeの数を増やしてファイル数の上限に達しないようにする必要があるかどうかを判断できます。

タスクの内容

パブリックinodeは、空き（ファイルに関連付けられていない）または使用済み（ファイルを参照している）のいずれかです。ボリュームの空きinodeの数は、ボリュームの合計inode数から使用済みinodeの数（ファイル数）を引いた値です。

qtreeレベルおよびボリュームレベルの共有が同じFlexVolまたはSCVMMプールに存在する場合、qtreeはFlexVol共有上のディレクトリとして表示されます。したがって、誤って削除しないように注意する必要があります。

手順

1. ボリュームのinode使用量を表示するには、次のコマンドを入力します。

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files-used
```

例

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files-used
Vserver Name: vs1
Files Used (for user-visible data): 98
```

ストレージ**QoS**で**FlexVol volume I/O**パフォーマンスを制御、監視

FlexVol ボリュームへの入出力（ I/O ）パフォーマンスは、ストレージ QoS ポリシーグループにボリュームを割り当てることによって制御できます。I/O パフォーマンスを制御することで、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりできます。

タスクの内容

ポリシーグループは最大スループット制限（ 100MB/s など）を適用します。ポリシーグループは最大スループットを指定せずに作成することもでき、ワークロードの制御に先立ってパフォーマンスを監視できます。

SVM 、 LUN 、およびファイルをポリシーグループに割り当てることもできます。

ポリシーグループへのボリュームの割り当てについては、次の要件に注意してください。

- ボリュームは、ポリシーグループが属するSVMに含まれている必要があります。

  SVM は、ポリシーグループを作成するときに指定します。

- ボリュームをポリシーグループに割り当てた場合、そのボリュームを含むSVMまたはそのボリュームの子LUNまたは子ファイルをポリシーグループに割り当てることはできません。

ストレージQoSの使用方法の詳細については、を参照して"システムアドミニストレーションリファレンス"ください。

手順

1. コマンドを使用し `qos policy-group create`て、ポリシーグループを作成します。
2. `volume create`コマンドまたは `volume modify`コマンドでパラメータを指定し `-qos-policy-group`て、ボリュームをポリシーグループに割り当てます。
3. パフォーマンスデータを表示するには、コマンドを使用し `qos statistics`ます。
4. 必要に応じて、コマンドを使用し `qos policy-group modify`てポリシーグループの最大スループット制限を調整します。

関連情報

- "QoS ポリシーグループ"
- "ボリュームの作成"
- "ボリュームの変更"
- "QoS統計"

FlexVol volumeの削除

不要になったFlexVol volumeは削除できます。

開始する前に

削除するボリューム内のデータにアプリケーションがアクセスしていない必要があります。

誤ってボリュームを削除した場合は、"NetAppナレッジベース: ボリュームリカバリキューの使用方法" 。

手順

1. ボリュームがマウントされている場合は、アンマウントします。

```
volume unmount -vserver vserver_name -volume volume_name
```

2. ボリュームがSnapMirror関係の一部である場合は、コマンドを使用して関係を削除します `snapmirror delete`。
3. ボリュームがオンラインの場合は、ボリュームをオフラインにします。

```
volume offline -vserver vserver_name volume_name
```

4. ボリュームを削除します。

```
volume delete -vserver vserver_name volume_name
```

結果

関連付けられているクォータポリシーおよびqtreeとともに、ボリュームが削除されます。

関連情報

- "SnapMirrorの削除"
- "ボリュームのアンマウント"
- "ボリュームはオフライン"
- "volume delete"

偶発的なボリューム削除の防止

デフォルトのボリューム削除動作は、誤って削除したFlexVolボリュームのリカバリに役立ちます。

`volume delete`タイプがまたは `DP`（コマンドの出力に表示される `volume show`）ボリュームに対する要求を
`RW`実行すると、そのボリュームは一部削除された状態に移行します。デフォルトでは、完全に削除されるまでに少なくとも12時間はリカバリキューに保持されます。

関連情報

- "ボリュームリカバリキューの使用方法"
- "volume delete"
- "volume show"

ONTAPの**FlexVol**ボリュームの管理用コマンド

ONTAP CLIには、FlexVolボリュームを管理するための固有のコマンドが用意されています。必要な作業に応じて、次のコマンドを使用してFlexVolボリュームを管理できます。

状況	使用するコマンド
ボリュームをオンラインにします	`volume online`
ボリュームのサイズを変更する	`volume size`
ボリュームに関連付けられているアグリゲートを特定します	`volume show`
Storage Virtual Machine （ SVM ）のすべてのボリュームに関連付けられているアグリゲートを判別する	`volume show -vserver -fields aggregate`
ボリュームの形式を決定します	`volume show -fields block-type`
ジャンクションを使用してボリュームを別のボリュームにマウントします	`volume mount`

状況	使用するコマンド
ボリュームを制限状態にします	`volume restrict`
ボリュームの名前を変更します	`volume rename`
ボリュームをオフラインにします	`volume offline`

の詳細については `volume`、を"ONTAPコマンド リファレンス"参照してください。

スペース情報を表示するコマンド

コマンドと `volume`コマンドを使用して `storage aggregate`、アグリゲート、ボリューム、およびそれらのSnapshotでスペースがどのように使用されているかを確認します。

表示する情報	使用するコマンド

アグリゲート（使用済みスペースの割合と使用可能スペースの割合に関する詳細、Snapshotリザーブのサイズ、およびその他のスペース使用量情報を含む）	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

アグリゲートでのディスクとRAIDグループの使用方法およびRAIDのステータス	`storage aggregate show-status`
特定のSnapshotを削除した場合に再利用されるディスクスペースの量	`volume snapshot compute-reclaimable`（アドバンスト）

ボリュームによって使用されているスペースの量	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

アグリゲート内でボリュームによって使用されているスペースの量	`volume show-footprint`

関連情報

- "storage aggregate show"
- "ストレージアグリゲートショースペース"
- "ストレージアグリゲートのステータス表示"
- "volume snapshot compute-reclaimableを使用します"
- "volume show"

ボリュームの移動とコピー

FlexVol volumeの移動の概要

容量利用率やパフォーマンスの向上、およびサービスレベル契約を満たすために、ボリュームを移動またはコピーできます。FlexVol ボリュームの移動の仕組みを理解しておくと、ボリュームの移動がサービスレベル契約を満たすかどうかの判断や、ボリューム移動がボリューム移動プロセスのどの段階にあるかを把握するのに役立ちます。

FlexVolボリュームは、1つのアグリゲートまたはノードから同じStorage Virtual Machine（SVM）内の別のアグリゲートまたはノードに移動されます。ボリュームを移動しても、移動中にクライアントアクセスが中断されることはありません。

ボリューム移動処理のカットオーバーフェーズ中は、 FlexVol ボリュームの FlexClone ファイルまたは FlexClone LUN を作成することはできません。

ボリュームの移動は次のように複数のフェーズで行われます。

- 新しいボリュームがデスティネーションアグリゲート上に作成されます。
- 元のボリュームのデータが新しいボリュームにコピーされます。

  この間、元のボリュームはそのままで、クライアントからアクセス可能です。

- 移動プロセスの最後に、クライアントアクセスが一時的にブロックされます。

  この間にソースボリュームからデスティネーションボリュームへの最終レプリケーションが実行され、ソースボリュームとデスティネーションボリュームの ID がスワップされ、デスティネーションボリュームがソースボリュームに変更されます。

- 移動が完了すると、クライアントトラフィックが新しいソースボリュームにルーティングされ、クライアントアクセスが再開されます。

クライアントアクセスのブロックはクライアントが中断とタイムアウトを認識する前に終了するため、移動によってクライアントアクセスが中断されることはありません。デフォルトでは、クライアントアクセスは30秒間ブロックされます。アクセスが拒否されている間にボリューム移動操作が完了しなかった場合、この最終フェーズは中止されてクライアントアクセスが許可されます。デフォルトでは、最終フェーズは3回試行されます。3回目の試行後、システムは1時間待機してから最後のフェーズシーケンスを再試行します。ボリューム移動処理の最後のフェーズは、ボリューム移動が完了するまで実行されます。

ボリュームを移動する際の考慮事項と推奨事項

ボリュームを移動する際の考慮事項と推奨事項がいくつかあります。これらは、移動するボリュームおよびMetroClusterなどのシステム構成に基づいています。ボリュームを移動する前に、関連する問題をすべて理解しておく必要があります。

一般的な考慮事項と推奨事項

- クラスタのリリースファミリーをアップグレードする場合は、クラスタ内のすべてのノードをアップグレードするまでボリュームを移動しないでください。

この推奨事項により、ボリュームを新しいリリースファミリーから古いリリースファミリーに誤って移動しないようにすることができます。

- ソースボリュームに整合性がある必要があります。
- 関連Storage Virtual Machine（SVM）に1つ以上のアグリゲートを割り当てている場合、デスティネーションアグリゲートは割り当てられたアグリゲートのいずれかである必要があります。
- ボリュームは新しいバージョンのONTAPにのみ移動してください。
- テイクオーバーされたCFOアグリゲートとの間でボリュームを移動することはできません。
- LUNを含むボリュームでNVFAILが有効になっていない場合、移動後にNVFAILが有効になります。
- ボリュームをFlash Poolアグリゲートから別のFlash Poolアグリゲートに移動できます。
  - ボリュームのキャッシングポリシーも一緒に移動されます。
  - ボリュームのパフォーマンスに影響する可能性があります。
- ボリュームは、Flash PoolアグリゲートとFlash Poolアグリゲート以外のアグリゲートの間で移動できます。
  - ボリュームを Flash Pool アグリゲートから Flash Pool アグリゲート以外のアグリゲートに移動する場合、ボリュームのパフォーマンスに影響する可能性があることを示す警告メッセージが ONTAP に表示され、続行するかどうかの確認を求められます。
  - ボリュームをFlash Poolアグリゲート以外のアグリゲートからFlash Poolアグリゲートに移動すると、ONTAPによってキャッシングポリシーが割り当てられ `auto`ます。
- ボリュームには、そのボリュームが配置されているアグリゲートの保管データの保護機能が適用されます。NSEドライブで構成されるアグリゲートからNSEドライブで構成されないアグリゲートにボリュームを移動すると、NSEの保存データは保護されなくなります。
- ONTAP 9.13.1以前からONTAP 9.15.1以降にFabricPool最適化ボリュームを移動する場合は、"NetAppナレッジベース: CONTAP-307878 - ソースONTAPが 9.14.1 未満で、宛先が 9.14.1 より大きい場合、FabricPoolの最適化されたボリュームの移動中に予期しない再起動が発生する" 。

FlexCloneボリュームに関する考慮事項と推奨事項

- FlexCloneボリュームは、移動中にオフラインにすることはできません。
- コマンドを実行せずに、同じSVM内の同じノードまたは別のノード上のアグリゲート間でFlexCloneボリュームを移動できます。 `vol clone split start`

  FlexCloneでボリューム移動処理を開始すると、移動プロセス中にクローンボリュームが別のアグリゲートにスプリットされます。クローンボリュームでのボリューム移動が完了すると、移動したボリュームはクローンとしてではなく、以前の親ボリュームとのクローン関係がない独立したボリュームとして表示されます。

- FlexCloneボリュームのSnapshotは、クローンを移動しても失われません。
- FlexCloneの親ボリュームをアグリゲート間で移動できます。

  FlexCloneの親ボリュームを移動すると、一時ボリュームが取り残され、すべてのFlexCloneボリュームの親ボリュームとして機能します。この一時ボリュームに対して実行できるのはオフラインにする処理と削除する処理だけで、それ以外の処理は実行できません。すべてのFlexCloneボリュームがスプリットまたは破棄されると、一時ボリュームは自動的にクリーンアップされます。

- FlexCloneの子ボリュームは、移動後はFlexCloneボリュームではなくなります。

- FlexCloneの移動処理とFlexCloneのコピー処理またはスプリット処理を同時に実行することはできません。
- クローンスプリット処理が実行中の場合、ボリュームの移動が失敗することがあります。

  クローンスプリット処理が完了するまでボリュームを移動しないでください。

MetroClusterに関する考慮事項と推奨事項

- MetroCluster構成でボリュームを移動する際に、ソースクラスタのデスティネーションアグリゲートに一時ボリュームが作成されると、ミラーされているが同期されていないアグリゲート内のボリュームに対応する一時ボリュームのレコードもサバイバークラスタに作成されます。
- カットオーバー前にMetroClusterスイッチオーバーが発生した場合、デスティネーションボリュームは一時ボリューム（タイプがTMPのボリューム）として記録されます。

  稼働している（ディザスタリカバリ）クラスタで移動ジョブが再開され、障害が報告され、移動に関連する項目（一時ボリュームなど）がすべてクリーンアップされます。クリーンアップを正しく実行できない場合は、必要なクリーンアップを実行するようシステム管理者に警告するEMSが生成されます。

- カットオーバーフェーズが開始されてから移動ジョブが完了する（つまり、移動がデスティネーションアグリゲートを参照するようにクラスタを更新できる段階に達した）前にMetroClusterのスイッチオーバーが発生した場合、移動ジョブは稼働している（ディザスタリカバリ）クラスタで再開され、最後まで実行されます。

  移動に関連する項目は、一時ボリューム（元のソース）を含めてすべてクリーンアップされます。クリーンアップを正しく実行できない場合は、必要なクリーンアップを実行するようシステム管理者に警告するEMSが生成されます。

- スイッチオーバーされたサイトに属するボリュームに対して実行中のボリューム移動処理がある場合、MetroClusterのスイッチバックは強制的かどうかに関係なく実行できません。

  サバイバーサイトのローカルボリュームに対してボリューム移動処理を実行中の場合、スイッチバックはブロックされません。

- 実行中のボリューム移動処理がある場合、MetroClusterの強制的でないスイッチオーバーはブロックされますが、MetroClusterの強制的なスイッチオーバーはブロックされません。

SAN環境でのボリューム移動に関する要件

SAN環境でボリュームを移動する前に、準備をしておく必要があります。

LUNまたはネームスペースを含むボリュームを移動する前に、次の要件を満たす必要があります。

- ボリュームに 1 つ以上の LUN が含まれている場合は、クラスタ内の各ノードに接続する LUN （ LIF ）ごとに少なくとも 2 つのパスが必要です。

  これにより、単一点障害（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

- ボリュームにネームスペースが含まれている場合は、クラスタで ONTAP 9.6 以降が実行されている必要があります。

ボリューム移動は、ONTAP 9を実行するNVMe構成ではサポートされません。5.

ONTAPボリュームを移動する

ストレージ容量に不均衡がある場合は、FlexVol volumeを同じStorage Virtual Machine（SVM）内の別のアグリゲート、ノード、またはその両方に移動してストレージ容量のバランスを調整できます。

タスクの内容

デフォルトでは、カットオーバー処理が30秒以内に完了しないと再試行されます。デフォルトの動作は、パラメータと `-cutover-action`パラメータを使用して調整でき `-cutover-window`ます。どちらのパラメータにもadvanced権限レベルが必要です。

このタスクを実行するには、クラスタ管理者である必要があります。

開始する前に

- 8Kアダプティブ圧縮を使用するボリュームを以下のいずれかのプラットフォームに移動する場合は、"ボリュームのアクティブファイルシステムのサイズを増やす"ボリュームを移動する前に。これらのプラットフォームではデータが異なる方法で圧縮されるため、ボリューム レベルではなく集約レベルでスペースが節約されます。この違いのため、ボリュームの移動中にボリュームのスペースが不足するのを防ぐために、ボリュームのアクティブ ファイル システムのサイズを 8k の圧縮節約分だけ増やす必要があります。
  - 専用オフロードプロセッサのストレージ効率をサポートするAFFおよびFASプラットフォーム

    AFFおよびFASプラットフォームの詳細については、"専用オフロードプロセッサのストレージ効率"。
  - AFF Cシリーズプラットフォーム

    参照"Hardware Universe"C シリーズ プラットフォームの完全なリストについては、こちらをご覧ください。
- データ保護ミラーを移動していて、ミラー関係を初期化していない場合は、 `snapmirror initialize`ミラー関係を初期化するコマンド。詳細はこちら `snapmirror initialize`の中で"ONTAPコマンド リファレンス" 。

  ボリュームを移動するには、データ保護のミラー関係を初期化する必要があります。

手順

1. ボリュームを移動できるアグリゲートを決定します。

   ```
   volume move target-aggr show
   ```

   ボリュームに使用できるスペースが十分にあるアグリゲート、つまり利用可能なサイズが移動するボリュームよりも大きいアグリゲートを選択する必要があります。

   次の例は、表示されている任意のアグリゲートにvs2ボリュームを移動できることを示しています。

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9GB          hdd
node12a_aggr3    10.34GB          hdd
node12a_aggr2    10.36GB          hdd
node12a_aggr1    10.36GB          hdd
node12a_aggr4    10.36GB          hdd
5 entries were displayed.
```

の詳細については `volume move target-aggr show`、を"ONTAPコマンド リファレンス"参照してください。

2. 検証チェックを実行して、ボリュームを目的のアグリゲートに移動できることを確認します。

```
volume move start -perform-validation-only
```

の詳細については `volume move start`、を"ONTAPコマンド リファレンス"参照してください。

3. 音量を移動します:

```
volume move start
```

SVM vs2 上の user_max ボリュームを node12a_aggr3 アグリゲートに移動するコマンドを次に示します。移動はバックグラウンドプロセスとして実行されます。

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

4. ボリューム移動操作のステータスを確認します。

```
volume move show
```

次の例は、レプリケーションフェーズを完了し、カットオーバーフェーズにあるボリューム移動の状態を示しています。

```
cluster1::> volume move show
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       user_max   healthy  cutover     -                -
```

コマンド出力に表示されなくなると、ボリューム移動は完了 `volume move show`です。

の詳細については `volume move show`、を"ONTAPコマンド リファレンス"参照してください。

5. オプションで、圧縮による節約を表示します。

```
volume show-footprint -vserver <SVM> -volume <volume_name>
```

ボリュームの移動が完了した直後に自動的に実行される後処理変換スキャンによって、集計レベルでの追加の節約が実現される可能性があります。

関連情報

- "ボリュームを移動する際の考慮事項と推奨事項"

8Kアダプティブ圧縮から移行する前に、 **ONTAP**ボリュームのアクティブファイルシステムを増やす

8k アダプティブ圧縮をサポートするプラットフォームは、ボリューム レベルでスペースを節約します。 AFF C シリーズ プラットフォームおよび 32k 圧縮をサポートするプラットフォームは、集約レベルでスペースを節約します。ボリュームを 8k アダプティブ圧縮からAFF C シリーズ プラットフォームまたは 32k 圧縮のプラットフォームに移行する場合は、ボリュームのアクティブ ファイル システムのサイズを 8k 圧縮による節約分だけ増やす必要があります。これにより、ボリュームの移動中にボリュームの空き領域が不足することがなくなります。

次のシステムは 32k 圧縮をサポートしています。

プラットフォーム	**ONTAP**のバージョン
• AFF A1K用 • AFF A90用 • AFF A70用 • FAS90 • FAS70	9.15.1以降

プラットフォーム	**ONTAP**のバージョン
• AFF A50用 • AFF A30用	9.16.1以降

詳細はこちら"32k圧縮をサポートするAFFおよびFASプラットフォーム" 。

参照"Hardware Universe"AFF C シリーズ プラットフォームの完全なリストについては、こちらをご覧ください。

タスクの内容

ボリューム移動操作を使用してデータを移行する場合は、次の手順を実行します。 SnapMirror操作を使用してデータを移行する場合は、アクティブなファイル システムのサイズを手動で増やす必要はありません。 SnapMirror の宛先ボリュームは、デフォルトでボリュームの自動サイズ設定を使用するため、ボリューム レイヤーではなくアグリゲート レイヤーで圧縮による節約が実現されるため、スペースが不足することは予想されません。

開始する前に

ボリューム上で論理スペースレポートと強制が有効になっていない場合は、オプションで有効にすることができます。 `-is-space-reporting-logical`そして `-is-space-enforcement-logical`パラメータを*true*に設定します。ボリュームの移動前にこれらの設定を有効にすると、8k 圧縮から変換するときにボリューム レイヤーでの圧縮節約損失を収容するのに十分なボリュームの大きさがあるかどうかを評価するのに役立ちます。ボリューム上でこれらの設定を有効にする必要があります。これらの設定を SVM レベルで有効にすると、新しく作成されたボリュームにのみ適用されます。

手順

1. ボリュームの現在のサイズとスナップショット予約を確認します。

```
volume show-space
```

2. ボリュームの圧縮スペース節約を確認します。

```
volume show -vserver -volume -fields compression-space-saved
```

3. ボリュームのアクティブファイルシステムのサイズを、表示されている量だけ増やします。 `compression-space-saved`スナップショットの予約も含みます。

```
volume size -vserver <vserver_name> -volume <volume_name> -new-size
+<size>
```

例

ボリュームが 100 GB で、スナップショット予約が 20% の場合、アクティブ ファイル システムは 80 GB、スナップショット予約は 20 GB になります。アクティブ ファイル システムを 20 GB 増やすには、全体のボリューム サイズに 25 GB を追加する必要があります。つまり、アクティブ ファイル システムに 20 GB、スナップショット リザーブに 5 GB (20%) を追加します。

```
volume size -vserver svm1 -volume volx -size +20GB
```

4. ボリュームのサイズが増加したことを確認します。

```
volume show -vserver <vserver_name> -volume <volume_name> -fields size
```

結果

ボリュームのアクティブなファイル システムのサイズが増加し、ボリュームを移動する準備が整いました。

次の手順

実行する"ボリューム移動"データを移行します。

ONTAPでのボリューム移動用コマンド

ONTAP CLIには、ボリューム移動を管理するための固有のコマンドが用意されています。必要な作業に応じて、次のコマンドを使用してクォータルールとクォータポリシーを管理します。

状況	使用するコマンド
実行中のボリューム移動処理を中止する。	`volume move abort`
アグリゲート間のボリューム移動のステータスを表示します。	`volume move show`
アグリゲート間のボリューム移動を開始する。	`volume move start`
ボリューム移動のターゲットアグリゲートを管理します。	`volume move target-aggr`
移動ジョブのカットオーバーをトリガーする。	`volume move trigger-cutover`
デフォルトの設定が適切でない場合は、クライアントアクセスがブロックされる時間を変更します。	`volume move start`または `volume move modify`パラメータを指定し `-cutover-window`ます。は `volume move modify`advanced権限レベルのコマンドで、 `-cutover-window`はadvanced権限レベルのパラメータです。
クライアントアクセスがブロックされている時間内にボリューム移動処理が完了しなかった場合のシステムの対応を指定する。	`volume move start`または `volume move modify`パラメータを指定し `-cutover-action`ます。は `volume move modify`advanced権限レベルのコマンドで、 `-cutover-action`はadvanced権限レベルのパラメータです。

関連情報

- "ボリューム移動"

ボリュームをコピーする方法

ボリュームをコピーする方法は、コピー先が同じアグリゲートか別のアグリゲートか、および元のボリュームのSnapshotを保持するかどうかによって異なります。ボリュームをコピーすると、ボリュームのスタンドアロンコピーが作成され、テストなどに使用できます。

次の表に、それぞれのコピーの特性と作成に使用する方法を示します。

ボリュームをコピーする状況	使用する方法
同じアグリゲート内にあり、元のボリュームからSnapshotをコピーしない。	元のボリュームの FlexClone ボリュームを作成します。
別のアグリゲートにコピーし、元のボリュームからSnapshotをコピーしない。	元のボリュームのFlexCloneボリュームを作成し、コマンドを使用して別のアグリゲートに移動します `volume move`。
別のアグリゲートに移動し、元のボリュームのすべてのSnapshotを保持します。	SnapMirror を使用して元のボリュームをレプリケートしたあと、 SnapMirror 関係を解除して読み書き可能なボリュームにします。

FlexCloneボリュームを使用して**FlexVol**ボリュームの効率的なコピーを作成する

FlexCloneボリュームの使用の概要

FlexCloneボリュームは、親FlexVol volumeの書き込み可能なポイントインタイムコピーです。FlexCloneボリュームは共通のデータについて親FlexVolと同じデータブロックを共有するため、スペース効率に優れています。FlexCloneボリュームの作成に使用されるSnapshotも親ボリュームと共有されます。

既存のFlexCloneボリュームをクローニングして、別のFlexCloneボリュームを作成できます。LUNとLUNクローンを含むFlexVol volumeのクローンを作成することもできます。

FlexCloneボリュームを親ボリュームからスプリットすることもできます。ONTAP 9 .4以降では、AFFシステムのボリュームギャランティがnonである場合、FlexCloneのスプリット処理では物理ブロックが共有され、データはコピーされません。したがって、AFFシステムのFlexCloneボリュームのスプリットは、ONTAP 9 .4以降のリリースの他のFASシステムのFlexCloneスプリット処理よりも高速です。

2種類のFlexClone（読み書き可能FlexCloneボリュームとデータ保護FlexCloneボリューム）を作成できます。通常のFlexVol volumeの読み書き可能FlexCloneボリュームは作成できますが、データ保護FlexCloneボリュームの作成にはSnapVaultセカンダリボリュームのみを使用する必要があります。

FlexCloneボリュームを作成する

データ保護FlexCloneボリュームは、SnapMirrorデスティネーションボリュームまたはSnapVaultセカンダリボリュームである親FlexVol volumeから作成できます。ONTAP 9.7以降では、FlexGroupボリュームからFlexCloneボリュームを作成できます。FlexCloneボリュームの作成後は、FlexCloneボリュームが存在する間は親ボリュームを削除できません。

開始する前に

- クラスタにFlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。
- クローニングするボリュームがオンラインである必要があります。

> MetroCluster構成では、ボリュームをFlexCloneボリュームとして別のSVMにクローニングすることはできません。

FlexVolまたはFlexGroupのFlexCloneボリュームを作成する

ステップ

1. FlexCloneボリュームを作成します。

```
volume clone create
```

> 読み書き可能な親ボリュームから読み書き可能なFlexCloneボリュームを作成する場合は、ベースSnapshotを指定する必要はありません。クローンのベースSnapshotとして使用するSnapshotを指定しない場合、ONTAPはSnapshotを作成します。親ボリュームがデータ保護ボリュームの場合は、FlexCloneボリュームを作成するためのベースSnapshotを指定する必要があります。

例

- 次のコマンドは、親ボリュームvol1から読み書き可能FlexCloneボリュームvol1_cloneを作成します。

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume
vol1
```

- 次に、ベースSnapshot snap1を使用して、親ボリュームdp_volからデータ保護FlexClone vol_dp_cloneを作成するコマンドを示します。

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent
-volume dp_vol -parent-snapshot snap1
```

任意のSnapLockタイプのFlexCloneを作成する

`non-snaplock`RWボリュームのFlexCloneを作成するときに、RW .13.1以降でONTAP 9は、`enterprise`3つのSnapLockタイプのいずれかを指定でき`compliance`ます。デフォルトでは、FlexCloneボリュームは親ボリュームと同じSnapLockタイプで作成されます。ただし、FlexCloneボリュームの作成時にオプションを使用すると、デフォルトの設定を上書きでき `snaplock-type`ます。

パラメータにオプションを指定 `snaplock-type`する `non-snaplock`と、SnapLockの親ボリュームからSnapLockタイプ以外のFlexCloneボリュームを作成して、必要に応じてデータを迅速にオンラインに戻すことができます。

詳細については、をご覧ください "SnapLock"。

開始する前に

SnapLockタイプが親ボリュームと異なる場合は、FlexCloneボリュームに関する次の制限事項に注意する必要があります。

- RWタイプのクローンのみがサポートされます。SnapLockタイプが親ボリュームと異なるDPタイプのクローンはサポートされません。
- SnapLockではLUNがサポートされないため、SnapLockタイプオプションを「non-lun SnapLock」以外の値に設定してLUNを含むボリュームをクローニングすることはできません。
- MetroClusterのミラーされたアグリゲートではSnapLock Complianceボリュームがサポートされないため、MetroClusterのミラーされたアグリゲート上のボリュームをCompliance SnapLockタイプでクローニングすることはできません。
- リーガルホールドのSnapLock Complianceボリュームを別のSnapLockタイプでクローニングすることはできません。リーガルホールドはSnapLock Complianceボリュームでのみサポートされます。
- SVM DRはSnapLockボリュームをサポートしません。SVM DR関係の一部であるSVMのボリュームからSnapLockクローンを作成しようとすると失敗します。
- FabricPoolのベストプラクティスでは、クローンの階層化ポリシーは親と同じにすることを推奨しています。ただし、FabricPool対応ボリュームのSnapLock Complianceクローンに、親と同じ階層化ポリシーを使用することはできません。階層化ポリシーはに設定する必要があり `none`ます。階層化ポリシーが以外の親からSnapLock Complianceクローンを作成しようとする `none`と失敗します。

手順

1. SnapLockタイプのFlexCloneボリュームを作成します。 `volume clone create -vserver` *`svm_name`* `-flexclone` *`flexclone_name`* `-type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]`

   例：

   ```
   > volume clone create -vserver vs0 -flexclone vol1_clone -type RW
   -snaplock-type enterprise -parent-volume vol1
   ```

FlexCloneボリュームを親ボリュームからスプリットします。

FlexCloneボリュームを親からスプリットして、クローンを通常のFlexVol volumeにする

ことができます。

クローンスプリット処理はバックグラウンドで実行されます。スプリット中は、クローンおよび親のデータにアクセスできます。ONTAP 9.4以降では、スペース効率が維持されます。スプリットプロセスではメタデータのみが更新され、IOは最小限に抑えられます。データブロックはコピーされません。

タスクの内容

- スプリット処理中は、FlexCloneボリュームの新しいSnapshotを作成できません。
- データ保護関係に属しているか負荷共有ミラーに属しているFlexCloneボリュームは、親ボリュームからスプリットすることはできません。
- スプリットの実行中にFlexCloneボリュームをオフラインにすると、スプリット処理が中断されます。FlexCloneボリュームをオンラインに戻すと、スプリット処理が再開されます。
- スプリット後は、親FlexVol volumeとクローンの両方で、それぞれのボリュームギャランティに基づいたスペースの完全な割り当てが必要になります。
- FlexCloneを親ボリュームからスプリットしたあとは、この2つを再結合することはできません。
- ONTAP 9 .4以降では、AFFシステムのボリュームギャランティがnonである場合、FlexCloneのスプリット処理では物理ブロックが共有され、データはコピーされません。したがって、AFFシステムのFlexCloneボリュームのスプリットは、ONTAP 9 .4以降の他のFASシステムのFlexCloneスプリット処理よりも高速です。AFFシステムでのFlexCloneスプリット処理の改善には、次の利点があります。
  - 親からクローンをスプリットしたあともストレージ効率が維持されます。
  - 既存のSnapshotは削除されません。
  - 処理時間が短縮されます。
  - FlexCloneボリュームは、クローン階層の任意のポイントからスプリットできます。

開始する前に

- クラスタ管理者である必要があります。
- FlexCloneボリュームは、スプリット処理の開始時にオンラインになっている必要があります。
- スプリットが成功するには、親ボリュームがオンラインである必要があります。

手順

1. スプリット処理を完了するために必要な空きスペースの量を確認します。

   `volume clone show -estimate -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`* `-parent-volume` *`parent_vol_name`*

   次の例は、FlexCloneボリューム「clone1」を親ボリューム「vol1」からスプリットするために必要な空きスペースに関する情報を表示します。

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1
-parent-volume volume1
                              Split
Vserver   FlexClone       Estimate
--------- ------------- ----------
vs1       clone1           40.73MB
```

2. FlexCloneボリュームとその親を含むアグリゲートに十分なスペースがあることを確認します。
   a. FlexCloneボリュームとその親を含むアグリゲートの空きスペースの量を確認します。

      ```
      storage aggregate show
      ```

   b. 包含アグリゲートに十分な空きスペースがない場合は、アグリゲートにストレージを追加します。

      ```
      storage aggregate add-disks
      ```

3. スプリット処理を開始します。

   ```
   volume clone split start -vserver vserver_name -flexclone clone_volume_name
   ```

   次の例は、FlexCloneボリューム「Clone1」を親ボリューム「vol1」からスプリットするプロセスを開始する方法を示しています。

   ```
   cluster1::> volume clone split start -vserver vs1 -flexclone clone1

   Warning: Are you sure you want to split clone volume clone1 in Vserver
   vs1 ?
   {y|n}: y
   [Job 1617] Job is queued: Split clone1.
   ```

4. FlexCloneスプリット処理のステータスを監視します。

   ```
   volume clone split show -vserver vserver_name -flexclone clone_volume_name
   ```

   次の例は、AFFシステムでのFlexCloneスプリット処理のステータスを表示します。

   ```
   cluster1::> volume clone split show -vserver vs1 -flexclone clone1
                                                 Inodes
   Blocks
                                       ---------------------
   ---------------------
   Vserver   FlexClone    Processed Total    Scanned  Updated      % Inode
   % Block

   Complete  Complete
   vs1       clone1        0         0       411247   153600         0
   37
   ```

5. スプリットボリュームがFlexCloneボリュームでなくなったことを確認します。

   ```
   volume show -volume volume_name -fields clone-volume
   ```

   FlexClone以外のボリュームの場合、オプションの値 `clone-volume`は「false」です。

次の例は、親からスプリットしたボリューム「Clone1」がFlexCloneボリュームでないかどうかを確認する方法を示しています。

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
------- ------ **-------------**
vs1     clone1 **false**
```

関連情報

- "storage aggregate add-disks"

FlexCloneボリュームで使用されているスペースを確認する

FlexClone ボリュームの使用スペースを公称サイズおよび親 FlexVol と共有しているスペースに基づいて判断できます。作成された FlexClone ボリュームは、そのすべてのデータを親ボリュームと共有します。FlexVol volumeの公称サイズは親のサイズと同じですが、アグリゲートの空きスペースはほとんど使用されません。

タスクの内容

新たに作成された FlexClone ボリュームが使用する空きスペースは、その公称サイズの約 0.5% です。このスペースは FlexClone ボリュームのメタデータの保存に使用されます。

親または FlexClone ボリュームのいずれかに書き込まれた新しいデータは、ボリューム間で共有されません。FlexClone ボリュームに書き込まれる新しいデータが増えるにつれて、 FlexClone ボリュームがその包含アグリゲートから使用するスペースも増えます。

ステップ

1. コマンドを使用して、FlexCloneボリュームで実際に使用されている物理スペースを確認します `volume show`。

   次の例は、 FlexClone ボリュームの使用済みの物理スペースの合計を示しています。

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver    volume     size  available  used   percent-used   physical-
used     physical-used-percent
-------   ----------  ----  ---------  -----  ------------
-------------   ---------------------
vs01     clone_vol1   20MB   18.45MB   564KB       7%             196KB
1%
```

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

SnapMirrorのソースボリュームまたはデスティネーションボリュームから**FlexClone**ボリュームを作成する場合の考慮事項

既存の Volume SnapMirror 関係にあるソースボリュームまたはデスティネーションボリュームから FlexClone ボリュームを作成できます。ただし、これを行うと、以降に行う SnapMirror のレプリケーション処理が正常に完了しないことがあります。

FlexCloneボリュームの作成時にSnapMirrorで使用されるSnapshotがロックされる可能性があるため、レプリケーションが機能しないことがあります。この場合、FlexCloneが破棄されるか親からスプリットされるまで、SnapMirrorはデスティネーションボリュームへのレプリケーションを停止します。この問題に対処するには、次の2つの方法があります。

- FlexCloneボリュームが一時的に必要で、SnapMirrorレプリケーションが一時的に停止しても構わない場合は、FlexCloneボリュームを作成し、可能なかぎり削除するか親からスプリットします。

  FlexCloneボリュームが削除されるか親からスプリットされると、SnapMirrorレプリケーションは正常に続行されます。

- SnapMirrorレプリケーションの一時的な停止を許容できない場合は、SnapMirrorソースボリュームでSnapshotを作成し、そのSnapshotを使用してFlexCloneボリュームを作成できます。（デスティネーションボリュームからFlexCloneボリュームを作成する場合は、そのSnapshotがSnapMirrorデスティネーションボリュームにレプリケートされるまで待機する必要があります）。

  この方法でSnapMirrorソースボリュームにSnapshotを作成すると、SnapMirrorで使用されているSnapshotをロックせずにクローンを作成できます。

FlexCloneファイルと**FlexClone LUN**を使用して、ファイルと**LUN**の効率的なコピーを作成する

FlexCloneファイルおよび**FlexClone LUN**の使用の概要

FlexClone ファイルと FlexClone LUN は、親ファイルや親 LUN の書き込み可能でスペース効率の高いクローンです。これらは、物理的なアグリゲートスペースを効率的に利用するのに役立ちます。FlexCloneファイルとFlexClone LUNは、FlexVolボリュームでのみサポートされます。

FlexCloneファイルとFlexClone LUNは、サイズの0.4%をメタデータの格納に使用します。クローンは、親ファイルおよび親 LUN のデータブロックを共有し、クライアントが親ファイルまたは LUN に、またはクローンに新しいデータを書き込むまで、わずかなストレージスペースを占有します。

クライアントはファイルおよび LUN のすべての処理を、親エンティティとクローンエンティティの両方で実行できます。

FlexClone ファイルと FlexClone LUN は複数の方法で削除できます。

ONTAPで**FlexClone**ファイルまたは**FlexClone LUN**を作成する

コマンドを使用すると、FlexVolまたはFlexCloneボリュームに存在するファイルやLUNのクローンを、スペースを効率よく、時間をかけずに作成できます `volume file clone create`。

開始する前に

- クラスタにFlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。
- サブLUNのクローニングまたはサブファイルのクローニングに複数のブロック範囲を使用する場合は、ブロック番号が重複しないようにする必要があります。
- 適応圧縮が有効なボリュームでサブLUNまたはサブファイルを作成する場合は、ブロック範囲がミスアライメントされないようにする必要があります。

  つまり、ソースの開始ブロック番号とデスティネーションの開始ブロック番号が、偶数または奇数のいずれかでアライメントされている必要があります。

タスクの内容

SVM管理者は、クラスタ管理者によって割り当てられたPrivilegesに応じて、FlexCloneファイルおよびFlexClone LUNを作成できます。

クローンを作成および変更するときに、FlexCloneファイルおよびFlexClone LUNの自動削除設定を指定できます。デフォルトでは、自動削除設定は無効になっています。

既存のFlexCloneファイルまたはFlexClone LUNをクローンの作成時に上書きするには、 `volume file clone create`コマンドでパラメータを指定し `-overwrite-destination`ます。

スプリット負荷の最大値に達すると、FlexCloneファイルおよびFlexClone LUNの作成要求の受け入れが一時的に停止し、エラーメッセージが表示されます。 `EBUSY`ノードのスプリット負荷が最大値を下回ると、FlexCloneファイルおよびFlexClone LUNの作成要求の受け入れが再開されます。クローンの作成に必要な容量がノードに確保されてから、次の作成要求を行うようにしてください。

FlexClone LUNは親LUNのスペースリザベーション属性を継承します。スペースリザーブFlexClone LUNには、親のスペースリザーブLUNと同じ量のスペースが必要です。FlexClone LUNのスペースをリザーブしない場合は、クローンに対する変更を保存するための十分なスペースがボリュームに必要です。

手順

1. LUNをクローニングする場合は、LUNのマッピングまたは書き込みが行われていないことを確認します。
2. FlexCloneのLUNまたはファイルを作成します。

   ```
   volume file clone create -vserver vserver_name -volume volume_name -source
   -path source_path -destination-path destination_path
   ```

   次の例は、ボリュームvol1内の親ファイルfile1_sourceのFlexCloneファイルfile1_cloneを作成する方法を示しています。

   ```
   cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
   -path /file1_source -destination-path /file1_clone
   ```

   の詳細については `volume file clone create`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム内の**Snapshot**から**FlexClone LUN**を作成する

ボリューム内のSnapshotを使用して、LUNのFlexCloneコピーを作成できます。LUNのFlexCloneコピーは読み書き可能です。

開始する前に

FlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。

タスクの内容

FlexClone LUNは親LUNのスペースリザベーション属性を継承します。スペースリザーブFlexClone LUNには、親のスペースリザーブLUNと同じ量のスペースが必要です。FlexClone LUNのスペースをリザーブしない場合は、クローンに対する変更を保存するための十分なスペースがボリュームに必要です。

手順

1. LUNがマッピングされていないこと、または書き込まれていないことを確認します。
2. LUNを含むボリュームのSnapshotを作成します。

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

   クローニングするLUNのSnapshot（元のSnapshot）を作成する必要があります。

3. SnapshotからFlexClone LUNを作成します。

   ```
   volume file clone create -vserver vserver_name -volume volume_name -source
   -path source_path -snapshot-name snapshot_name -destination-path
   destination_path
   ```

   FlexClone LUNを自動削除できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してボリュームにこのFlexClone LUNを作成する場合は、すべてのFlexClone LUNに対して自動削除を有効にする必要があります。

4. FlexClone LUNが正しいことを確認します。

   ```
   lun show -vserver vserver_name
   ```

   ```
   Vserver Path                      State    Mapped    Type     Size
   ------- ----------------------    -------- --------- -------- -------
   vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
   vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
   ```

FlexCloneファイルおよび**FlexClone LUN**の作成および削除前のノード容量の表示

FlexCloneファイルおよびFlexClone LUNの作成要求や削除要求を受信する容量がノードにあるかどうかを確認する必要があります。そのためには、ノードのスプリット負荷を確認します。スプリット負荷の最大値に達すると、スプリット負荷が最大値を下回るまで新しい要求が受け付けられなくなります。

タスクの内容

スプリット負荷の最大値に達すると、`EBUSY`作成要求と削除要求に対する応答としてエラーメッセージが表示されます。ノードのスプリット負荷が最大値を下回ると、FlexCloneファイルおよびFlexClone LUNの作成要求や削除要求の受け入れが再開されます。

> `Allowable Split Load`フィールドに容量が表示され、作成要求が使用可能な容量に収まる場合、ノードは新しい要求を受け入れることができます。

手順

1. コマンドを使用して、FlexCloneファイルおよびFlexClone LUNの作成や削除にノードに必要な容量を表示します `volume file clone split load show`。

   次の例では、cluster1のすべてのノードのスプリット負荷を表示しています。Allowable Split Loadフィールドの値から、クラスタ内のすべてのノードに、FlexCloneファイルおよびFlexClone LUNの作成や削除に使用できる容量があることがわかります。

```
cluster1::> volume file clone split load show
Node        Max         Current    Token          Allowable
            Split Load  Split Load Reserved Load  Split Load
----------- ----------- ---------- -------------- ----------
node1          15.97TB          0B          100MB    15.97TB
node2          15.97TB          0B          100MB    15.97TB
2 entries were displayed.
```

関連情報

- "volume file clone split load showコマンドを使用します"

FlexCloneファイルおよび**FlexClone LUN**によるスペース削減量の表示

FlexCloneファイルおよびFlexClone LUNを含むボリュームでブロック共有によって削減されたディスクスペースの割合を表示できます。これは、キャパシティプランニングの一環として行うこともできます。

手順

1. FlexCloneファイルおよびFlexClone LUNによって達成されたスペース削減量を表示するには、次のコマンドを入力します。

   ```
   df -s volname
   ```

   `volname`は、FlexVol volumeの名前です。

   > 重複排除が有効なFlexVol volumeに対してコマンドを実行すると、`df -s`重複排除とFlexCloneファイルおよびLUNの両方で削減されたスペースを表示できます。

例

次の例は、FlexCloneボリュームtest1でのスペース削減量を示しています。

```
systemA> df -s test1

Filesystem          used   saved   %saved Vserver
/vol/test1/         4828    5744     54%  vs1
```

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

FlexCloneファイルおよび**FlexClone LUN**の削除方法

FlexClone ファイルと FlexClone LUN は複数の方法で削除できます。使用可能な方法を理解しておくと、クローンの管理方法を計画する際に役立ちます。

FlexCloneファイルおよびFlexClone LUNを削除するには、次の方法を使用します。

- FlexVol volumeの空きスペースが特定のしきい値を下回ったときに自動削除を有効にしたクローンを自動的に削除するようにFlexVol volumeを設定できます。
- NetApp Manageability SDKを使用して、クローンを削除するようにクライアントを設定できます。
- クライアントでは、NASプロトコルとSANプロトコルを使用してクローンを削除できます。

  この方法ではNetApp Manageability SDKが使用されないため、遅い削除方法はデフォルトで有効になっています。ただし、コマンドを使用して、FlexCloneファイルを削除するときに高速削除方式を使用するようにシステムを設定することができます `volume file clone deletion`。

自動削除設定で**FlexVol volume**が空きスペースを再生する仕組み

自動削除による**FlexVol**ボリュームと空きスペースの再生の概要

FlexVol の自動削除設定を有効にすると、 FlexClone ファイルおよび FlexClone LUN を自動的に削除できます。自動削除を有効にすると、ボリュームがフルに近くなったときに、指定した量の空きスペースをボリューム内に再生できます。

ボリュームの空きスペースが一定のしきい値を下回ったときに FlexClone ファイルおよび FlexClone LUN の削除を自動的に開始し、ボリュームの空きスペースを指定の量だけ再生したらクローンの削除を自動的に中止するように設定できます。クローンの自動削除を開始するしきい値を指定することはできませんが、それぞれのクローンを削除対象に含めるかどうかと、ボリュームの空きスペースの目標量を指定することができます。

ボリュームの空きスペースが一定のしきい値を下回ったとき、および次の要件の両方に達したときに、FlexClone ファイルおよび FlexClone LUN が自動的に削除されます。

- FlexClone ファイルおよび FlexClone LUN が格納されているボリュームに対して自動削除機能が有効になっている。

  FlexVol volumeに対して自動削除機能を有効にするには、コマンドを使用し `volume snapshot autodelete modify`ます。ボリュームで`FlexClone`ファイルおよび`FlexClone LUN`を自動的に削除

するには、パラメータをまたは `snap_reserve`に `volume`設定する必要があります `-trigger。の詳細については volume snapshot autodelete modify、を"ONTAPコマンド リファレンス"参照してください。

- FlexClone ファイルおよび FlexClone LUN に対して自動削除機能が有効になっている。

  FlexCloneファイルまたはFlexClone LUNに対して自動削除を有効にするには、 file clone create`コマンドでパラメータを指定し `-autodelete`ます。このクローン設定はボリュームの他の設定よりも優先されるため、この設定で個別に自動削除を無効にすることで、特定の FlexClone ファイルや FlexClone LUN を保持することができます。の詳細については `file clone create、を"ONTAPコマンド リファレンス"参照してください。

FlexCloneファイルおよびFlexClone LUNを自動的に削除するようにFlexVol volumeを設定する

ボリュームの空きスペースが一定のしきい値を下回ったときに FlexClone ファイルおよび FlexClone LUN の削除を自動的に開始し、ボリュームの空きスペースを指定の量だけ再生したらクローンの削除を自動的に中止するように設定できます。クローンの自動削除を開始するしきい値を指定することはできませんが、それぞれのクローンを削除対象に含めるかどうかと、ボリュームの空きスペースの目標量を指定することができます。

ボリュームの空きスペースが一定のしきい値を下回ったとき、および次の要件の両方に達したときに、FlexClone ファイルおよび FlexClone LUN が自動的に削除されます。

- FlexClone ファイルおよび FlexClone LUN が格納されているボリュームに対して自動削除機能が有効になっている。

  FlexVol volumeに対して自動削除機能を有効にするには、コマンドを使用し volume snapshot autodelete modify`ます。ボリュームでFlexCloneファイルおよびFlexClone LUNを自動的に削除するには、パラメータをまたは `snap_reserve`に `volume`設定する必要があります `-trigger。

- FlexClone ファイルおよび FlexClone LUN に対して自動削除機能が有効になっている。

  FlexCloneファイルまたはFlexClone LUNに対して自動削除を有効にするには、 `file clone create`コマンドでパラメータを指定し `-autodelete`ます。このクローン設定はボリュームの他の設定よりも優先されるため、この設定で個別に自動削除を無効にすることで、特定の FlexClone ファイルや FlexClone LUN を保持することができます。

開始する前に

- FlexVol volumeにFlexCloneファイルとFlexClone LUNが含まれていて、オンラインになっている必要があります。
- FlexVol volumeを読み取り専用ボリュームにすることはできません。

手順

1. コマンドを使用して、FlexVol volumeでFlexCloneファイルおよびFlexClone LUNの自動削除を有効にします volume snapshot autodelete modify。の詳細については volume snapshot autodelete modify、を"ONTAPコマンド リファレンス"参照してください。

   - パラメータには -trigger、またはを snap_reserve`指定できます `volume。

◦ パラメータには `-destroy-list`、1種類のクローンのみを削除するかどうかに関係なく、常に指定する必要があり `lun_clone,file_clone`ます。次の例は、ボリュームvol1でFlexCloneファイルとFlexClone LUNの自動削除を有効にし、ボリュームの25%が空きスペースになるまでスペースが再生されるようにする方法を示しています。

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

FlexVolボリュームで自動削除を有効にする際にパラメータの値をに `destroy`設定する `-commitment`と、ボリュームの空きスペースが指定したしきい値を下回った場合に、パラメータがに設定された `true`すべてのFlexCloneファイルおよびFlexClone LUNが `-autodelete`削除される可能性があります。ただし、パラメータがに設定されて `false`いるFlexCloneファイルとFlexClone LUN `-autodelete`は削除されません。

2. コマンドを使用して、FlexVol volumeでFlexCloneファイルおよびFlexClone LUNの自動削除が有効になっていることを確認します `volume snapshot autodelete show`。の詳細については `volume snapshot autodelete show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、ボリュームvol1でFlexCloneファイルとFlexClone LUNの自動削除が有効になっていることを示しています。

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
           Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)
    Target Free Space: 25%
              Trigger: volume
     *Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. 次の手順を実行して、削除するボリューム内のFlexCloneファイルおよびFlexClone LUNで自動削除が有効になっていることを確認します。

   a. コマンドを使用して、特定のFlexCloneファイルまたはFlexClone LUNの自動削除を有効にします `volume file clone autodelete`。の詳細については `volume file clone autodelete`、を"ONTAPコマンド リファレンス"参照してください。

      コマンドでパラメータを指定する `-force`と、特定の`FlexClone`ファイルまたは`FlexClone LUN`を強制的に自動削除できます `volume file clone autodelete`。

次の例は、ボリュームvol1に含まれるFlexClone LUN lun1_cloneの自動削除が有効になっていることを示しています。

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

自動削除は、FlexCloneファイルおよびFlexClone LUNの作成時に有効にすることができます。

b. コマンドを使用して、FlexCloneファイルまたはFlexClone LUNで自動削除が有効になっていることを確認します `volume file clone show-autodelete`。の詳細については `volume file clone show-autodelete`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、FlexClone LUN lun1_cloneで自動削除が有効になっていることを示しています。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
**Autodelete Enabled: true**
```

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

FlexCloneファイルまたはFlexClone LUNの自動削除を禁止する

FlexCloneファイルおよびFlexClone LUNを自動的に削除するようにFlexVol volumeを設定すると、指定した条件を満たすクローンがすべて削除される可能性があります。特定のFlexCloneファイルまたはFlexClone LUNを保持したい場合は、それらのファイルまたはLUNをFlexCloneの自動削除プロセスから除外できます。

開始する前に

FlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。

タスクの内容

FlexCloneファイルまたはFlexClone LUNを作成すると、クローンの自動削除設定はデフォルトで無効になります。自動削除が無効になっているFlexCloneファイルおよびFlexClone LUNは、ボリュームのスペースを再生するためにクローンを自動的に削除するようにFlexVol volumeを設定しても保持されます。

> ボリュームのレベルをまたは `disrupt`に `try`設定した場合は `commitment`、特定のFlexCloneファイルまたはFlexClone LUNの自動削除を無効にすることで、それらのクローンを個別に保持できます。ただし、ボリュームのレベルをに `destroy`設定し、削除リストに`include`を指定 `lun_clone,file_clone`した場合は `commitment`、ボリューム設定がクローン設定よりも優先され、クローンの自動削除設定に関係なく、すべてのFlexCloneファイルとFlexClone LUNが削除されます。

手順

1. コマンドを使用して、特定のFlexCloneファイルまたはFlexClone LUNが自動的に削除されないようにし `volume file clone autodelete`ます。

   次の例は、vol1に含まれるFlexClone LUN lun1_cloneの自動削除を無効にする方法を示しています。

   ```
   cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
   -clone-path lun1_clone -enable false
   ```

   自動削除を無効にしたFlexCloneファイルまたはFlexClone LUNは、ボリュームのスペース再生のために自動的に削除することはできません。

2. コマンドを使用して、FlexCloneファイルまたはFlexClone LUNで自動削除が無効になっていることを確認します `volume file clone show-autodelete`。

   次の例は、FlexClone LUN lun1_cloneの自動削除がfalseになっていることを示しています。

   ```
   cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
   vol/vol1/lun1_clone
                                                                  Vserver
   Name: vs1
                                                                  Clone Path:
   vol/vol1/lun1_clone
                                                                  Autodelete
   Enabled: false
   ```

FlexCloneファイルの削除の設定用コマンド

クライアントがNetAppマネージャビリティSDKを使用せずにFlexCloneファイルを削除する場合は、コマンドを使用して、FlexVol volumeからのFlexCloneファイルの高速削除を有効にできます `volume file clone deletion`。高速削除では、 FlexClone ファイルの拡張子と最小サイズが使用されます。

コマンドを使用して、ボリューム内のFlexCloneファイルでサポートされる拡張子のリストと最小サイズの要件を指定でき `volume file clone deletion`ます。高速削除方式は、要件を満たす FlexClone ファイルに対してのみ使用され、要件を満たさない FlexClone ファイルに対しては、より低速な削除方式が使用されます。

クライアントが NetApp Manageability SDK を使用してボリュームから FlexClone ファイルおよび FlexClone LUN を削除する場合は、常に高速削除方式が使用されるため、拡張子とサイズの要件は適用されません。

目的	使用するコマンド
ボリュームでサポートされる拡張子のリストに拡張子を追加します	`volume file clone deletion add-extension`

目的	使用するコマンド
高速削除方式でボリュームから削除する FlexClone ファイルの最小サイズを変更します	`volume file clone deletion modify`
ボリュームでサポートされる拡張子のリストから拡張子を削除します	`volume file clone deletion remove-extension`
クライアントが高速削除方式でボリュームから削除可能な、サポートされる拡張子のリストと FlexClone ファイルの最小サイズを表示します	`volume file clone deletion show`

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

関連情報

- "volume file clone deletion"

qtreeを使用してFlexVolをパーティショニングする

qtreeとONTAP FlexVol volumeパーティショニング

qtreeを使用すると、FlexVolボリュームを小さなセグメントにパーティショニングして、個別に管理できます。qtreeによって有効になるボリュームパーティショニングを使用すると、プロジェクト、ユーザ、またはグループごとにストレージをより細かく管理できます。qtreeを使用すると、クォータ、セキュリティ形式、およびCIFS oplockの管理を効率化できます。

ONTAPは、各ボリュームにデフォルトのqtreeを* qtree0 *という名前で作成します。特定のqtreeにデータを配置しない場合、データはqtree0に配置されます。

一般的な制限事項

本番環境でqtreeを使用する前に、qtreeの制限事項を理解しておく必要があります。qtreeの拡張パフォーマンス監視機能を使用する場合は、も確認してください[運用と制限事項]。

- qtree名の最大文字数は64文字です。
- qtree名で使用されている一部の特殊文字（カンマやスペースなど）は、他のONTAP機能で問題が発生する可能性があるため、使用しないでください。
- 異なるqtree間でディレクトリを移動することはできません。qtree 間で移動できるのはファイルだけです。
- qtree レベルの共有とボリュームレベルの共有を同じ FlexVol または SCVMM プールに作成すると、 qtree が FlexVol 共有上のディレクトリとして表示されます。誤って削除しないように注意する必要があります。

qtreeの管理および設定用コマンド

ONTAP CLIを使用してqtreeを管理および設定できます。目的に応じて、次のコマンドを使用してqtreeを管理する必要があります。

> コマンドを実行する `volume rehost`と、同じボリュームを対象とした他の同時管理処理が失敗することがあります。

状況	使用するコマンド
qtreeを作成する	`volume qtree create`
フィルタリングされたqtreeリストを表示します。	`volume qtree show`
qtreeを削除する	`volume qtree delete` > qtreeが空でない場合、またはフラグが使用されていない場合、このコマンドは失敗します `-force true`。
qtreeのUNIX権限を変更する	`volume qtree modify -unix-permissions`
qtreeのCIFS oplock設定を変更する	`volume qtree oplocks`
qtreeのセキュリティ設定を変更する	`volume qtree security`
qtreeの名前を変更する	`volume qtree rename`
qtreeの統計を表示する	`volume qtree statistics`
qtreeの統計をリセットする	`volume qtree statistics -reset`

qtreeのパフォーマンス監視機能の拡張

ONTAP 9 .16.1以降では、ONTAP REST APIを使用して、レイテンシ指標や履歴統計などの拡張されたqtree監視機能にアクセスできます。

ONTAP REST APIには、qtreeに関連するエンドポイントがいくつか含まれています。ONTAP 9 .16.1より前のバージョンでは、1秒あたりのIO処理数（IOPS）や、読み取り、書き込み、その他の処理のスループットなど、qtreeのリアルタイム統計にアクセスできました。

ONTAP 9 .16.1以降では、拡張されたqtreeパフォーマンス監視機能を使用して、NFSv3、NFSv4.0、NFSv4.1、NFSv4.2、pNFS（技術的にはNFSv4.1およびNFSv4.2の一部）、およびCIFSのリアルタイムのレイテンシ統計、IOPSおよびスループットを監視できます。また、統計情報を収集してアーカイブし、過去のパフォーマンスデータを表示できるようにします。

この拡張された監視機能により、ストレージ管理者はシステムパフォーマンスをより詳細に把握できます。こ

のデータを使用して、サービス品質の向上に取り組む際に、使用率の高いqtree、潜在的なボトルネック、その他の領域を特定できます。長期的な傾向など、これらの指標を分析できれば、より多くの情報に基づいてデータ主体の意思決定を下すことができます。

運用と制限事項

本番環境で拡張qtreeパフォーマンス監視機能を使用する前に、制限事項など、いくつかの動作特性を考慮する必要があります。

再マウントが必要

qtreeの拡張監視を有効にしたら、該当するボリュームを再マウントして機能をアクティブ化する必要があります。

トウケイノカヨウセイ

拡張パフォーマンス監視を有効にすると、統計データはすぐには使用できなくなります。これには、IOPS、スループット、レイテンシの統計が含まれます。qtreeのこのデータが表示されるまでに最大5分かかることがあります。

クラスタあたりの**qtree**数

ONTAPクラスタでは、最大50、000個のqtreeに対して拡張パフォーマンス監視を有効にできます。

ONTAP REST APIを使用した拡張指標へのアクセス

ONTAP 9 .16.1以降では、ONTAP REST APIを使用してqtreeの拡張パフォーマンス監視機能にアクセスできます。基本機能は、次のようにいくつかのカテゴリに分類されます。

拡張パフォーマンス監視の有効化と無効化

エンドポイントの `/api/storage/qtrees`プロパティにアクセスして、拡張監視機能を有効または無効にできます `ext_performance_monitoring.enabled`。POSTメソッドとPATCHメソッドは、新しいqtreeを作成するか既存のqtreeを設定するかに応じて使用できます。

グローバル監視の指標と設定を取得

いくつかの新しいグローバルプロパティがエンドポイントに追加され `/api/storage/qtrees`ました。これらのフィールドは、getメソッドを使用して取得できます。

特定の**qtree**の指標を取得する

エンドポイントでgetメソッドを使用すると、特定のボリュームで定義されている特定のqtreeの新しい統計情報と指標のプロパティを取得できます `/api/storage/qtrees/{volume.uuid}/{id}/metrics`。

アップグレードとリバート

ONTAP 9 .16.1でこの機能を有効にすると、制限なしで後続のONTAPリリースにアップグレードできます。ただし、2つのシナリオを考慮する必要があります。

9.16.1へのアップグレードとバージョンの混在クラスタの処理

クラスタの有効なクラスタバージョン（ECV）が9.16.1になるまで、拡張パフォーマンス監視機能は使用できません `ext_performance_monitoring.enabled`（に設定することはできません `true`）。

9.16.1からのリバート

プロパティがに設定されて `true`いる`qtree`がある場合 `ext_performance_monitoring.enabled`

、9.16.1から9.15.1にリバートすることはできません。リバート処理がブロックされます。ONTAPの以前のリリースにリバートする前に、すべてのqtreeのをに `false`設定することを推奨 `ext_performance_monitoring.enabled`します。

詳細

を含むONTAP REST APIの詳細については、ONTAP自動化に関するドキュメントを参照し "ONTAP REST APIの新機能"てください。また、ONTAP REST APIの詳細については、ONTAP自動化に関するドキュメントを参照して "qtreeエントホイント"ください。

qtreeのジャンクションパスを取得する

qtreeのジャンクションパスまたはネームスペースパスを取得することで、個 々 のqtreeをマウントできます。CLIコマンドでは、の形式のqtreeパスが表示され `qtree show -instance`ます `/vol/<volume_name>/<qtree_name>`。ただし、このパスはqtreeのジャンクションパスまたはネームスペースパスではありません。

の詳細については `qtree show`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

qtreeのジャンクションパスまたはネームスペースパスを取得するには、ボリュームのジャンクションパスを確認しておく必要があります。

手順

1. コマンドを使用し `vserver volume junction-path`て、ボリュームのジャンクションパスを取得します。

   次の例は、vs0という名前のStorage Virtual Machine（SVM）上にあるvol1という名前のボリュームのジャンクションパスを表示します。

   ```
   cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

   ------- ------ -------------

   vs0 vol1 /vol1
   ```

   上記の出力から、ボリュームのジャンクションパスはです `/vol1`。qtreeは常にボリュームにルートされるため、qtreeのジャンクションパスまたはネームスペースパスはになります `/vol1/qtree1`。

の詳細については `vserver volume junction-path`、を"ONTAPコマンド リファレンス"参照してください。

ディレクトリから**qtree**への変換

ディレクトリを**qtree**に変換する

FlexVol volumeのルートにあるディレクトリをqtreeに変換する場合は、クライアントアプリケーションを使用して、ディレクトリに格納されているデータを同じ名前の新しいqtreeに移行する必要があります。

タスクの内容

ディレクトリをqtreeに変換する手順は、使用するクライアントによって異なります。次のプロセスでは、完了する必要がある一般的なタスクの概要を説明します。

開始する前に

既存のCIFS共有に関連付けられているディレクトリは削除できません。

手順

1. qtreeにするディレクトリの名前を変更します。
2. 元のディレクトリ名を使用して新しいqtreeを作成します。
3. クライアントアプリケーションを使用して、ディレクトリの内容を新しいqtreeに移動します。
4. 空になったディレクトリを削除します。

Windowsクライアントを使用したディレクトリの**qtree**への変換

Windowsクライアントを使用してディレクトリをqtreeに変換するには、ディレクトリの名前を変更し、ストレージシステムにqtreeを作成して、ディレクトリの内容をqtreeに移動します。

タスクの内容

この手順を実行するには、エクスプローラを使用する必要があります。Windowsコマンドラインインターフェイスまたはdosプロンプト環境は使用できません。

手順

1. エクスプローラを開きます。
2. 変更するディレクトリのフォルダ表示をクリックします。

   ディレクトリは、そのディレクトリを含むボリュームのルートに配置する必要があります。

3. 「 * ファイル」メニューから「 * 名前の変更 * 」を選択して、このディレクトリに別の名前を付けます。
4. ストレージシステムで、コマンドを使用し `volume qtree create`て、ディレクトリの元の名前を指定した新しい`qtree`を作成します。の詳細については `volume qtree create`、を"ONTAPコマンド リファレンス"参照してください。
5. エクスプローラで、名前を変更したディレクトリフォルダを開き、フォルダ内のファイルを選択します。
6. 新しいqtreeのフォルダ表示に、これらのファイルをドラッグします。

   移動するフォルダ内のサブフォルダ数が多いほど、移動処理に時間がかかります。

7. 「 * ファイル」メニューから「 * 削除 * 」を選択して、名前が変更された空のディレクトリ・フォルダを削除します。

UNIXクライアントを使用したディレクトリの**qtree**への変換

UNIXでディレクトリをqtreeに変換するには、ディレクトリの名前を変更し、ストレー

ジシステムにqtreeを作成して、ディレクトリの内容をqtreeに移動します。

手順

1. UNIXクライアントのウィンドウを開きます。
2. コマンドを使用し `mv`て、ディレクトリの名前を変更します。

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. ストレージシステムから、コマンドを使用し `volume qtree create`て、元の名前のqtreeを作成します。

```
system1: volume qtree create /n/user1/vol1/dir1
```

の詳細については `volume qtree create`、を"ONTAPコマンド リファレンス"参照してください。

4. クライアントからコマンドを使用し `mv`て、古いディレクトリの内容をqtreeに移動します。

移動するディレクトリ内のサブディレクトリ数が多いほど、移動処理に時間がかかります。

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. コマンドを使用し `rmdir`て、空になった古いディレクトリを削除します。

```
client: rmdir /n/user1/vol1/olddir
```

終了後

UNIXクライアントでのコマンドの実装方法によっては `mv`、ファイルの所有権と権限が維持されない場合があります。この場合は、ファイルの所有者と権限を以前の値に更新します。

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

ボリュームの論理スペースのレポートと適用

ボリュームの論理スペースのレポートと適用の概要

ONTAP 9 .4以降では、ボリュームで使用されている論理スペースと残りのストレージスペースの量をユーザに表示できます。ONTAP 9 .5以降では、ユーザが消費する論理スペースの量を制限できます。

論理スペースのレポートと適用は、デフォルトでは無効になっています。

論理スペースのレポートと適用は、次のボリュームタイプでサポートされます。

ボリュームタイプ	スペースのレポートはサポートされますか。	スペースの適用はサポートされますか。
FlexVolホリユウム	はい（ONTAP 9 .4以降）	はい（ONTAP 9 .5以降）
SnapMirrorデスティネーションボリューム	はい。ONTAP 9 .8以降	はい。ONTAP 9 13.1以降
FlexGroupホリユウム	○（ONTAP 9 .9.1以降）	○（ONTAP 9 .9.1以降）
FlexCacheホリユウム	元の設定はキャッシュで使用されます。	該当なし

ロンリスヘエスノテキヨウ

論理スペースの適用では、ボリュームがフルになったときやフルに近づいたときにユーザに通知されます。ONTAP 9 .5以降で論理スペースの適用を有効にすると、ONTAPはボリューム内の使用済み論理ブロック数をカウントして、使用可能な残りのスペースを判断します。ボリュームに使用可能なスペースがない場合は、ENOSPC（スペース不足）エラーメッセージが返されます。

論理スペースの適用から、ボリューム内の使用可能スペースについて3種類のアラートが返されます。

- `Monitor.vol.full.inc.sav`：このアラートは、ボリュームの論理スペースの使用率が98%に達するとトリガーされます。
- `Monitor.vol.nearFull.inc.sav`：このアラートは、ボリュームの論理スペースの95%が使用されたときにトリガーされます。
- `Vol.log.overalloc.inc.sav`：このアラートは、ボリュームで使用されている論理スペースがボリュームの合計サイズよりも大きい場合にトリガーされます。

  このアラートがトリガーされた場合、ボリュームにスペースを追加しても超過した論理ブロックによって使用されてしまうため、使用可能なスペースにならない可能性があります。

論理スペースの適用を使用するボリュームの合計論理スペースは、プロビジョニングスペースからSnapshotリザーブを差し引いた容量と同じにする必要があります。

詳細については、を参照してください "ボリュームがフルになったときにスペースを自動的に確保するための設定"。

論理スペースのレポート

ボリュームで論理スペースのレポートを有効にすると、ボリュームの合計スペースに加えて、使用済みの論理スペースと使用可能な論理スペースの量が表示されます。また、LinuxおよびWindowsクライアントシステムのユーザは、使用済みの物理スペースと使用可能な物理スペースではなく、使用済み論理スペースと使用可能な論理スペースを確認できます。

定義：

- 物理スペースとは、ボリューム内で使用可能または使用済みのストレージの物理ブロックのことです。
- 論理スペースとは、ボリューム内で使用可能なスペースのことです。
- 使用済み論理スペースとは、使用済みの物理スペースに、設定済みのStorage Efficiency機能（重複排除や圧縮など）による削減効果を加えたものです。

ONTAP 9 5以降では、論理スペースの適用とスペースのレポートを有効にすることができます。

論理スペースのレポートを有効にすると、コマンドで次のパラメータが表示され `volume show`ます。

パラメータ	意味
`-logical-used`	使用済み論理サイズが指定した値に一致するボリュームに関する情報のみを表示します。この値には、Storage Efficiency機能で削減されたすべてのスペースと使用済みの物理スペースが含まれます。これにはSnapshotリザーブは含まれませんが、Snapshotオーバーフローは考慮されます。
`-logical-used-by-afs`	アクティブファイルシステムで使用されている論理サイズが指定した値に一致するボリュームに関する情報のみを表示します。この値は、スナップショット予約を超過したスナップショットオーバーフローの量によって値と異なり`-logical-used`ます。
`-logical-available`	論理スペースのレポートのみが有効になっている場合は、使用可能な物理スペースのみが表示されます。スペースのレポートと適用の両方が有効になっている場合は、使用中のStorage Efficiency機能によって削減されたスペースが反映された、現在使用可能な空きスペースの量が表示されます。Snapshotリザーブは含まれません。
`-logical-used-percent`	ボリュームのSnapshotリザーブを除くプロビジョニング済みサイズに対する現在の値の割合が表示されます `-logical-used`。 この値にはボリュームでの効率化による削減効果が含まれるため、この値は100%を超える場合があります `-logical-used-by-afs`。 `-logical-used-by-afs`ボリュームの値には、使用済みスペースとしてSnapshotオーバーフローは含まれません。 `-physical-used`ボリュームの値には、使用済みスペースとしてSnapshotオーバーフローが含まれます。
`-used`	ユーザデータおよびファイルシステムメタデータによって占有されているスペースの量が表示されます。スペースとは `physical-used`、以降の書き込み用にリザーブされているスペースとアグリゲートのストレージ効率化によって削減されたスペースの合計です。これには、スナップショットオーバーフロー（スナップショットリザーブを超過するスナップショットの容量）が含まれます。Snapshotリザーブは含まれません。

CLIで論理スペースのレポートを有効にすると、使用済み論理スペース（%）と論理スペースの値をSystem Managerでも表示することができます。

クライアント・システムでは ' 次のシステム・ディスプレイに論理スペースが使用済みスペースとして表示さ

れます

- * Linux システムでの df * 出力
- Windowsシステムのエクスプローラを使用した[プロパティ]の下のスペースの詳細。

> 論理スペースの適用を有効にせずに論理スペースのレポートを有効にすると、クライアントシステムに表示される合計容量がプロビジョニングスペースよりも大きくなることがあります。

論理スペースのレポートと適用を有効にする

ONTAP 9 .4以降では、論理スペースのレポートを有効にできます。9.5以降では、論理スペースの適用を有効にするか、レポートと適用の両方を同時に有効にすることができます。

タスクの内容

論理スペースのレポートと適用は、個 々 のボリュームレベルだけでなく、この機能をサポートするすべてのボリュームに対してSVMレベルでも有効にすることができます。SVM全体で論理スペース機能を有効にした場合は、個 々 のボリュームで無効にすることもできます。

ONTAP 9 8以降では、SnapMirrorソースボリュームで論理スペースのレポートを有効にすると、転送後にデスティネーションボリュームで自動的に有効になります。

ONTAP 9 .13.1以降では、SnapMirrorソースボリュームで適用オプションが有効になっていると、デスティネーションで論理スペースの消費が報告されて適用が適用されるため、より適切なキャパシティプランニングが可能になります。

> ONTAP 9 13.1より前のONTAPリリースを実行している場合、適用設定はSnapMirrorデスティネーションボリュームに転送されますが、デスティネーションボリュームでは適用がサポートされないことを理解しておく必要があります。そのため、デスティネーションでは論理スペースの使用量は報告されますが、適用は実行されません。

詳細については、をご覧ください "ONTAP リリースでの論理スペースのレポートのサポート"。

手順

次の1つまたは複数を有効にします。

- ボリュームに対して論理スペースのレポートを有効にします。

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true
```

- ボリュームに対して論理スペースの適用を有効にします。

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-enforcement-logical true
```

- ボリュームに対して論理スペースのレポートと適用を同時に有効にします。

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true -is-space-enforcement-logical true
```

- 新しいSVMに対して論理スペースのレポートまたは適用を有効にします。

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

- 既存のSVMに対して論理スペースのレポートまたは適用を有効にします。

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

SVMの容量制限を管理します。

ONTAP 9 .13.1以降では、Storage VM（SVM）に最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。

タスクの内容

SVM上の容量は、FlexVol、FlexGroup、FlexClone、FlexCacheの合計として計算されます。削除後にボリュームが制限状態、オフライン状態、またはリカバリキュー内にある場合でも、ボリュームは容量の計算に影響します。ボリュームで自動拡張が設定されている場合は、ボリュームの最大オートサイズの値がSVMのサイズに合わせて計算されます。自動拡張を設定しない場合は、ボリュームの実際のサイズが計算されます。

次の表に、パラメータが容量の計算に与える影響を示し `autosize-mode`ます。

`autosize-mode off`	サイズパラメーターは計算に使用されます
`autosize-mode grow`	`max-autosize`パラメーターは計算に使用されます
`autosize-mode grow-shrink`	`max-autosize`パラメーターは計算に使用されます

開始する前に

- SVM数の上限を設定するには、クラスタ管理者である必要があります。
- ONTAP 9.16.1以降では、データ保護ボリュームを含むSVMに対してストレージの制限を設定できます。これには、次のデータ保護タイプが含まれます。
  - カスケードを使用しない非同期DRのFlexVolボリューム
  - 同期DRのFlexVolボリューム（syncポリシーとstrict-syncポリシーの両方）
  - "リストア"
- SVMのストレージ制限は、次の構成で_not_supportedになります。
  - SnapMirrorハツクアツフカンケイ
  - SnapMirrorアクティブ同期
  - FlexGroupホリユウム
  - 整合グループ
  - SVM DR
  - カスケード
  - MetroCluster

- ONTAP 9.16.1 以降では、負荷共有ミラー関係を作成するときに、デスティネーション SVM でストレージ制限を有効にすることはできません。
- SVMを移行する際、ソースSVMでストレージの制限を有効にすることはできません。移行処理を完了するには、ソースのストレージ制限を無効にしてから移行を完了してください。
- SVMの容量はとはクォータ異なります。クォータは最大サイズを超えることはできません。
- SVMで他の処理を実行中のときは、ストレージ制限を設定することはできません。既存のジョブを表示するには、コマンドを使用し `job show vserver <svm_name>` ます。ジョブが完了したら、もう一度コマンドを実行してください。の詳細については `job show`、を"ONTAPコマンド リファレンス"参照してください。

容量への影響

容量制限に達すると、次の処理が失敗します。

- LUN、ネームスペース、またはボリュームの作成
- LUN、ネームスペース、またはボリュームのクローニング
- LUN、ネームスペース、またはボリュームの変更
- LUN、ネームスペース、またはボリュームのサイズの拡張
- LUN、ネームスペース、またはボリュームの拡張
- LUN、ネームスペース、またはボリュームのリホスト

新しい**SVM**に容量制限を設定する

System Manager

手順

1. **>**[Storage VMs]*を選択します。
2. を選択 してSVMを作成します。
3. SVMに名前を付け、*アクセスプロトコル*を選択します。
4. で、[最大容量制限を有効にする]*を選択します。

   SVMの最大容量サイズを指定します。

5. [保存（ Save ）] を選択します。

CLI

手順

1. SVMを作成ストレージの制限を設定するには、値を指定し `storage-limit`ます。ストレージ制限のしきい値アラートを設定するには、の割合を指定します `-storage-limit-threshold-alert`。

   ```
   vserver create -vserver <vserver_name> -aggregate <aggregate_name>
   -rootvolume <root_volume_name> -rootvolume-security-style
   {unix|ntfs|mixed} -storage-limit <value> [GiB|TIB] -storage-limit
   -threshold-alert <percentage> [-ipspace <IPspace_name>] [-language
   <language>] [-snapshot-policy <snapshot_policy_name>] [-quota-policy
   <quota_policy_name>] [-comment <comment>]
   ```

   しきい値を指定しない場合、デフォルトでは、SVMの容量が90%に達したときにアラートがトリガーされます。しきい値アラートを無効にするには、値を0にします。

2. SVMが作成されたことを確認します。

   ```
   vserver show -vserver <vserver_name>
   ```

3. ストレージの制限を無効にする場合は、SVMのパラメータを0に設定し `-storage-limit`ます。

   ```
   vserver modify -vserver <vserver_name> -storage-limit 0
   ```

既存の**SVM**の容量制限を設定または変更する

既存のSVMに対して容量制限としきい値アラートを設定したり、容量制限を無効にしたりできます。

容量制限を設定したあとに、現在割り当てられている容量よりも小さい値に変更することはできません。

System Manager

手順

1. >[Storage VMs]*を選択します。
2. 変更するSVMを選択します。SVM名の横にある*[編集]*を選択します ⋮ 。
3. 容量制限を有効にするには、*容量制限を有効にする*の横にあるボックスを選択します。[Maximum capacity]に値を入力し、[Alert threshold]にパーセント値を入力します。

   容量制限を無効にする場合は、[容量制限を有効にする]*の横にあるチェックボックスをオフにします。

4. [保存（ Save ）] を選択します。

CLI

手順

1. SVMをホストしているクラスタで、コマンドを実行し `vserver modify`ます。には数値、にはパーセント値を `-storage-limit-threshold-alert`指定します `-storage-limit`。

   ```
   vserver modify -vserver <vserver_name> -storage-limit <value>
   [GiB|TIB] -storage-limit-threshold-alert <percentage>
   ```

   しきい値を指定しない場合は、容量の90%を超えるデフォルトのアラートが生成されます。しきい値アラートを無効にするには、値を0にします。

2. ストレージの上限を無効にする場合は、SVMのを0に設定し `-storage-limit`ます。

   ```
   vserver modify -vserver <vserver_name> -storage-limit 0
   ```

容量の上限に達している

最大容量やアラートしきい値に達したときは、EMSメッセージを確認するか、System Managerの* Insights *ページで、考えられる対処方法を確認できます `vserver.storage.threshold`。考えられる解決策は次のとおりです。

- SVMの最大容量制限の編集
- スペースを解放するためのボリュームリカバリキューのパージ
- ボリュームにスペースを確保するためのSnapshotの削除

関連情報

- System Managerでの容量測定
- System Managerでクラスタ、階層、SVMの容量を監視する
- "SVMの作成"
- "vserver show"

- "vserver modify"

クォータを使用してリソース使用量を制限または追跡する

クォータプロセスの概要

クォータ、クォータルール、クォータポリシーについて理解する

クォータは、 FlexVol ボリュームに固有のクォータルールで定義されます。これらのクォータルールはStorage Virtual Machine（SVM）のクォータポリシーにまとめられ、SVM上の各ボリュームでアクティブ化されます。

クォータルールは常にボリュームに固有です。クォータルールは、クォータルールに定義されているボリュームでクォータがアクティブ化されるまでは効果がありません。

クォータポリシーは、SVMのすべてのボリュームに対するクォータルールの集まりです。クォータポリシーは SVM 間で共有されません。SVMには最大5つのクォータポリシーを設定できるため、クォータポリシーのバックアップコピーを保持できます。1つのSVMに割り当てられるクォータポリシーは常に1つです。ボリューム上のクォータを初期化またはサイズ変更すると、その SVM に現在割り当てられているクォータポリシー内のクォータルールがアクティブ化されます。

クォータは、 ONTAP で適用される実際の制限、または ONTAP で実行される実際の追跡処理です。クォータルールからは常に少なくとも 1 つのクォータが作成され、そのほかに多数の派生クォータが作成されることもあります。適用クォータの一覧は、クォータレポートでのみ表示できます。

アクティブ化とは、割り当てられたクォータポリシーの現在のクォータルールセットから適用クォータを作成するように ONTAP をトリガーするプロセスです。アクティブ化はボリューム単位で実行されます。ボリュームでのクォータの最初のアクティブ化を初期化と呼びます。以降のアクティブ化は、変更の範囲に応じて再初期化またはサイズ変更と呼びます。

クォータを使用するメリット

クォータを使用して、FlexVolボリュームのリソース使用量を管理および監視できます。

クォータを定義すると、いくつかのメリットがあります。デフォルトクォータ、明示クォータ、派生クォータ、および追跡クォータを使用すると、最も効率的な方法でディスク使用量を管理できます。

リソース消費の制限

ユーザやグループが使用する、またはqtreeに格納されるディスクスペースの量やファイル数を制限できます。

リソース使用量の追跡

ユーザ、グループ、またはqtreeによって使用されているディスクスペースの量またはファイル数は、制限を課すことなく追跡できます。

ユーザーに通知

リソースの使用量が特定のレベルに達したときに通知を生成できます。これは、ディスクまたはファイルの使用率が高すぎるとユーザーに警告します。

クォータを使用すると、ユーザ、グループ、またはqtreeによって使用されるディスクスペースやファイル数を制限したり、追跡したりできます。クォータは、特定のFlexVol volumeまたはqtreeに適用されます。

クォータには、ソフトクォータとハードクォータがあります。ソフトクォータでは、指定された制限を超えるとONTAPによって通知が送信されますが、ハードクォータでは、指定された制限を超えると書き込み処理が失敗します。

ONTAPは、ユーザまたはユーザグループからFlexVol volumeへの書き込み要求を受信すると、そのボリュームでそのユーザまたはユーザグループに対してクォータがアクティブ化されているかどうかを確認し、次の点を判断します。

- ハードリミットに達するかどうか

  「はい」の場合、ハードリミットに達したときに書き込み処理が失敗し、ハードクォータ通知が送信されます。

- ソフトリミットを超えるかどうか

  「yes」の場合は、ソフトリミットを超えたときに書き込み処理が成功し、ソフトクォータ通知が送信されます。

- 書き込み処理がソフトリミットを超えないかどうか

  yesの場合、書き込み処理は成功し、通知は送信されません。

ハードクォータは処理を禁止し、ソフトクォータは通知をトリガーします。

ハードクォータはシステムリソースにハードリミットを適用します。この制限を超えることになる処理はすべて失敗します。以下の設定でハードクォータを作成します。

- ディスク制限パラメータ
- ファイル制限パラメータ

ソフトクォータでは、リソース使用量が一定のレベルに達すると警告メッセージが送信されますが、データアクセス処理には影響しません。そのため、クォータを超過する前に適切な措置を講じることができます。ソフトクォータは以下の設定で構成されます。

- ディスク制限しきい値パラメータ
- ディスクのソフトリミットパラメータ
- ファイルのソフトリミットパラメータ

しきい値クォータとソフトディスククォータを使用すると、管理者はクォータについての通知を複数受け取ることができます。通常、書き込みが失敗し始める前にしきい値によって「最終警告」が通知されるようにするため、管理者はディスク制限のしきい値をディスク制限よりもわずかに小さい値に設定します。

クォータ通知は Event Management System （ EMS ；イベント管理システム）に送信されるメッセージであり、 SNMP トラップとしても設定されます。

通知は次のイベントに対応して送信されます。

- つまり、ハードクォータに達したときに、クォータを超えようとしたときです
- ソフトクォータを超えています
- ソフトクォータを超過しなくなりました

しきい値は他のソフトクォータとは若干異なります。しきい値を指定した場合に通知がトリガーされるのは、しきい値を超えた場合だけです。しきい値を超えた場合は

ハードクォータ通知は、volume quota modifyコマンドを使用して設定できます。不必要なメッセージが送信されないように、通知を完全にオフにしたり、頻度を変更したりすることができます。

ソフトクォータ通知は、冗長なメッセージが生成される可能性は低く、通知が唯一の目的であるため、設定できません。

次の表に、クォータが EMS システムに送信するイベントを示します。

発生する状況	**EMS** に送信されるイベント
ツリークォータのハードリミットに達した	`wafl.quota.qtree.exceeded`
ボリューム上のユーザクォータのハードリミットに達した	`wafl.quota.user.exceeded`（UNIXユーザの場合）（Windowsユーザの場合 `wafl.quota.user.exceeded.win`）
qtree 上のユーザクォータのハードリミットに達した	`wafl.quota.userQtree.exceeded`（UNIXユーザの場合）（Windowsユーザの場合 `wafl.quota.userQtree.exceeded.win`）
ボリューム上のグループクォータのハードリミットに達した	`wafl.quota.group.exceeded`
qtree 上のグループクォータのハードリミットに達した	`wafl.quota.groupQtree.exceeded`
しきい値を含むソフトリミットを超えている	`quota.softlimit.exceeded`
ソフトリミットを超過しなくなりました	`quota.softlimit.normal`

次の表に、クォータで生成される SNMP トラップを示します。

発生する状況	送信される **SNMP** トラップ
ハードリミットに達しました	quotaExceeded
しきい値を含むソフトリミットを超えている	quotaExceeded および softQuotaExceeded です
ソフトリミットを超過しなくなりました	quotaNormal および softQuotaNormal です

通知には、 qtree 名ではなく qtree の ID 番号が含まれます。コマンドを使用すると、qtree名をID番号に関連付けることができます `volume qtree show -id`。

クォータのターゲットとタイプ

すべてのクォータには特定のタイプがあります。クォータターゲットはタイプから派生し、クォータ制限を適用するユーザ、グループ、またはqtreeを指定します。

次の表に、クォータターゲット、各クォータターゲットが関連付けられているクォータのタイプ、および各クォータターゲットの指定方法を示します。

クォータターゲット	クォータタイプ	ターゲットの指定方法	脚注
ユーザ	ユーザ クォータ	UNIXユーザ名 UNIX UID UIDがユーザと一致するファイルまたはディレクトリ Windows 2000より前の形式のWindowsユーザ名 Windows SID ユーザのSIDが所有するACLが設定されたファイルまたはディレクトリ	ユーザ クォータは、特定のボリュームまたはqtreeに適用できます
グループ	グループ クォータ	UNIXグループ名 UNIX GID GIDがグループと一致するファイルまたはディレクトリ	グループ クォータは、特定のボリュームまたはqtreeに適用できます グループ クォータの適用にWindows IDは使用されません。
qtree	ツリー クォータ	qtree名	ツリー クォータは特定のボリュームに適用され、他のボリューム内のqtreeには影響しません

""	ユーザ クォータ□□グループ クォータ ツリー クォータ	二重引用符（""）	と表示されたクォータターゲットは、 a_default QUOTA_示さ れています。デフォルトクォータの場合、クォータタイプはtypeフィールドの値によって決まります。

特殊なクォータ

デフォルトクォータの機能

デフォルトクォータを使用すると、特定のクォータタイプのすべてのインスタンスにクォータを適用できます。たとえば、デフォルトユーザクォータは、指定したFlexVol volumeまたはqtreeについて、システム上のすべてのユーザに適用されます。また、デフォルトクォータを使用すると、クォータを簡単に変更できます。

デフォルトクォータを使用すると、大量のクォータターゲットに自動的に制限を適用できます。ターゲットごとに別 々 のクォータを作成する必要はありません。たとえば、ほとんどのユーザのディスクスペースを10GBに制限する場合は、ユーザごとにクォータを作成する代わりに、10GBのディスクスペースのデフォルトユーザクォータを指定できます。特定のユーザに別の制限を適用する場合は、それらのユーザに明示的クォータを作成できます。（明示的クォータ：特定のターゲットまたはターゲットのリストを指定したクォータは、デフォルトクォータを上書きします）。

また、デフォルトクォータでは、クォータの変更を有効にする場合に、再初期化ではなくサイズ変更を使用できます。たとえば、すでにデフォルトユーザクォータが設定されているボリュームに明示的ユーザクォータを追加した場合、サイズ変更によって新しいクォータをアクティブ化できます。

デフォルトクォータは、3種類のクォータターゲット（ユーザ、グループ、およびqtree）のすべてに適用できます。

デフォルトクォータには、必ずしも制限が指定されているとは限りません。デフォルトクォータを追跡クォータにすることができます。

クォータは、コンテキストに応じて、空の文字列（ "" ）またはアスタリスク（ * ）であるターゲットによって示されます。

- コマンドを使用してクォータを作成する場合、 `volume quota policy rule create`パラメータを空の文字列（""）に設定する `-target`と、デフォルトクォータが作成されます。

  の詳細については `volume quota policy rule create`、を"ONTAPコマンド リファレンス"参照してください。

- `volume quota policy rule create`コマンドでは `-qtree`、パラメータは、クォータルールを適用するqtreeの名前を指定します。このパラメータは、ツリータイプのルールには適用されません。ボリュームレベルのユーザまたはグループタイプのルールの場合、このパラメータには""を指定する必要があります。
- コマンドの出力で `volume quota policy rule show`は、デフォルトクォータのターゲットとして空の文字列（""）が表示されます。

  の詳細については `volume quota policy rule show`、を"ONTAPコマンド リファレンス"参照してください。

- コマンドの出力で `volume quota report`は、デフォルトクォータのIDとクォータ指定子にアスタリスク（*）が表示されます。

  の詳細については `volume quota report`、を"ONTAPコマンド リファレンス"参照してください。

デフォルトユーザクォータの例

次のクォータルールでは、デフォルトユーザクォータを使用して、vol1の各ユーザに50MBの制限を適用しています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0                Policy: default           Volume: vol1
                                                 Soft              Soft
                          User          Disk     Disk    Files     Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit     Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""      off           50MB        -       -         -
-
```

システム上のいずれかのユーザが、そのユーザのデータがvol1で50MBを超えるようなコマンドを入力した場合（エディタからのファイルへの書き込みなど）、そのコマンドは失敗します。

明示的クォータの使用方法

明示的クォータを使用すると、特定のクォータターゲットのクォータを指定したり、特定のターゲットのデフォルトクォータを上書きしたりできます。

明示的クォータは、特定のユーザ、グループ、またはqtreeの制限を指定します。同じターゲットに設定されているデフォルトクォータは、明示的クォータによって置き換えられます。

派生ユーザクォータがあるユーザに明示的ユーザクォータを追加する場合は、デフォルトユーザクォータと同じユーザマッピング設定を使用する必要があります。そうしないと、クォータのサイズを変更するときに、明示的ユーザクォータは新しいクォータとみなされるため拒否されます。

明示的クォータは、同じレベル（ボリュームまたはqtree）のデフォルトクォータにのみ影響します。たとえば、qtreeの明示的ユーザクォータは、そのqtreeを含むボリュームのデフォルトユーザクォータには影響しません。ただし、qtreeの明示的ユーザクォータは、そのqtreeのデフォルトユーザクォータを上書きします（制限を置き換えます）。

明示的クォータの例

次のクォータ ルールでは、vol1の全ユーザのスペースを50MBに制限するというデフォルト ユーザ クォータが定義されています。ただし、jsmithというユーザだけは、明示的クォータ（太字）によりスペース制限

が80MBに設定されています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -        -
-
user   jsmith    ""      off          80MB        -       -        -
-
```

次のクォータルールでは、4つのIDで表されるユーザを、vol1ボリューム内の550MBのディスクスペースと10、000ファイルに制限しています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"
                 ""      off         550MB        -   10000        -
-
```

次のクォータルールは、eng1グループのディスクスペースを150MBに制限し、proj1 qtree内のファイル数を無制限に制限します。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                  Soft             Soft
                         User         Disk       Disk    Files    Files
Type    Target    Qtree  Mapping      Limit      Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
group  eng1      proj1   off          150MB         -       -        -
-
```

次のクォータルールでは、vol2ボリューム内のproj1 qtreeのディスクスペースが750MB、ファイル数が75、000に制限されています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                  Soft             Soft
                         User         Disk       Disk    Files    Files
Type    Target    Qtree  Mapping      Limit      Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   proj1     ""      -            750MB         -   75000        -
-
```

派生クォータの機能

明示的クォータ（特定のターゲットを指定したクォータ）によってではなく、デフォルトクォータによって適用されるクォータを、 _derived quota _ と呼びます。

派生クォータの数と場所は、クォータタイプによって異なります。

- ボリューム上のデフォルトツリークォータによって、そのボリューム上のすべてのqtreeに派生デフォルトツリークォータが作成されます。

- デフォルトユーザクォータまたはデフォルトグループクォータは、同じレベル（ボリュームまたはqtree）でファイルを所有するすべてのユーザまたはグループに、派生ユーザクォータまたは派生グループクォータを作成します。
- ボリューム上のデフォルトユーザクォータまたはデフォルトグループクォータによって、ツリークォータもあるすべてのqtreeに、派生デフォルトユーザクォータまたは派生グループクォータが作成されます。

派生クォータの設定（制限やユーザマッピングを含む）は、対応するデフォルトクォータの設定と同じです。たとえば、ボリュームに20GBのディスク制限があるデフォルトツリークォータを作成すると、ボリューム内のqtreeに20GBのディスク制限が設定された派生ツリークォータが作成されます。デフォルトクォータが追跡クォータ（制限なし）の場合、派生クォータも追跡クォータになります。

派生クォータを確認するには、クォータレポートを生成します。レポートでは、派生ユーザクォータまたは派生グループクォータは、ブランクまたはアスタリスク（ * ）のクォータ指定子で示されます。ただし、派生ツリークォータにはクォータ指定子があります。派生ツリークォータを特定するには、ボリューム上で同じ制限が適用されているデフォルトツリークォータを探す必要があります。

明示的クォータは、派生クォータと次のように連動します。

- 同じターゲットにすでに明示的クォータが存在する場合は、派生クォータは作成されません。
- 派生クォータが存在するターゲットに明示的クォータを作成するときに、サイズ変更によって明示的クォータをアクティブ化できます。クォータを完全に初期化する必要はありません。

追跡クォータの使用

追跡クォータでは、ディスクとファイルの使用量のレポートが生成され、リソースの使用量は制限されません。追跡クォータを使用している場合、クォータのサイズを変更すると、クォータをいったんオフにしてから再度オンにするのではなく、サイズを変更できるため、クォータ値の変更によるシステム停止が少なくなります。

追跡クォータを作成するには、ディスク制限パラメータとファイル制限パラメータを省略します。これにより、ONTAPは、制限を課すことなく、ターゲットのレベル（ボリュームまたはqtree）でそのターゲットのディスクとファイルの使用状況を監視するようになります。追跡クォータは、コマンドの出力 `show`およびクォータレポートで、すべての制限にダッシュが表示されます。ONTAPでは、System Manager UIを使用して明示的クォータ（特定のターゲットを持つクォータ）を作成すると、追跡クォータが自動的に作成されます。CLIを使用する場合、ストレージ管理者は明示的クォータの上に追跡クォータを作成します。

また、ターゲットのすべてのインスタンスを環境で管理する _default 追跡 quota_policy_を 指定することもできます。デフォルト追跡クォータを使用すると、あるクォータタイプのすべてのインスタンス（すべてのqtreeまたはすべてのユーザなど）の使用量を追跡できます。また、クォータの変更を有効にする必要がある場合に、クォータの再初期化ではなくサイズ変更を使用できます。

例

ボリュームレベルの追跡ルールの次の例に示すように、追跡ルールの出力には、qtree、ユーザ、およびグループの追跡クォータが表示されます。

```
Vserver: vs0              Policy: default              Volume: fv1

                                        Soft           Soft
                        User    Disk    Disk   Files   Files
Type  Target   Qtree    Mapping Limit   Limit  Limit   Limit  Threshold
----- -------- -------  ------- ------  ------ ------  ------ ---------
tree  ""       ""       -       -       -      -       -      -
user  ""       ""       off     -       -      -       -      -
group ""       ""       -       -       -      -       -      -
```

クォータの適用方法

クォータの適用方法を理解しておくと、クォータを適切に設定し、想定される制限を設定できます。

クォータが有効な FlexVol ボリュームでファイルの作成またはファイルへのデータの書き込みを試行されると、処理が続行される前にクォータ制限がチェックされます。その処理がディスク制限またはファイル制限を超える場合、その処理は実行されません。

クォータ制限は次の順序でチェックされます。

1. その qtree のツリークォータ（ファイルの作成または書き込みが qtree0 に対して行われる場合、このチェックは行われません）
2. ボリューム上のファイルを所有しているユーザのユーザクォータ
3. ボリューム上のファイルを所有しているグループのグループクォータ
4. その qtree のファイルを所有しているユーザのユーザクォータ（ファイルの作成または書き込みが qtree0 に対して行われる場合、このチェックは行われません）
5. その qtree のファイルを所有しているグループのグループクォータ（ファイルの作成または書き込みが qtree0 に対して行われる場合、このチェックは行われません）

最も上限の低いクォータが、最初に超過するクォータとはかぎりません。たとえば、ボリューム vol1 のユーザクォータが 100GB の場合、 また、ボリューム vol1 に含まれる qtree q2 のユーザクォータは 20GB 、そのユーザがすでに 80GB を超えるデータをボリューム vol1 に（ただし qtree q2 以外）書き込んでいる場合、ボリュームの制限を最初に超過する可能性があります。

関連情報

- "rootユーザへのクォータの適用方法"
- "複数のIDを持つユーザにクォータを適用する方法"

クォータポリシーの割り当てに関する考慮事項

クォータポリシーは、 SVM のすべての FlexVol に対するクォータルールをグループ化したものです。クォータポリシーを割り当てる際には、一定の考慮事項に注意する必要があります。

- SVM には、常に 1 つのクォータポリシーが割り当てられています。SVM が作成されると、空のクォータ

ポリシーが作成され、 SVM に割り当てられます。このデフォルトのクォータポリシーには、 SVM の作成時に別の名前を指定しないかぎり、「 default 」という名前が付けられます。

- SVM には、最大 5 つのクォータポリシーを設定できます。1 つの SVM に 5 つのクォータポリシーが存在する場合、既存のクォータポリシーを削除しないかぎり、その SVM に新しいクォータポリシーを作成できません。
- クォータポリシーのクォータルールを作成または変更する必要がある場合は、次のいずれかの方法を選択できます。
  - SVM に割り当てられているクォータポリシーを直接編集します。その場合、そのクォータポリシーを SVM に割り当てる必要はありません。
  - 割り当てられていないクォータポリシーを編集し、そのポリシーを SVM に割り当てます。その場合、必要に応じて元に戻せるように、クォータポリシーのバックアップを作成しておく必要があります。

    たとえば、割り当てられているクォータポリシーのコピーを作成して、そのコピーを変更して変更したコピーを SVM に割り当て、元のクォータポリシーの名前を変更します。
- クォータポリシーの名前変更は、そのクォータポリシーが SVM に割り当てられている場合でも可能です。

ユーザおよびグループとクォータ

ユーザおよびグループに対するクォータの処理の概要

クォータのターゲットとしてユーザまたはグループを指定できます。クォータを定義するときは、実装上のいくつかの違いを考慮する必要があります。

次のような相違点に注意する必要があります。

- ユーザまたはグループ
- UNIXまたはWindows
- 特殊なユーザとグループ
- 複数のIDを含む

また、環境に応じてユーザのIDを指定する方法もいくつかあります。

クォータの**UNIX**ユーザを指定する

クォータにUNIXユーザを指定するには、いくつかの形式を使用できます。

クォータにUNIXユーザを指定する場合は、次の3つの形式を使用できます。

- ユーザ名（jsmithなど）。

  UNIX ユーザ名にバックスラッシュ（ \ ）または @ 記号が含まれている場合、その名前を使用してクォータを指定することはできません。ONTAP では、これらの文字を含む名前は Windows 名として処理されます。

- ユーザIDまたはUID（20など）。

- ユーザが所有するファイルまたはディレクトリのパス。ファイルの UID がユーザと一致するように設定されます。

> ファイル名またはディレクトリ名を指定する場合は、システム上で対象のユーザアカウントを使用するかぎり削除されることのないファイルまたはディレクトリを選択する必要があります。
>
> UID のファイルまたはディレクトリ名原因 ONTAP を指定しても、そのファイルまたはディレクトリにクォータを適用されるわけではありません。

クォータに**Windows**ユーザを指定する

クォータにWindowsユーザを指定するには、いくつかの形式を使用できます。

クォータのWindowsユーザを指定するときに使用できる3つの形式は次のとおりです。

- Windows 2000 より前の形式の Windows 名。
- Windowsによってテキスト形式（など）で表示されるセキュリティID（SID） `S-1-5-32-544`。
- ユーザの SID によって所有されている ACL を持つファイルまたはディレクトリの名前。

> ファイル名またはディレクトリ名を指定する場合は、システム上で対象のユーザアカウントを使用するかぎり削除されることのないファイルまたはディレクトリを選択する必要があります。
>
> ONTAP が ACL から SID を取得するには、その ACL が有効である必要があります。
>
> ファイルまたはディレクトリが UNIX 形式の qtree に存在する場合、またはストレージシステムでユーザ認証に UNIX モードが使用されている場合、 ONTAP は、 SID ではなく UID * がファイルまたはディレクトリの UID に一致するユーザにユーザクォータを適用します。
>
> ファイルまたはディレクトリ原因 ONTAP の名前でクォータのユーザを指定しても、そのファイルまたはディレクトリにクォータを適用されるわけではありません。

デフォルトのユーザクォータおよびグループクォータで派生クォータを作成する方法

デフォルトのユーザクォータまたはグループクォータを作成すると、同じレベルでファイルを所有するユーザまたはグループごとに、対応する派生ユーザクォータまたは派生グループクォータが自動的に作成されます。

派生ユーザクォータと派生グループクォータは、次のように作成されます。

- FlexVol 上のデフォルトユーザクォータによって、ボリューム上のファイルを所有するすべてのユーザに派生ユーザクォータが作成されます。
- qtree 上のデフォルトユーザクォータによって、 qtree 内のファイルを所有するすべてのユーザに派生ユーザクォータが作成されます。
- FlexVol 上のデフォルトグループクォータによって、ボリューム上の任意の場所のファイルを所有するすべてのグループに派生グループクォータが作成されます。

- qtree 上のデフォルトグループクォータによって、 qtree 内のファイルを所有するすべてのグループに派生グループクォータが作成されます。

デフォルトのユーザクォータまたはグループクォータのレベルでファイルを所有していないユーザまたはグループには、派生クォータは作成されません。たとえば、 qtree proj1 にデフォルトユーザクォータが作成され、ユーザ jsmith が異なる qtree 上のファイルを所有している場合、 jsmith には派生ユーザクォータが作成されません。

派生クォータの設定は、制限やユーザマッピングなど、デフォルトクォータと同じです。たとえば、デフォルトユーザクォータのディスク制限が 50MB でユーザマッピングが有効の場合、作成される派生クォータもディスク制限が 50MB でユーザマッピングが有効になります。

ただし、 3 つの特殊なユーザとグループの場合、派生クォータに制限はありません。次のユーザとグループがデフォルトのユーザクォータまたはグループクォータのレベルでファイルを所有している場合、派生クォータはデフォルトのユーザクォータまたはグループクォータと同じユーザマッピング設定で作成されますが、単なる追跡クォータになります（制限なし）。

- UNIX root ユーザ（ UID 0 ）
- UNIX ルートグループ（ GID 0 ）
- Windows BUILTIN\Administrators グループ

  Windows グループのクォータはユーザクォータとして追跡されるため、このグループの派生クォータは、デフォルトグループクォータではなくデフォルトユーザクォータから派生するユーザクォータになります。

派生ユーザクォータの例

root、jsmith、bobという3人のユーザがファイルを所有しているボリュームにデフォルトユーザクォータを作成すると、ONTAPによって自動的に3つの派生ユーザクォータが作成されます。このため、このボリュームのクォータを再初期化すると、次の 4 つの新しいクォータがクォータレポートに表示されます。

```
cluster1::> volume quota report
  Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *          0B   50MB       0       -   *
vol1               user    root       5B      -       1       -
vol1               user    jsmith    30B   50MB      10       -   *
vol1               user    bob       40B   50MB      15       -   *
4 entries were displayed.
```

最初の新しい行は作成したデフォルトユーザクォータで、 ID がアスタリスク（ * ）であることから判別できます。ほかの新しい行は派生ユーザクォータです。jsmith と bob の派生クォータのディスク制限は、デフォルトクォータと同じく 50MB です。root ユーザの派生クォータは、制限のない追跡クォータです。

rootユーザへのクォータの適用方法

UNIXクライアントのrootユーザ（UID=0）にはツリークォータが適用されますが、ユーザクォータまたはグループクォータは適用されません。これにより、 root ユーザは、通常ならクォータによって妨げられるような操作を他のユーザに代わって実行できます。

`chown` Privilegesの少ないユーザの代わりにrootユーザがファイルやディレクトリの所有権の変更やその他の処理（UNIXコマンドなど）を実行すると、ONTAPは新しい所有者に基づいてクォータをチェックしますが、新しい所有者のハードクォータ制限を超えた場合でも、エラーの報告や処理の停止は行いません。これは、消失データのリカバリなど、管理作業のために一時的にクォータを超過する場合に役立ちます。

ただし、所有権の変更後、クォータの超過中にユーザがディスクスペースの割り当てサイズを増やそうとすると、クライアントシステムによりディスクスペースエラーが報告されます。

関連情報

- "クォータの適用方法"
- "複数のIDを持つユーザにクォータを適用する方法"

特殊なWindowsグループとクォータ

クォータの処理が他のWindowsグループとは異なる特別なWindowsグループがいくつかあります。これらの特殊グループにクォータがどのように適用されるかを理解しておく必要があります。

ONTAP では、 Windows GID に基づいたグループクォータはサポートされません。Windowsグループ IDをクォータターゲットとして指定した場合、そのクォータはユーザクォータとみなされます。

Everyone

クォータターゲットがEveryoneグループの場合、ACLの所有者がEveryoneであるファイルは、EveryoneのSIDの下にカウントされます。

組み込み管理者

クォータターゲットがBUILTIN\Administratorsグループの場合、そのエントリはユーザクォータとみなされ、追跡のみに使用されます。BUILTIN\Administrators には制限を適用できません。BUILTIN\Administratorsのメンバーがファイルを作成すると、そのファイルはBUILTIN\Administratorsによって所有され、BUILTIN\AdministratorsのSID（ユーザの個人SIDではなく）でカウントされます。

複数のIDを持つユーザにクォータを適用する方法

ユーザは複数のIDで表すことができます。IDのリストをクォータターゲットとして指定することで、そのようなユーザに対して単一のユーザクォータを定義できます。これらのIDのいずれかが所有するファイルには、ユーザクォータの制限が適用されます。

ユーザがUNIX UID `20`と`Windows ID `corp\john_smith`とを持っているとします

`engineering\jsmith。このユーザに対して、UIDとWindows IDのリストをクォータターゲットとするクォータを指定できます。このユーザがストレージシステムに書き込むと、書き込み元がUID 20、corp\john_smith、、のいずれであるかに関係なく、指定されたクォータが適用され `engineering\jsmith`ます。

複数のIDが同じユーザに属している場合でも、別 々 のクォータルールは別 々 のターゲットとみなされます。たとえば、UID 20`が1GBのディスクスペースに制限されるクォータとcorp\john_smithが2GBのディスクスペースに制限されるクォータを同じユーザに対して指定できます。ただし、どちらのIDも同じユーザを表しています。ONTAPはUIDにクォータを `20 `corp\john_smith`個別に適用します。この場合、`engineering\jsmith`同じユーザが使用する他のIDに制限が適用されても、制限はに適用されません。

関連情報

- "クォータの適用方法"
- "rootユーザへのクォータの適用方法"

混在環境での**ONTAP**によるユーザ**ID**の決定方法

ユーザがWindowsクライアントとUNIXクライアントの両方からONTAPストレージにアクセスしている場合は、ファイルの所有権の決定にWindowsセキュリティとUNIXセキュリティの両方のセキュリティが使用されます。ONTAP では、ユーザクォータの適用時に UNIX ID と Windows ID のどちらを使用するかを、複数の条件から決定します。

ファイルを含む qtree または FlexVol ボリュームのセキュリティ形式が NTFS のみまたは UNIX のみである場合、そのセキュリティ形式によって、ユーザクォータの適用時に使用される ID の種類が決定されます。mixed セキュリティ形式の qtree の場合、使用される ID の種類は、ファイルに ACL が設定されているかどうかによって決まります。

次の表は、使用されるIDのタイプをまとめたものです。

セキュリティ形式	**ACL**	**ACL** はありません
UNIX	UNIX ID	UNIX ID
mixed	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

複数のユーザに対するクォータの処理

複数のユーザを同じクォータターゲットに配置した場合、クォータによって定義された制限は各ユーザに適用されません。クォータ制限は、クォータターゲット内のすべてのユーザで共有されます。

ボリュームやqtreeなどのオブジェクトの管理用コマンドとは異なり、クォータターゲット（マルチユーザクォータを含む）の名前は変更できません。つまり、マルチユーザクォータが定義されたあとは、クォータターゲット内のユーザを変更できず、ターゲットへのユーザの追加やターゲットからのユーザの削除もできません。マルチユーザクォータに対してユーザを追加または削除する場合は、そのユーザを含むクォータを削除し、ターゲットにユーザのセットを含む新しいクォータルールを定義する必要があります。

複数のユーザクォータを1つのマルチユーザクォータに結合した場合、クォータのサイズを変更して変更をアクティブ化できます。ただし、複数のユーザが含まれているクォータターゲットからユーザを削除したり、すでに複数のユーザが含まれているターゲットにユーザを追加したりする場合は、変更を有効にする前にクォータを再初期化する必要があります。

クォータルールに複数のユーザが含まれる例

次の例では、クォータエントリに2人のユーザがリストされています。2人のユーザーは、合計で最大80MBのスペースを使用できます。一方が75MBを使用している場合、もう一方は5MBしか使用できません。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0                Policy: default           Volume: vol1
                                                     Soft             Soft
                               User         Disk     Disk    Files    Files
Type    Target         Qtree   Mapping     Limit    Limit    Limit    Limit
Threshold
-----  --------       ------- -------  --------  -------  ------  -------
---------
user    "jsmith,chen"  ""      off          80MB        -       -        -
-
```

クォータの**UNIX**名と**Windows**名のリンク

混在環境では、ユーザは Windows ユーザまたは UNIX ユーザとしてログインできます。クォータは、ユーザの UNIX ID と Windows ID が同じユーザを表すことを認識するように設定できます。

次の両方の条件に該当する場合、Windowsユーザ名のクォータはUNIXユーザ名に（またはその逆に）マッピングされます。

- この `user-mapping`パラメータは、ユーザのクォータルールで「on」に設定されています。
- ユーザ名がコマンドにマッピングされている `vserver name-mapping`。

UNIX名とWindows名が一緒にマッピングされると、クォータ使用量の決定には同じユーザとして扱われます。

ツリークォータの機能

ツリークォータの機能の概要

qtree をターゲットとしてクォータを作成して、ターゲットの qtee の大きさを制限できます。これらのクォータは、 _tree quotas _ とも呼ばれます。

特定の qtree に対して、ユーザクォータやグループクォータを作成することもできます。また、 FlexVol ボリュームのクォータは、そのボリュームに含まれる qtree に継承される場合があります。

qtree にクォータを適用すると、ディスクパーティションと同様の結果が得られます。ただし、クォータを変更することで、 qtree の最大サイズをいつでも変更できます。ツリークォータを適用すると、 ONTAP は所有者に関係なく qtree のディスクスペースとファイル数を制限します。書き込み処理によってツリークォータを超える場合、 root ユーザと BUILTIN\Administrators グループのメンバーを含むすべてのユーザは qtree への書き込みを行うことができません。

クォータのサイズは、利用可能なスペースの量を保証するものではありません。クォータのサイズは、 qtree で使用可能な空きスペースの量よりも多く設定できます。コマンドを使用すると、qtree内で実際に利用可能なスペースの量を確認できます `volume quota report`。

の詳細については `volume quota report`、を"ONTAPコマンド リファレンス"参照してください。

qtreeとユーザクォータおよびグループクォータ

ツリークォータは、qtreeの全体的なサイズを制限します。個 々 のユーザまたはグループがqtree全体を使用しないようにするには、そのqtreeのユーザクォータまたはグループクォータを指定します。

qtree内のユーザクォータの例

次のクォータルールがあるとします。

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                          User          Disk     Disk    Files    Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""      off           50MB        -       -        -
45MB
user    jsmith    ""      off           80MB        -       -        -
75MB
```

あるユーザkjonesが、vol1に存在する重要なqtree proj1で大量のスペースを消費しています。次のクォータルールを追加することで、このユーザのスペースを制限できます。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                         User         Disk       Disk    Files    Files
Type    Target    Qtree  Mapping      Limit      Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""     off           50MB        -       -        -
45MB
user    jsmith    ""     off           80MB        -       -        -
75MB
user    kjones    proj1  off           20MB        -       -        -
15MB
```

FlexVol volumeのデフォルトツリークォータで派生ツリークォータを作成する方法

FlexVol ボリューム上にデフォルトのツリークォータを作成すると、そのボリューム内のすべての qtree に、対応する派生ツリークォータが自動的に作成されます。

これらの派生ツリークォータには、デフォルトのツリークォータと同じ制限があります。他のクォータが存在しない場合、これらの制限は次のように作用します。

- ユーザはそのボリューム全体で割り当てられているスペースと同じスペースを qtree で使用できます（ただし、ルートまたは別の qtree のスペースを使用してボリュームの制限値を超えていない場合）。
- 各 qtree がボリュームの全容量まで拡張できます。

ボリューム上のデフォルトのツリークォータは、そのボリュームに追加されるすべての新しい qtree に引き続き適用されます。新しい qtree が作成されるたびに、派生ツリークォータも作成されます。

すべての派生クォータと同様に、派生ツリークォータは次のように動作します。

- ターゲットに明示的クォータがない場合にのみ作成されます。
- クォータレポートには表示されますが、コマンドを使用してクォータルールを表示する場合は表示されません。`volume quota policy rule show`の詳細については、`volume quota policy rule show`を"ONTAPコマンド リファレンス"参照してください。

派生ツリークォータの例

3 つの qtree （ proj1 、 proj2 、および proj3 ）を含むボリュームが存在し、唯一のツリークォータがディスクサイズを 10GB に限定する proj1 qtree 上の明示的クォータであるとします。このボリュームでデフォルトのツリークォータを作成し、ボリュームのクォータを再初期化すると、クォータレポートには 4 つのツリークォータが表示されます。

```
                                      ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     tree    1           0B   10GB       1       -   proj1
vol1               tree    *           0B   20GB       0       -   *
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj3     tree    3           0B   20GB       1       -   proj3
...
```

最初の行には、 proj1 qtree 上の当初の明示的クォータが示されます。このクォータは変更されません。

2 行目には、ボリュームの新しいデフォルトのツリークォータが示されます。アスタリスク（ * ）クォータ指定子は、デフォルトクォータであることを示します。このクォータは、作成したクォータルールの結果です。

最後の 2 行には、 proj2 および proj3 qtree の新しい派生ツリークォータが示されます。これらのクォータは、ボリューム上のデフォルトのツリークォータの結果として、 ONTAP によって自動的に作成されました。これらの派生ツリークォータには、ボリューム上のデフォルトのツリークォータと同じ 20GB のディスク制限があります。proj1 qtree にはすでに明示的クォータが存在するため、 proj1 qtree には派生ツリークォータが作成されませんでした。 ONTAP

FlexVol volumeのデフォルトユーザクォータがそのボリュームの**qtree**のクォータに与える影響

FlexVol ボリュームにデフォルトユーザクォータが定義されている場合、明示的ツリークォータまたは派生ツリークォータが存在する、そのボリュームに含まれるすべての qtree にデフォルトユーザクォータが自動的に作成されます。

qtree にデフォルトユーザクォータがすでに存在する場合は、ボリュームにデフォルトユーザクォータが作成されても qtree のデフォルトユーザクォータが影響を受けることはありません。

qtree に自動的に作成されるデフォルトユーザクォータには、ユーザがボリュームに作成するデフォルトユーザクォータと同じ制限があります。

qtree の明示的ユーザクォータは、管理者が作成した qtree のデフォルトユーザクォータを上書きするのと同様に、自動的に作成されるデフォルトユーザクォータを上書きします（制限を置き換えます）。

qtreeの変更がクォータに与える影響

qtree を削除したり、名前やセキュリティ形式を変更したりすると、現在適用されているクォータに応じて、 ONTAP が適用するクォータが変更される場合があります。

qtreeの削除とツリークォータ

qtree を削除すると、その qtree に適用されるクォータはすべて、明示的クォータか派生クォータかにかかわらず、 ONTAP によって適用されなくなります。

クォータルールが維持されるかどうかは、qtreeを削除する場所によって異なります。

- ONTAP を使用して qtree を削除した場合、ツリークォータルールや、その qtree に設定されているユーザおよびグループクォータルールも含め、その qtree のクォータルールは自動的に削除されます。
- CIFSクライアントまたはNFSクライアントを使用してqtreeを削除した場合、クォータの再初期化時のエラーを回避するために、そのqtreeのクォータルールをすべて削除する必要があります。削除したqtreeと同じ名前の新しいqtreeを作成した場合、既存のクォータルールは、クォータを再初期化するまで新しいqtreeに適用されません。

qtree名の変更がクォータに与える影響

ONTAP を使用して qtree の名前を変更すると、その qtree のクォータルールは自動的に更新されます。CIFS または NFS クライアントを使用して qtree の名前を変更する場合、その qtree のクォータルールをすべて更新する必要があります。

CIFSまたはNFSクライアントを使用してqtreeの名前を変更し、クォータを再初期化する前に新しい名前でそのqtreeのクォータルールを更新しないと、クォータはqtreeに適用されません。qtreeの明示的クォータ（ツリークォータ、qtreeのユーザクォータまたはグループクォータなど）は、派生クォータに変換されることがあります。

qtreeのセキュリティ形式とユーザクォータ

アクセス制御リスト（ ACL ）は、 NTFS または mixed セキュリティ形式では qtree に適用できますが、 UNIX セキュリティ形式では適用できません。qtreeのセキュリティ形式を変更すると、クォータの計算方法に影響することがあります。qtree のセキュリティ形式を変更した場合は、必ずクォータを再初期化してください。

qtreeのセキュリティ形式をNTFS形式またはmixed形式からUNIX形式に変更した場合、そのqtree内のファイルのACLはすべて無視され、ファイルの使用量はUNIXユーザIDに基づいて加算されます。

qtreeのセキュリティ形式をUNIX形式からmixed形式またはNTFS形式に変更すると、それまで非表示だったACLが表示されるようになります。また、無視されたACLは再び有効になり、NFSユーザ情報は無視されます。既存のACLがない場合は、引き続きNFS情報がクォータの計算に使用されます。

qtreeのセキュリティ形式を変更したあとにUNIXユーザとWindowsユーザの両方のクォータ使用量が正しく計算されるようにするには、そのqtreeを含むボリュームのクォータを再初期化する必要があります。

例

次の例は、qtreeのセキュリティ形式を変更した場合に、そのqtree内のファイルの使用料として別のユーザに課金されることを示しています。

qtree AでNTFSセキュリティが有効で、ACLによってWindowsユーザに `corp\joe`5MBのファイルの所有権が付与されているとします。ユーザ `corp\joe`には、qtree Aの5MBのディスクスペース使用量が課金されます。

次に、qtree Aのセキュリティ形式をNTFSからUNIXに変更します。クォータが再初期化されると、 `corp\joe` このファイルはWindowsユーザに課金されなくなり、ファイルのUIDに対応するUNIXユーザに課金されます。UIDには、マッピング先のUNIXユーザ `corp\joe`またはrootユーザを指定できます。

クォータをアクティブ化する方法

クォータをアクティブ化する方法の概要

新しいクォータおよび既存のクォータに対する変更を有効にするには、アクティブ化する必要があります。アクティブ化はボリュームレベルで実行されます。クォータのアクティブ化の仕組みを理解しておくと、システム停止を抑えてクォータを管理するのに役立ちます。

クォータは、 _initializing （有効にする）または _resizing _ でアクティブ化されます。クォータを無効にして再度有効にすることを再初期化と呼びます。

アクティブ化にかかる時間とアクティブ化がクォータ適用に及ぼす影響は、アクティブ化のタイプによって異なります。

- 初期化プロセスは、ジョブとボリュームのファイルシステム全体のクォータスキャンの2つの部分で `quota on`構成されます。スキャンは、ジョブが正常に完了した後に開始され `quota on`ます。クォータスキャンには時間がかかることがあります。ボリュームのファイル数が多いほど、スキャンにかかる時間は長くなります。スキャンが完了するまで、クォータのアクティブ化は完了せず、クォータも適用されません。
- サイズ変更プロセスにはジョブのみが含まれ `quota resize`ます。サイズ変更にはクォータスキャンが含まれないため、クォータの初期化よりも短時間で完了します。サイズ変更プロセス中もクォータは引き続き適用されます。

デフォルトでは `quota on`、および `quota resize`ジョブはバックグラウンドで実行されるため、他のコマンドを同時に使用できます。

アクティブ化プロセスのエラーと警告は、イベント管理システムに送信されます。パラメータをコマンドまたは `volume quota resize`コマンドとともに `volume quota on`使用する `-foreground`と、ジョブが完了するまでコマンドは戻りません。これは、スクリプトから再初期化する場合に便利です。あとでエラーや警告を表示するには、パラメータを指定してコマンドを `-instance`使用し `volume quota show`ます。

クォータのアクティブ化は、停止およびリブート後も維持されます。クォータのアクティブ化プロセスは、ストレージシステムデータの可用性には影響しません。

関連情報

- "ボリュームクォータ"
- "ボリュームクォータのサイズ変更"
- "volume quota show"

サイズ変更を使用する状況について理解する

クォータのサイズ変更はONTAPの便利な機能です。また、サイズ変更はクォータの初期化よりも高速であるため、可能なかぎりサイズ変更を使用してください。ただし、注意が必要な制限事項がいくつかあります。

サイズ変更は、特定のタイプのクォータ変更に対してのみ機能します。次の種類の変更をクォータルールに加えた場合、クォータのサイズを変更できます。

- 既存のクォータを変更する場合

  たとえば、既存のクォータの制限を変更する場合などです。

- デフォルトクォータまたはデフォルト追跡クォータが存在するクォータターゲットにクォータを追加する。
- デフォルトクォータまたはデフォルト追跡クォータエントリが指定されているクォータを削除する。
- 複数のユーザクォータを1つのマルチユーザクォータに結合します。

クォータの大幅な変更を行った場合は、完全な再初期化を実行して、すべての変更を確実に有効にしてください。

サイズを変更しようとしてサイズ変更処理では反映できないクォータの変更があった場合、ONTAP は警告を発行します。ストレージシステムが特定のユーザ、グループ、または qtree のディスク使用量を追跡しているかどうかは、クォータレポートから判断できます。クォータレポートにクォータが表示される場合、ストレージシステムは、クォータターゲットによって所有されているディスクスペースとファイル数を追跡しています。

サイズ変更によって有効にできるクォータ変更の例

一部のクォータルール変更は、サイズ変更によって有効にできます。次のクォータを考えてみましょう。

```
#Quota Target type              disk  files thold sdisk sfile
#------------ ----              ----  ----- ----- ----- -----
*              user@/vol/vol2    50M   15K
*              group@/vol/vol2  750M   85K
*              tree@/vol/vol2      -     -
jdoe           user@/vol/vol2/  100M   75K
kbuck          user@/vol/vol2/  100M   75K
```

次の変更を行ったとします。

- デフォルトユーザターゲットのファイル数を増やします。
- デフォルトユーザクォータよりも多くのディスク制限が必要な新規ユーザ boris への、新しいユーザクォータの追加
- kbuckユーザの明示的クォータエントリを削除します。新しいユーザに必要なのはデフォルトクォータ制限だけです。

これらの変更により、クォータは次のようになります。

```
#Quota Target type              disk  files thold sdisk sfile
#------------ ----              ----  ----- ----- ----- -----
*              user@/vol/vol2    50M   25K
*              group@/vol/vol2  750M   85K
*              tree@/vol/vol2      -     -
jdoe           user@/vol/vol2/  100M   75K
boris          user@/vol/vol2/  100M   75K
```

サイズ変更によって、これらの変更がすべてアクティブ化されます。完全なクォータ再初期化は必要ありませ

ん。

クォータの完全な再初期化が必要な状況

クォータのサイズ変更の方が高速ですが、クォータに特定の小規模または大規模な変更を加える場合は、クォータの完全な再初期化を実行する必要があります。

次の状況では、クォータの完全な再初期化を実行する必要があります。

- これまでクォータがなかった（明示的クォータとデフォルト クォータから派生したクォータのいずれも）ターゲットにクォータを作成する場合。
- qtreeのセキュリティ形式をUNIX形式からmixed形式、またはNTFS形式に変更した場合
- qtreeのセキュリティ形式をmixed形式またはNTFS形式からUNIX形式に変更した場合
- 複数のユーザを含むクォータ ターゲットからユーザを削除した場合、またはすでに複数のユーザを含むターゲットにユーザを追加した場合
- クォータに大幅な変更を加えた場合

初期化を必要とするクォータの変更例

3つのqtreeを含むボリュームがあり、ボリューム内のクォータは明示的ツリー クォータ3つだけであるとします。このボリュームに次の変更を加えることにしました。

- 新しいqtreeを追加し、新しいツリー クォータを作成する
- ボリュームのデフォルト ユーザ クォータを追加する

これらのどちらの変更にも、クォータの完全な初期化が必要です。サイズ変更では対応できません。

クォータ情報の表示方法

クォータ情報の表示の概要

クォータレポートを使用して、クォータルールおよびクォータポリシーの設定、適用および設定されたクォータ、クォータのサイズ変更および再初期化中に発生したエラーなどの詳細を表示できます。

クォータ情報は、次のような場合に表示すると役に立ちます。

- クォータの設定（クォータの設定や設定の検証など）
- ディスクスペースまたはファイルの制限にまもなく到達する、または制限に達したという通知への対応
- スペースの追加要求への対応

クォータレポートを使用して有効なクォータを確認する

クォータはさまざまな方法で作用するため、明示的に作成したクォータよりも多くのクォータが有効になります。有効なクォータを確認するには、クォータレポートを表示します。

次の例は、FlexVol volume vol1と、そのボリュームに含まれるqtree q1に適用されている各種クォータのクォ

ータレポートを表示します。

qtreeにユーザクォータが指定されていない例

この例では、ボリュームvol1に含まれるqtree q1が1つあります。管理者が3つのクォータを作成しました。

- vol1に対するデフォルトのツリークォータ制限は400MB
- vol1に対して100MBのデフォルトユーザクォータ制限
- ユーザjsmith用にvol1に対して200MBの明示的ユーザクォータ制限

これらのクォータのクォータルールは、次の例のようになります。

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                  Soft             Soft
                          User          Disk      Disk    Files    Files
Type    Target    Qtree   Mapping      Limit     Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree    ""        ""      -           400MB        -       -        -
-
user    ""        ""      off         100MB        -       -        -
-
user    jsmith    ""      off         200MB        -       -        -
-
```

これらのクォータのクォータレポートの例を次に示します。

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith    150B  200MB       7       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     q1         user   *           0B  100MB       0       -
vol1     q1         user   jsmith      0B  100MB       5       -
vol1     -          user   root        0B    0MB       1       -
vol1     q1         user   root        0B    0MB       8       -
```

クォータレポートの最初の3行には、管理者が指定した3つのクォータが表示されます。これらのクォータのうち2つはデフォルトクォータであるため、ONTAPによって自動的に派生クォータが作成されます。

4行目には、vol1のすべてのqtree（この例ではq1のみ）のデフォルトツリークォータから派生するツリークォータが表示されます。

5行目には、ボリュームにデフォルトユーザクォータが存在することによってqtreeに作成されるデフォルトユーザクォータとqtreeクォータが表示されます。

6行目には、qtreeのjsmithに作成される派生ユーザクォータが表示されます。これは、qtreeにはデフォルトユーザクォータ（5行目）があり、ユーザjsmithがそのqtreeのファイルを所有しているためです。qtree q1のユーザjsmithに適用される制限は、明示的ユーザクォータ制限（200MB）では決定されません。これは、明示的ユーザクォータ制限がボリュームに対して適用されるため、qtreeの制限には影響しないためです。代わりに、qtreeの派生ユーザクォータ制限は、qtreeのデフォルトユーザクォータ（100MB）で決定されます。

最後の2行には、そのボリュームおよびqtreeのデフォルトユーザクォータから派生するその他のユーザクォータが表示されます。rootユーザがボリュームとqtreeの両方にファイルを所有しているため、ボリュームとqtreeの両方のrootユーザに派生ユーザクォータが作成されました。rootユーザはクォータに関して特別な扱いを受けるため、rootユーザの派生クォータは追跡クォータのみです。

qtreeにユーザクォータを指定した例

この例は前の例に似ていますが、管理者がqtreeに2つのクォータを追加している点が異なります。

ボリュームは1つ（vol1）、qtreeは1つ（q1）です。管理者が次のクォータを作成しました。

- vol1に対するデフォルトのツリークォータ制限は400MB
- vol1に対して100MBのデフォルトユーザクォータ制限
- ユーザjsmithのためにvol1に対して200MBの明示的ユーザクォータ制限
- qtree q1に対する50MBのデフォルトユーザクォータ制限
- ユーザjsmithのためにqtree q1に対して75MBの明示的ユーザクォータ制限

これらのクォータのクォータルールは次のようになります。

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                  Soft             Soft
                          User         Disk      Disk    Files     Files
Type   Target    Qtree    Mapping      Limit     Limit   Limit     Limit
Threshold
-----  --------  -------  -------  --------  -------  ------  -------
---------
tree   ""        ""       -           400MB        -       -        -
-
user   ""        ""       off         100MB        -       -        -
-
user   ""        q1       off          50MB        -       -        -
-
user   jsmith    ""       off         200MB        -       -        -
-
user   jsmith    q1       off          75MB        -       -        -
-
```

これらのクォータのクォータレポートは次のようになります。

```
cluster1::> volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith   2000B  200MB       7       -   jsmith
vol1     q1         user   *           0B   50MB       0       -   *
vol1     q1         user   jsmith      0B   75MB       5       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     -          user   root        0B    0MB       2       -
vol1     q1         user   root        0B    0MB       1       -
```

クォータレポートの最初の5行には、管理者によって作成された5つのクォータが表示されます。これらのクォータの一部はデフォルトクォータであるため、ONTAPによって自動的に派生クォータが作成されます。

6行目には、vol1のすべてのqtree（この例ではq1のみ）のデフォルトツリークォータから派生するツリークォータが表示されます。

最後の2行には、そのボリュームおよびqtreeのデフォルトユーザクォータから派生するユーザクォータが表示

されます。rootユーザがボリュームとqtreeの両方にファイルを所有しているため、ボリュームとqtreeの両方のrootユーザに派生ユーザクォータが作成されました。rootユーザはクォータに関して特別な扱いを受けるため、rootユーザの派生クォータは追跡クォータのみです。

次の理由により、他のデフォルトクォータまたは派生クォータは作成されませんでした。

- このユーザにはすでに両方のレベルで明示的クォータが設定されているため、ボリュームとqtreeの両方にファイルを所有していても、jsmithユーザに派生ユーザクォータは作成されませんでした。
- このボリュームまたはqtreeに他のユーザがファイルを所有していないため、他のユーザに派生ユーザクォータは作成されませんでした。
- qtreeにはすでにデフォルトユーザクォータが設定されているため、このボリュームのデフォルトユーザクォータによってqtreeにデフォルトユーザクォータが作成されませんでした。

適用クォータが設定されたクォータとは異なる理由

適用クォータは、設定されたクォータとは異なります。派生クォータが設定されることなく適用されるのに対し、設定されたクォータは正常に初期化されたあとにのみ適用されるためです。これらの違いを理解すると、クォータレポートに表示される適用クォータを、設定したクォータと比較しやすくなります。

クォータレポートに示される適用クォータは、次の理由から、設定されたクォータルールとは異なる場合があります。

- 派生クォータはクォータルールとして設定されることなく適用されます。派生クォータは、デフォルトクォータに応じてONTAPによって自動的に作成されます。
- あるボリュームで、クォータルールが設定されたあとにクォータが再初期化されていない可能性があるため。
- ボリュームでクォータが初期化されたときにエラーが発生した可能性がある。

クォータレポートを使用して、特定のファイルへの書き込みを制限するクォータを特定する

特定のファイルパスを指定して volume quota report コマンドを実行し、どのクォータ制限がファイルへの書き込み処理に影響しているかを特定できます。これは、どのクォータが書き込み処理を妨げているかを把握するのに役立ちます。

手順

1. path パラメータを指定して volume quota report コマンドを実行します。

特定のファイルに影響しているクォータを表示する例

次の例は、 FlexVol ボリューム vol2 の qtree q1 にあるファイル file1 への書き込みに対して有効なクォータを確認するコマンドと出力を示しています。

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
                                       ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     q1        tree    jsmith     1MB  100MB       2   10000   q1
vol2     q1        group   eng        1MB  700MB       2   70000
vol2               group   eng        1MB  700MB       6   70000   *
vol2               user    corp\jsmith
                                      1MB   50MB       1       -   *
vol2     q1        user    corp\jsmith
                                      1MB   50MB       1       -
5 entries were displayed.
```

ONTAPのクォータに関する情報を表示するコマンド

コマンドを使用して、適用クォータとリソース使用量が含まれるクォータレポート、クォータの状態とエラーに関する情報、またはクォータポリシーとクォータルールに関する情報を表示できます。

次のコマンドは、FlexVolボリュームに対してのみ実行できます。

状況	使用するコマンド
適用クォータに関する情報を表示します	`volume quota report`
クォータターゲットのリソース使用量（ディスクスペースとファイル数）を表示します	`volume quota report`
ファイルへの書き込みが許可された場合にどのクォータ制限に影響するかを確認します	`volume quota report`パラメータを指定した場合 `-path`
クォータの状態（、 `off`など）を表示する `on initializing`	`volume quota show`
クォータのメッセージロギングに関する情報を表示します	`volume quota show`パラメータを指定した場合 `-logmsg`
クォータの初期化とサイズ変更中に発生するエラーを表示する	`volume quota show`パラメータを指定した場合 `-instance`

状況	使用するコマンド
クォータポリシーに関する情報を表示します	`volume quota policy show`
クォータルールに関する情報を表示します	`volume quota policy rule show`
Storage Virtual Machine（SVM、旧Vserver）に割り当てられているクォータポリシーの名前を表示する	`vserver show`パラメータを指定した場合 `-instance`

の詳細については `volume quota`、を"ONTAPコマンド リファレンス"参照してください。

volume quota policy rule showコマンドと**volume quota report**コマンドを使用する状況

どちらのコマンドでもクォータに関する情報が表示されますが、には `volume quota policy rule show`設定されたクォータルールがすぐに表示され、コマンドでは `volume quota report`より多くの時間とリソースが消費されるため、適用クォータとリソース使用量が表示されます。

この `volume quota policy rule show`コマンドは、次の場合に役立ちます。

- アクティブ化する前にクォータルールの設定を確認してください

  このコマンドは、クォータが初期化されているかサイズ変更されているかに関係なく、設定されているクォータルールをすべて表示します。

- システムリソースに影響を与えずにクォータルールを迅速に表示します

  ディスクとファイルの使用量は表示されないため、このコマンドはクォータレポートほどリソースを消費しません。

- SVM に割り当てられていないクォータポリシー内のクォータルールを表示する

の詳細については `volume quota policy rule show`、を"ONTAPコマンド リファレンス"参照してください。

この `volume quota report`コマンドは、次の場合に役立ちます。

- 派生クォータも含め、適用クォータを表示する
- 派生クォータの影響を受けるターゲットも含め、有効になっているすべてのクォータによって使用されているディスクスペースとファイル数を表示する

  （デフォルトクォータの場合、生成される派生クォータに照らして使用状況が追跡されるため、使用量は「 0 」と表示されます。）

- ファイルへの書き込みが許可される状況にどのクォータ制限が影響するかを確認します

  パラメータをコマンドに `volume quota report`追加します `-path`。

クォータレポートの生成には大量のリソースを消費します。クラスタ内の多数のFlexVolに対して実行すると、完了までに時間がかかることがあります。SVM 内の個々のボリュームのクォータレポートを表示する方が効率的です。

の詳細については `volume quota report`、を"ONTAPコマンド リファレンス"参照してください。

クォータレポートと**UNIX**クライアントで表示されるスペース使用量の相違

クォータレポートと**UNIX**クライアントで表示されるスペース使用量の違いの概要

クォータレポートに表示されるFlexVol volumeまたはqtreeの使用済みディスクスペースの値は、UNIXクライアントに表示される同じボリュームまたはqtreeの値と異なる場合があります。これらの値が異なるのは、クォータレポートとUNIXコマンドによるボリュームまたはqtree内のデータブロックの計算方法が異なるためです。

たとえば、空のデータブロック（データが書き込まれていないブロック）を含むファイルがボリュームに含まれている場合、ボリュームのクォータレポートでは、スペース使用量の報告時に空のデータブロックはカウントされません。ただし、ボリュームがUNIXクライアントにマウントされていて、このファイルがコマンドの出力として表示される場合は `ls`、空のデータブロックもスペース使用量に含まれます。そのため、 `ls`クォータレポートに表示されるスペース使用量よりも、コマンドで表示されるファイルサイズの方が大きくなります。

同様に、クォータレポートに表示されるスペース使用量の値は、や `du`などのUNIXコマンドの結果として表示される値と異なる場合があります `df`。

クォータレポートのディスクスペースとファイル使用量の表示

FlexVol volumeまたはqtreeのクォータレポートに指定される使用済みファイル数とディスクスペース容量は、ボリュームまたはqtree内のすべてのinodeに対応する使用済みデータブロックの数によって異なります。

ブロック数には、通常のファイルとストリームファイルに使用される直接ブロックと間接ブロックの両方が含まれます。ディレクトリ、アクセス制御リスト（ACL）、ストリームディレクトリ、およびメタファイルに使用されるブロックは、クォータレポートでは考慮されません。UNIXのスパースファイルの場合、空のデータブロックはクォータレポートに含まれません。

クォータサブシステムは、ユーザが制御可能なファイルシステムの要素だけを考慮し、含めるように設計されています。ディレクトリ、ACL、およびSnapshotスペースは、いずれもクォータ計算から除外されるスペースの例です。クォータは、保証ではなく制限の適用に使用され、アクティブなファイルシステム上でのみ動作します。クォータ計算では、特定のファイルシステム構成はカウントされず、ストレージ効率（圧縮や重複排除など）も考慮されません。

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

lsコマンドとクォータレポートのスペース使用量の不一致

`ls`コマンドを使用してUNIXクライアントにマウントされたFlexVol volumeの内容を表示する場合、出力に表示されるファイルサイズは、ファイルのデータブロックのタイプに応じて、ボリュームのクォータレポートに表示されるスペース使用量と異なることがあります。

コマンドの出力 `ls`には、ファイルサイズのみが表示され、ファイルで使用される間接ブロックは含まれません。ファイルの空ブロックも、コマンドの出力に含まれます。

したがって、空ブロックがないファイルの場合、コマンドによって表示されるサイズは `ls`、クォータレポートのディスク使用量よりも少なくなる可能性があります。これは、クォータレポートに間接ブロックが含まれるためです。逆に、ファイルに空ブロックがある場合、コマンドによって表示されるサイズは `ls`、クォータレポートで指定されたディスク使用量よりも多くなることがあります。

コマンドの出力 `ls`には、ファイルサイズのみが表示され、ファイルで使用される間接ブロックは含まれません。ファイルの空ブロックも、コマンドの出力に含まれます。

lsコマンドとクォータレポートにおけるスペース使用量の違いの例

次のクォータレポートには、 qtree q1 の制限が 10MB であると表示されています。

```
                                      ----Disk----  ----Files-----   Quota
  Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
  -------  ---------  ------  --------  -----  -----  ------  ------
---------
  vol1     q1           tree    user1   10MB  10MB        1       -   q1

...
```

UNIXクライアントからコマンドを使用して表示した場合、次の例に示すように、同じqtree内のファイルのサイズがクォータ制限を超えることがあります `ls`。

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

の詳細については `ls`、を"ONTAPコマンド リファレンス"参照してください。

dfコマンドによるファイルサイズの表示

コマンドでスペース使用量が報告される方法は `df`、2つの条件（qtreeを含むボリュームでクォータが有効か無効か、qtree内のクォータ使用量が追跡されるか）によって異なります。

qtreeを含むボリュームでクォータが有効になっていて、qtree内のクォータ使用量が追跡される場合、コマンドで報告されるスペース使用量は `df`、クォータレポートの値に等しくなります。この場合、クォータ使用量は、ディレクトリ、ACL、ストリームディレクトリ、およびメタファイルによって使用されるブロックを除外します。

ボリュームでクォータが有効になっていない場合、またはqtreeにクォータルールが設定されていない場合、報告されるスペース使用量には、ボリューム内の他のqtreeを含むボリューム全体のディレクトリ、ACL、ストリームディレクトリ、およびメタファイルによって使用されるブロックが含まれます。この場合、コマンドで報告されるスペース使用量は、クォータの追跡時に報告される `df`想定値よりも大きくなります。

クォータ使用量が追跡されているqtreeのマウントポイントからコマンドを実行する `df` と、コマンド出力には、クォータレポートの値と同じスペース使用量が表示されます。ほとんどの場合、ツリークォータルールにディスクのハードリミットが設定されている場合、コマンドで報告される合計サイズは `df` ディスク制限に等しく、使用可能なスペースはクォータのディスク制限とクォータ使用量の差に等しくなります。

ただし、コマンドで報告される使用可能なスペースが、ボリューム全体で使用可能なスペースと同じである場合 `df` があります。これは、qtreeにディスクのハードリミットが設定されていない場合に発生することがあります。ONTAP 9 .9.1以降では、ボリューム全体で使用可能なスペースが残りのツリークォータスペースよりも少ない場合にも発生することがあります。これらのいずれかの状況が発生すると、コマンドによって報告される合計サイズは、qtree内で使用されているクォータにFlexVol volumeで使用可能なスペースを加えた合計サイズ `df` になります。

> この合計サイズは、qtreeのディスク制限でもボリュームの設定サイズでもありません。また、他のqtree内の書き込みアクティビティやバックグラウンドのStorage Efficiencyアクティビティに基づいて変わることもあります。

コマンドおよびクォータレポートのスペース使用量の例 `df`

次のクォータレポートには、qtree aliceには1GB、qtree bobには2GB、qtree project1には無制限のディスク制限が表示されています。

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
                                     ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     alice     tree    1
                                   502.0MB    1GB       2       -   alice
vol2     bob       tree    2
                                    1003MB    2GB       2       -   bob
vol2     project1  tree    3
                                   200.8MB      -       2       -
project1
vol2               tree    *           0B      -       0       -   *
4 entries were displayed.
```

次の例では、qtree AliceおよびBobに対するコマンドの出力で、 `df` クォータレポートと同じ使用済みスペース、および合計サイズ（ブロック数1M）がディスク制限と同じであることが報告されています。これは、qtree aliceとbobのクォータルールにはディスク制限が定義されており、ボリュームの使用可能スペース（1211MB）がqtree alice（523MB）およびqtree bob（1045MB）のツリークォータスペースよりも大きいためです。

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1024   502       523  50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2048  1004      1045  50% /mnt/vol2
```

次の例のqtree Project1に対するコマンドの出力で `df`は、クォータレポートと同じ使用済みスペースが報告されますが、合計サイズは、qtree Project1（201MB）のクォータ使用量にボリューム全体の使用可能スペース（1211MB）を加算して合計1412MBになります。これは、qtree Project1のクォータルールにディスク制限がないためです。

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412   201      1211  15% /mnt/vol2
```

次の例は、ボリューム全体に対するコマンドの出力で、Project1と同じ使用可能スペースが報告されていることを示しています。 `df`

```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
```

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

duコマンドとクォータレポートのスペース使用量の不一致

UNIXクライアントにマウントされたqtreeまたはFlexVol volumeのディスクスペース使用量を確認するコマンドを実行する `du`と、使用量の値は、qtreeまたはボリュームのクォータレポートに表示される値よりも大きくなることがあります。

コマンドの出力 `du`には、コマンドを実行したディレクトリレベルから始まるディレクトリツリー内のすべてのファイルの合計スペース使用量が表示されます。コマンドで表示される使用量の値にはディレクトリのデータブロックも含まれるため `du`、クォータレポートで表示される値よりも大きくなります。

duコマンドとクォータレポートにおけるスペース使用量の違いの例

次のクォータレポートには、 qtree q1 の制限が 10MB であると表示されています。

```
                                        ----Disk----  ----Files-----   Quota
  Volume   Tree      Type    ID         Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  vol1     q1        tree    user1    10MB   10MB   1       -        q1

...
```

次の例では、コマンドの出力に表示されるディスクスペース使用量の `du`値がクォータ制限を超える大きな値になっています。

```
[user1@lin-sys1 q1]$ du -sh
**11M**     q1
```

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

クォータ設定の例

これらの例は、クォータを設定する方法とクォータレポートを確認する方法を理解するのに役立ちます。

これらの例について

次の例は、 `vs1`1つのボリュームを含むSVMを含むストレージシステムを想定してい `vol1`ます。

1. クォータのセットアップを開始するには、SVMの新しいクォータポリシーを作成します。

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

2. 新しいクォータポリシーであるため、このクォータポリシーをSVMに割り当てます。

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

例**1**：デフォルトユーザクォータ

1. では、各ユーザに50MBのハードリミットを課すことにしまし `vol1`た。

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtree ""
```

2. 新しいルールをアクティブ化するには、ボリュームのクォータを初期化します。

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

3. クォータレポートを表示します。

```
cluster1::>volume quota report
```

次のようなクォータレポートが表示されます。

```
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     49MB   50MB      37       -   *
vol1               user    root        0B      -       1       -
```

1 行目には、ディスクリミットを含めて作成したデフォルトユーザクォータが表示されます。すべてのデフォルトクォータと同様に、このデフォルトユーザクォータにはディスクまたはファイルの使用量に関する情報は表示されません。作成されたクォータのほかに、他に2つのクォータが表示されます。のファイルを現在所有しているユーザごとにクォータが1つ設定され `vol1`ます。これらの追加クォータは、デフォルトユーザクォータから自動的に派生するユーザクォータです。このユーザの派生ユーザクォータの `jsmith`ディスク制限は、デフォルトユーザクォータと同じ50MBです。root ユーザの派生ユーザクォータは、追跡クォータ（制限なし）です。

システム上のユーザー（rootユーザー以外）がで50MBを超えるアクション `vol1`（エディタからのファイルへの書き込みなど）を実行しようとすると、アクションは失敗します。

例**2**：デフォルトユーザクォータを無効にする明示的ユーザクォータ

1. `vol1`**`ユーザにボリュームのスペースを追加する必要がある場合は** `jsmith`、次のコマンドを入力します。

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree ""
```

ユーザがクォータルールのターゲットとして明示的に示されるため、これは明示的ユーザクォータになります。

これは `jsmith`、ボリューム上のユーザの派生ユーザクォータのディスク制限を変更するため、既存のクォータ制限に対する変更です。したがって、変更をアクティブ化するためにボリュームのクォータを再初

期化する必要はありません。

2. クォータのサイズを変更するには：

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

サイズを変更する間、クォータは有効なままです。サイズ変更プロセスは短時間で完了します。

次のようなクォータレポートが表示されます。

```
cluster1::> volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    50MB   80MB      37       -   jsmith
vol1               user    root        0B      -       1       -
3 entries were displayed.
```

2行目には、ディスク制限が `80MB`、クォータ指定子が表示され `jsmith`ます。

したがって、 `jsmith` `vol1`他のすべてのユーザーが50MBに制限されていても、では最大80MBのスペースを使用できます。

例**3**：しきい値

ここでは、ユーザが 5MB のディスク制限に達するという時点で通知を受け取ることを想定します。

1. すべてのユーザに45MBのしきい値を作成し、に75MBのしきい値を作成するには `jsmith`、既存のクォータルールを変更します。

```
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree ""
-threshold 45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
-threshold 75MB
```

既存のルールのサイズが変更されるため、変更をアクティブ化するには、ボリュームのクォータのサイズを変更します。サイズ変更プロセスが完了するまで待ちます。

2. クォータレポートとしきい値を表示するには、コマンドにパラメータを `volume quota report`追加し `-thresholds`ます。

```
cluster1::>volume quota report -thresholds
Vserver: vs1
                                     ----Disk----  ----Files-----
Volume   Tree      Type    ID        Used  Limit   Used    Limit  Quota
                                          (Thold)
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -  *
                                         (45MB)
vol1               user    jsmith     59MB   80MB      55       -  jsmith
                                         (75MB)
vol1               user    root        0B      -       1       -
                                         ( -)
3 entries were displayed.
```

しきい値は、 Disk Limit 列にかっこ内に表示されます。

の詳細については `volume quota report`、を"ONTAPコマンド リファレンス"参照してください。

例**4**：**qtree**のクォータ

2 つのプロジェクトのために、いくつかのスペースを分割する必要があるとします。 `proj1` `proj2`これらのプロジェクトに対応するために、という名前の2つの`qtree`を作成できます `vol1`。

現在、ユーザはそのボリューム全体で割り当てられているスペースと同じスペースを qtree で使用できます（ただし、ルートまたは別の qtree でのスペースの使用によってボリュームの制限値を超えていない場合）。さらに、 1 つの qtree で、ボリュームの全容量を使用することもできます。

1. どちらのqtreeも20GBを超えないようにするには、ボリュームにデフォルトのツリークォータを作成します。

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```

正しいタイプは、qtreeではなく_tree_です。

2. これは新しいクォータであるため、サイズ変更によってアクティブ化することはできません。ボリュームのクォータを再初期化します。

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```

影響を受ける各ボリュームのクォータは、コマンドの実行直後にアクティブ化しようとするとエラーが発生する可能性があるため、5分ほど待ってから再アクティブ化してください。`volume quota off`また、コマンドを実行して、特定のボリュームを含むノードからボリュームのクォータを再初期化することもできます。の詳細については `volume quota off`、を"ONTAPコマンド リファレンス"参照してください。

クォータの再初期化プロセスでは強制的にクォータが適用されないため、サイズ変更プロセスよりも時間がかかります。

クォータレポートを表示すると、いくつかの新しい行が表示されます。一部の行はツリークォータ用で、一部の行は派生ユーザクォータ用です。

以下の新しい行は、ツリークォータについてのものです。

```
                                     ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
-------  ---------  ------  --------  -----  -----  ------  ------
---------
...
vol1                tree    *           0B   20GB       0       -   *
vol1     proj1      tree    1           0B   20GB       1       -   proj1
vol1     proj2      tree    2           0B   20GB       1       -   proj2
...
```

作成したデフォルトのツリークォータが最初の新しい行に表示されます。この行の ID 列にはアスタリスク（ * ）が付きます。ボリュームのデフォルトツリークォータに対応して、 ONTAP ではボリューム内の qtree ごとに派生ツリークォータを自動的に作成します。これらは `proj1` `proj2` `Tree`、列にとが表示されている行に表示されます。

以下の新しい行には、派生ユーザクォータについての情報が表示されます。

```
                                     ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
-------  ---------  ------  --------  -----  -----  ------  ------
---------
...
vol1     proj1      user    *           0B   50MB       0       -
vol1     proj1      user    root        0B      -       1       -
vol1     proj2      user    *           0B   50MB       0       -
vol1     proj2      user    root        0B      -       1       -
...
```

ボリュームのデフォルトユーザクォータは、 qtree に対してクォータが有効になっている場合、そのボリュームに含まれるすべての qtree に自動的に継承されます。最初の qtree クォータを追加したときに、 qtree のク

ォータを有効にしました。このため、 qtree ごとに派生デフォルトユーザクォータが作成されました。これらは、 ID がアスタリスク（ * ）である行に示されています。

root ユーザはファイルの所有者であるため、 qtree ごとにデフォルトユーザクォータが作成されたときに、各 qtree の root ユーザに対して特別な追跡クォータも作成されました。これらは、 ID が root である行に示されています。

例**5**：**qtree**のユーザクォータ

1. ユーザが `proj1`qtree内で使用できるスペースは、ボリューム全体で使用できるスペースよりも少なくなります。これらのユーザが `proj1`qtree内で10MBを超えるデータを使用しないようにする。したがって、qtreeのデフォルトユーザクォータを作成します。

   ```
   cluster1::>volume quota policy rule create -vserver vs1 -policy-name
   quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
   -qtree proj1
   ```

   これは、このボリュームのデフォルトユーザクォータから派生した proj1 qtree のデフォルトユーザクォータを変更するため、既存のクォータに対する変更になります。したがって、クォータのサイズを変更して変更をアクティブ化します。サイズ変更プロセスが完了したら、クォータレポートを表示できます。

   qtree の新しい明示的ユーザクォータが示された、次の新しい行がクォータレポートに表示されます。

   ```
                                       ----Disk----  ----Files-----   Quota
   Volume   Tree      Type    ID        Used  Limit    Used   Limit
   Specifier
   -------  --------  ------  -------  -----  -----  ------  ------
   ---------
   vol1     proj1     user    *           0B   10MB       0       -   *
   ```

   ただし、 `jsmith`デフォルトユーザクォータを上書きする（スペースを増やす）ために作成したクォータがボリューム上にあったため、ユーザはproj1 qtreeにこれ以上データを書き込むことができません。`proj1`qtreeにデフォルトユーザクォータを追加したため、そのクォータが適用され、を含むqtree内のすべてのユーザのスペースを制限して `jsmith`います。

2. ユーザにスペースを追加するに `jsmith`は、ディスク制限が80MBのqtreeに対する明示的ユーザクォータルールを追加して、qtreeのデフォルトユーザクォータルールを上書きします。

   ```
   cluster1::>volume quota policy rule create -vserver vs1 -policy-name
   quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
   80MB -qtree proj1
   ```

   これはデフォルトクォータがすでに存在する明示的クォータであるため、クォータのサイズを変更することで変更をアクティブ化できます。サイズ変更プロセスが完了したら、クォータレポートを表示します。

クォータレポートに次の新しい行が表示されます。

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
```

最終的に次のようなクォータレポートが表示されます。

```
cluster1::>volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               tree    *           0B   20GB       0       -   *
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    70MB   80MB      65       -   jsmith
vol1     proj1     tree    1           0B   20GB       1       -   proj1
vol1     proj1     user    *           0B   10MB       0       -   *
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
vol1               user    root        0B      -       3       -
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
11 entries were displayed.
```

ユーザ `jsmith`がのファイルに書き込むには、次のクォータ制限を満たす必要があり `proj1`ます。

1. `proj1`qtreeのツリークォータ
2. `proj1`qtreeのユーザクォータ
3. ボリュームのユーザクォータ。

SVMにクォータを設定する

新しいSVMにクォータを設定して、リソース利用率を管理および監視できます。

タスクの内容

クォータを設定する際には、大まかに言って次の手順を実行します。

1. クォータポリシーを作成します。

2. クォータルールをポリシーに追加する
3. ポリシーをSVMに割り当てる
4. SVM上の各FlexVol volumeでクォータを初期化する

手順

1. コマンドを入力し `vserver show -instance`て、SVMの作成時に自動的に作成されたデフォルトのクォータポリシーの名前を表示します。

   SVMの作成時に名前を指定しなかった場合、名前は「default」です。コマンドを使用すると、デフォルトポリシーに名前を付けることができます `vserver quota policy rename`。

   > コマンドを使用して新しいポリシーを作成することもできます `volume quota policy create`。

2. コマンドを使用し `volume quota policy rule create`て、SVM上の各ボリュームに次のクォータルールの_any_ofを作成します。
   - すべてのユーザに対するデフォルトのクォータルール
   - 特定のユーザに対する明示的クォータルール
   - すべてのグループに対するデフォルトのクォータルール
   - 特定のグループに対する明示的クォータルール
   - すべての qtree に対するデフォルトのクォータルール
   - 特定の qtree に対する明示的クォータルール
3. コマンドを使用し `volume quota policy rule show`て、クォータルールが正しく設定されていることを確認します。
4. 新しいポリシーを使用する場合は、コマンドを使用し `vserver modify`て新しいポリシーをSVMに割り当てます。
5. コマンドを使用し `volume quota on`て、SVM上の各ボリュームでクォータを初期化します。

   初期化プロセスは、次の方法で監視できます。
   - コマンドを使用する場合は `volume quota on`、パラメータを追加してフォアグラウンドのジョブでクォータを実行できます `-foreground`。（デフォルトでは、このジョブはバックグラウンドで実行されます）。

     バックグラウンドでジョブが実行される場合は、コマンドを使用して進捗状況を監視できます `job show`。
   - コマンドを使用すると、クォータの初期化のステータスを監視できます `volume quota show`。
6. コマンドを使用し `volume quota show -instance`て、初期化に失敗したクォータルールなどの初期化エラーを確認します。
7. コマンドを使用し `volume quota report`てクォータレポートを表示し、適用クォータが想定どおりであることを確認します。

関連情報

- "vserver show"
- "vserver modify"
- "ジョブの表示"
- "ボリュームクォータ"

クォータ制限を変更またはサイズ変更する

影響を受けるすべてのボリューム上のクォータを変更またはサイズ変更できます。これは、それらのボリューム上のクォータを再初期化するよりも高速です。

タスクの内容

クォータが適用されているStorage Virtual Machine（SVM、旧Vserver）があり、既存のクォータのサイズ制限を変更するか、すでに派生クォータが存在するターゲットに対してクォータを追加または削除する。

手順

1. コマンドでパラメータを指定し `-instance`て、 `vserver show`SVMに現在割り当てられているポリシーの名前を確認します。
2. 次のいずれかの操作を実行してクォータルールを変更します。
   - コマンドを使用して `volume quota policy rule modify`、既存のクォータルールのディスク制限またはファイル制限を変更します。
   - コマンドを使用し `volume quota policy rule create`て、現在派生クォータが存在するターゲット（ユーザ、グループ、またはqtree）に対する明示的クォータルールを作成します。
   - コマンドを使用して `volume quota policy rule delete`、デフォルトクォータを持つターゲット（ユーザ、グループ、またはqtree）に対する明示的クォータルールを削除します。
3. コマンドを使用し `volume quota policy rule show`て、クォータルールが正しく設定されていることを確認します。
4. クォータを変更した各ボリュームでコマンドを使用し `volume quota resize`て、各ボリュームで変更をアクティブ化します。

   サイズ変更プロセスは、次のいずれかの方法で監視できます。

   - コマンドを使用する場合 `volume quota resize`は、パラメータを追加してサイズ変更ジョブをフォアグラウンドで実行できます `-foreground`。（デフォルトでは、このジョブはバックグラウンドで実行されます）。

     バックグラウンドでジョブが実行される場合は、コマンドを使用して進捗状況を監視できます `job show`。
   - サイズ変更ステータスは、コマンドを使用して監視できます `volume quota show`。
5. コマンドを使用し `volume quota show -instance`て、サイズ変更に失敗したクォータルールなどのサイズ変更エラーがないかどうかを確認します。

   特に ' 派生クォータがまだ存在しないターゲットの明示的クォータを追加した後でクォータのサイズを変更すると発生する "new definition" エラーをチェックします
6. コマンドを使用し `volume quota report`てクォータレポートを表示し、適用クォータが要件を満たしてい

ることを確認します。

関連情報

- "ボリュームクォータポリシールール"
- "ボリュームクォータ"
- "ジョブの表示"

大幅な変更を行ったあとのクォータの再初期化

既存のクォータ定義に大幅な変更を加えたら、影響を受けるすべてのボリュームでクォータを再初期化する必要があります。このような変更の例としては、クォータが適用されていないターゲットに対するクォータの追加または削除があります。

タスクの内容

クォータが適用されているStorage Virtual Machine（SVM）で、クォータの完全な再初期化が必要な変更を行う場合。

手順

1. コマンドでパラメータを指定し `-instance`て、 `vserver show`SVMに現在割り当てられているポリシーの名前を確認します。
2. 次のいずれかの操作を実行してクォータルールを変更します。

状況	そしたら...。
新しいクォータルールを作成する	コマンドを使用する `volume quota policy rule create`
既存のクォータルールの設定を変更する	コマンドを使用する `volume quota policy rule modify`
既存のクォータルールを削除する	コマンドを使用する `volume quota policy rule delete`

3. コマンドを使用し `volume quota policy rule show`て、クォータルールが正しく設定されていることを確認します。
4. クォータを変更した各ボリュームで、クォータをオフにしてからクォータをオンにして、クォータを再初期化します。
   a. 影響を受ける各ボリュームでコマンドを使用して `volume quota off`、そのボリュームのクォータを非アクティブ化します。
   b. 影響を受ける各ボリュームでコマンドを使用して `volume quota on`、そのボリュームでクォータをアクティブ化します。

影響を受ける各ボリュームのクォータは、コマンドの実行直後にアクティブ化しようとするとエラーが発生する可能性があるため、5分ほど待ってから再アクティブ化してください。 `volume quota off`

また、コマンドを実行して、特定のボリュームを含むノードからボリュームのクォータを再初期化することもできます。

初期化プロセスは、次のいずれかの方法で監視できます。

- コマンドを使用する場合は `volume quota on`、パラメータを追加してフォアグラウンドのジョブでクォータを実行できます `-foreground`。（デフォルトでは、このジョブはバックグラウンドで実行されます）。

  バックグラウンドでジョブが実行される場合は、コマンドを使用して進捗状況を監視できます `job show`。

- コマンドを使用すると、クォータの初期化のステータスを監視できます `volume quota show`。

5. コマンドを使用し `volume quota show -instance`て、初期化に失敗したクォータルールなどの初期化エラーを確認します。
6. コマンドを使用し `volume quota report`てクォータレポートを表示し、適用クォータが想定どおりであることを確認します。

関連情報

- "vserver show"
- "ボリュームクォータポリシールール"
- "ボリュームクォータ"
- "ジョブの表示"

クォータルールとクォータポリシーを管理するコマンド

`volume quota policy rule`コマンドを使用してクォータルールを設定し、 `volume quota policy`コマンドと一部の `vserver`コマンドを使用してクォータポリシーを設定できます。必要な作業に応じて、次のコマンドを使用してクォータルールとクォータポリシーを管理します。

次のコマンドは、FlexVolボリュームに対してのみ実行できます。

クォータルールの管理用コマンド

状況	使用するコマンド
新しいクォータルールを作成します。	`volume quota policy rule create`
既存のクォータルールを削除します。	`volume quota policy rule delete`

状況	使用するコマンド
既存のクォータルールを変更します。	`volume quota policy rule modify`
設定されているクォータルールに関する情報を表示する	`volume quota policy rule show`

クォータポリシーの管理用コマンド

状況	使用するコマンド
クォータポリシーとクォータポリシーに含まれるクォータルールを複製する	`volume quota policy copy`
新しい空のクォータポリシーを作成する	`volume quota policy create`
Storage Virtual Machine（SVM）に現在割り当てられていない既存のクォータポリシーを削除する	`volume quota policy delete`
クォータポリシーの名前を変更します。	`volume quota policy rename`
クォータポリシーに関する情報を表示する	`volume quota policy show`
クォータポリシーをSVMに割り当てる	`vserver modify -quota-policy` *`policy_name`*
SVMに割り当てられているクォータポリシーの名前を表示する	`vserver show`

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

関連情報

- "ボリュームクォータポリシー"
- "vserver modify -quota-policy policy_name"
- "vserver show"

ONTAPでクォータをアクティブ化および変更するコマンド

`volume quota`コマンドを使用すると、クォータの状態を変更したり、クォータのメッセージロギングを設定したりできます。必要な処理に応じて、次のコマンドを使用してクォータをアクティブ化および変更できます。

状況	使用するコマンド
クォータをオンにする（ _initialing_them ）	`volume quota on`
既存のクォータのサイズを変更する	`volume quota resize`
クォータをオフにします	`volume quota off`
クォータのメッセージロギングの変更、クォータのオンへの切り替え、クォータのオフへの切り替え、または既存のクォータのサイズ変更を行います	`volume quota modify`

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

関連情報

- "ボリュームクォータ"
- "ボリュームクォータのサイズ変更"
- "ボリュームクォータオフ"
- "ボリュームクォータの変更"

重複排除、データ圧縮、データコンパクションを使用してストレージ効率を向上

重複排除、データ圧縮、データコンパクション、**Storage Efficiency**

重複排除、データ圧縮、データコンパクションを一緒に、または個別に実行して、FlexVol で最適なスペース削減効果を得ることができます。重複排除は、重複するデータブロックを排除します。データ圧縮は、データブロックを圧縮して、必要な物理ストレージの量を削減します。データコンパクションでは、より少ないスペースにより多くのデータが格納され、ストレージ効率が向上します。

インライン重複排除やインライン圧縮などのすべてのインライン ストレージ効率機能は、 AFF ボリュームではデフォルトで有効になっています。

ボリュームで重複排除を有効にする

FlexVol volumeで重複排除を有効にしてストレージ効率を高めることができます。ポストプロセス重複排除はすべてのボリュームで有効にし、インライン重複排除はAFFアグリゲートまたはFlash Poolアグリゲートに配置されたボリュームで有効にすることができます。

他の種類のボリュームでインライン重複排除を有効にする場合は、"NetAppナレッジベース: 非AFF (All Flash FAS) アグリゲートでボリュームのインライン重複排除を有効にする方法" 。

開始する前に

FlexVol volumeの場合、ボリュームおよびアグリゲート内に重複排除メタデータ用の十分な空きスペースがあることを確認しておく必要があります。重複排除メタデータには、アグリゲート内に最小限の空きスペースが必要です。アグリゲート内の重複排除機能が有効なすべてのFlexVolまたはデータコンスティチュエントについて、物理データの合計量の3%に相当します。各FlexVol volumeまたはデータコンスティチュエントには総物理データ量の4%に相当する空きスペースを確保する必要があるため、合計で7%が必要です。

AFFシステムでは、インライン重複排除がデフォルトで有効になっています。

選択肢

- コマンドを使用し `volume efficiency on`て、ポストプロセス重複排除を有効にします。の詳細については `volume efficiency on`、を"ONTAPコマンド リファレンス"参照してください。

  次のコマンドは、ボリュームVolAでポストプロセス重複排除を有効にします。

  ```
  volume efficiency on -vserver vs1 -volume VolA
  ```

- コマンドのあとにオプションをに設定し `true`てコマンドを `-inline-deduplication`実行し `volume efficiency on`、 `volume efficiency modify`ポストプロセス重複排除とインライン重複排除の両方を有効にします。の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

  次のコマンドは、ボリュームVolAでポストプロセス重複排除とインライン重複排除の両方を有効にします。

  ```
  volume efficiency on -vserver vs1 -volume VolA

  volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
  ```

- コマンドを実行し、 `volume efficiency modify`オプションをに、オプションをに設定し `true`てコマンドを `-inline-deduplication`実行し `volume efficiency on`、 `-policy`オプションをに設定し `inline-only`てインライン重複排除のみを有効にします。

  次のコマンドは、ボリュームVolAでインライン重複排除のみを有効にします。

  ```
  volume efficiency on -vserver vs1 -volume VolA

  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline
  -dedupe true
  ```

終了後

ボリューム効率化の設定を表示して、設定が変更されたことを確認します。
`volume efficiency show -instance`

の詳細については `volume efficiency show -instance`、を"ONTAPコマンド リファレンス"参照してください。

ボリュームの重複排除を無効にする

ポストプロセス重複排除とインライン重複排除は、ボリュームで個別に無効にすることができます。

開始する前に

ボリューム上で現在アクティブになっているボリューム効率化処理を停止します。 `volume efficiency stop`

の詳細については `volume efficiency stop`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

ボリュームでデータ圧縮が有効になっている場合は、コマンドを実行して `volume efficiency off`データ圧縮を無効にします。の詳細については `volume efficiency off`、を"ONTAPコマンド リファレンス"参照してください。

選択肢

- コマンドを使用し `volume efficiency off`て、ポストプロセス重複排除とインライン重複排除の両方を無効にします。

  次のコマンドは、ボリュームVolAでポストプロセス重複排除とインライン重複排除の両方を無効にします。

  ```
  volume efficiency off -vserver vs1 -volume VolA
  ```

- オプションをに設定して `inline only`コマンドを `-policy`実行し `volume efficiency modify`、ポストプロセス重複排除を無効にします。ただし、インライン重複排除は有効なままです。

  次のコマンドは、ボリューム VolA でポストプロセス重複排除を無効にします。ただし、インライン重複排除は有効なままになります。

  ```
  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
  ```

- オプションをに設定して `false`コマンドを `-inline-deduplication`実行し、 `volume efficiency modify`インライン重複排除のみを無効にします。

  次のコマンドは、ボリューム VolA でインライン重複排除だけを無効にします。

  ```
  volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
  ```

  の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

AFFシステムでのボリュームレベルの自動バックグラウンド重複排除

ONTAP 9 3以降では、事前定義されたAFFポリシーを使用してボリュームレベルのバックグラウンド重複排除が自動的に実行されるように設定でき `auto`ます。スケジュールを手動で設定する必要はありません。このポリシーは、 `auto`バックグラウンドで継続的な重複排除を実行します。

この `auto`ポリシーは、新しく作成したすべてのボリューム、およびアップグレードしたボリュームのうち、バックグラウンド重複排除の対象として手動で設定されていないボリュームに対して設定されます。 `default`またはその他のポリシーを使用して、この機能を無効にすることができます"ポリシーの変更"。

ボリュームがAFF以外のシステムからAFFシステムに移動した場合、 `auto`デスティネーションノードでポリシーがデフォルトで有効になります。ボリュームがAFFノードからAFF以外のノードに移動した場合、 `auto`

デフォルトではデスティネーションノードのポリシーがポリシーに置き換えられ `inline-only`ます。

AFFでは、ポリシーが設定されているすべてのボリュームが監視さ `auto`れ、削減量が少ないボリュームや頻繁に上書きされるボリュームの優先度が解除されます。優先度が下がったボリュームは、自動バックグラウンド重複排除の対象ではなくなります。優先度が下がったボリュームの変更ロギングは無効になり、ボリューム上のメタデータは切り捨てられます。

advanced権限レベルで使用できるコマンドを使用すると、優先度が下がったボリュームを昇格して、自動バックグラウンド重複排除の対象に戻すことができます `volume efficiency promote`。

の詳細については `volume efficiency promote`、を"ONTAPコマンド リファレンス"参照してください。

AFFシステムでアグリゲートレベルのインライン重複排除を管理します。

アグリゲートレベルの重複排除は、同じアグリゲートに属するボリューム間で重複ブロックを排除します。AFFAFFでは、アグリゲートレベルの重複排除をインラインで実行できます。この機能は、新規に作成されたすべてのボリュームと、ボリュームインライン重複排除が有効になっているすべてのアップグレードボリュームでデフォルトで有効になっています。

タスクの内容

重複排除処理は、データがディスクに書き込まれる前に重複するブロックを排除します。アグリゲートレベルのインライン重複排除の対象となるのは、がに設定され `none`たボリュームだけ `space guarantee`です。これは、 AFF システムのデフォルト設定です。

アグリゲートレベルのインライン重複排除は、ボリューム間インライン重複排除とも呼ばれます。

ステップ

1. AFF システムでアグリゲートレベルのインライン重複排除を管理します。

状況	使用するコマンド
アグリゲートレベルのインライン重複排除を有効にします	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true`
アグリゲートレベルのインライン重複排除を無効にします	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false`
アグリゲートレベルのインライン重複排除のステータスを表示します	`volume efficiency config -volume vol_name`

例

次のコマンドは、アグリゲートレベルのインライン重複排除のステータスを表示します。

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                    vs0
Volume:                                     choke0_wfit_8020_03_0
Schedule:                                   -
Policy:                                     choke_VE_policy
Compression:                                true
Inline Compression:                         true
Inline Dedupe:                              true
Data Compaction:                            true
Cross Volume Inline Deduplication:          false
```

AFFシステムでアグリゲートレベルのバックグラウンド重複排除を管理します。

アグリゲートレベルの重複排除は、同じアグリゲートに属するボリューム間で重複するブロックを排除します。ONTAP 9.3 以降では、 AFF システムでアグリゲートレベルの重複排除をバックグラウンドで実行できます。この機能は、新規に作成したすべてのボリューム、およびボリュームのバックグラウンド重複排除をオンにしてアップグレードしたすべてのボリュームに対してデフォルトで有効になります。

タスクの内容

この処理は、変更ログがある程度いっぱいになった時点で自動的にトリガーされます。スケジュールもポリシーも関連付けられません。

ONTAP 9.4 以降では、 AFF ユーザがアグリゲートレベルの重複排除スキャンを実行して、アグリゲート内のボリューム間で既存データの重複を排除することもできます。オプションを指定してコマンドを `-scan-old-data=true`実行すると、スキャナを起動でき `storage aggregate efficiency cross-volume-dedupe start`ます。

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

重複排除スキャンには時間がかかることがあります。この処理はオフピークの時間帯に実行することを推奨します。

> アグリゲートレベルのバックグラウンド重複排除は、ボリューム間バックグラウンド重複排除とも呼ばれます。

の詳細については `storage aggregate efficiency cross-volume-dedupe start`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. AFF システムでアグリゲートレベルのバックグラウンド重複排除を管理します。

状況	使用するコマンド
アグリゲートレベルのバックグラウンド重複排除を有効にする	`volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe true`
アグリゲートレベルのバックグラウンド重複排除を無効にします	`volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe false`
アグリゲートレベルのバックグラウンド重複排除のステータスを表示します	`aggregate efficiency cross-volume-dedupe show`

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

関連情報

- "volume efficiency modify"
- "aggregate efficiency cross-volume-dedupe show"

ONTAPの温度に敏感なストレージ効率について学ぶ

ONTAP は、ボリュームのデータへのアクセス頻度を評価し、その頻度をそのデータに適用される圧縮度にマッピングすることで、温度に敏感なストレージ効率 (TSSE) の利点を実現します。あまりアクセスされないコールド データは大きなデータ ブロックで圧縮され、頻繁にアクセスされて上書きされるホット データは小さなデータ ブロックで圧縮されるため、プロセスが効率化されます。

TSSE はONTAP 9.8 で導入され、新しく作成されたシンプロビジョニングされたAFFボリュームで自動的に有効になります。Temperature Sensitive Storage Efficiencyは、既存のAFFボリュームと、シンプロビジョニングされた非AFF DPボリュームで有効にできます。

温度に敏感なストレージ効率は、次のプラットフォームには適用されません。

プラットフォーム	**ONTAP**のバージョン
• AFF A1K用 • AFF A90用 • AFF A70用 • FAS90 • FAS70	9.15.1以降
• AFF A50用 • AFF A30用	9.16.1以降

これらのプラットフォームは"CPUまたは専用オフロードプロセッサのストレージ効率"。圧縮は、ホット データまたはコールド データに基づかず、メイン CPU または専用のオフロード プロセッサを使用して実行されます。

> 時間が経つにつれて、ボリューム内で使用されるスペースの量は、8K アダプティブ圧縮と比較して TSSE でより顕著になる可能性があります。この動作は、TSSE と 8K アダプティブ圧縮のアーキテクチャ上の違いにより予想されるものです。

「デフォルト」モードと「効率的」モードの導入

ONTAP 9 .10.1以降では、AFFシステムにのみ_default_and_efficient_volume-levelのStorage Efficiencyモードが導入されています。この2つのモードでは、ファイル圧縮（デフォルト）（新しいAFFボリュームの作成時のデフォルトモード）と、自動アダプティブ圧縮を使用してコールドデータやアクセス頻度の低いデータに対して圧縮による削減効果を高める温度重視のStorage Efficiency（効率的）のどちらかを選択できます。

ONTAP 9 .10.1以降にアップグレードする場合、既存のボリュームには、ボリュームで現在有効になっている圧縮のタイプに基づいてStorage Efficiencyモードが割り当てられます。アップグレードの実行中、圧縮が有効なボリュームにはデフォルトモードが割り当てられ、温度に基づくStorage Efficiencyが有効なボリュームには効率モードが割り当てられます。圧縮が有効になっていない場合、Storage Efficiencyモードは空白のままです。

"温度に基づくストレージ効率化は明示的に設定する必要があります"自動アダプティブ圧縮を有効にするには、ONTAP 9 .10.1を使用します。ただし、AFFプラットフォームでは、データコンパクション、自動重複排除スケジュール、インライン重複排除、ボリューム間インライン重複排除、ボリューム間バックグラウンド重複排除などの他のStorage Efficiency機能が、デフォルトモードと効率モードのどちらでもデフォルトで有効になります。

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

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

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

- ONTAP 9.12.1P4以降
- ONTAP 9.13.1以降

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

既存のボリュームでは、温度に基づくStorage Efficiencyは自動的には有効になりませんが、手動で効率化モードに変更できます。"Storage Efficiencyモードを変更します"

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

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

ONTAP 9 .13.1以降では、温度に左右されるストレージ効率化機能によって、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率がさらに向上します。システムをONTAP 9にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでは、シーケンシャルパッキングが自動的に有効になります。13.1シーケンシャルパッキングを有効にした後は、を実行する必要があります"既存のデータを手動で再パックします"。

Storage Efficiencyの動作は、アクティブな他のストレージ処理または同時に開始された他のストレージ処理の影響を受ける可能性があります。これらの処理がStorage Efficiencyに与える影響を理解しておく必要があります。

ボリュームのストレージ効率化は、ボリュームの移動、SnapMirror関係、FabricPoolボリューム、などの他の処理の影響を受けることがあります"温度に基づくStorage Efficiency（TSSE）"。

FabricPool

`all`データ保護ボリュームでは、データをすぐにコールドとしてマークしてできるだけ早く階層化するために、一般に階層化ポリシーが使用されます。データがコールドになり、階層化されるまでの最短日数を待つ必要はありません。

階層化ポリシーではできるだけ早くデータが階層化されるため、`all`32Kの効率的なアダプティブ圧縮（TSSE）などのバックグラウンドプロセスに依存するストレージ効率化を適用する時間が不足します。8K圧縮などのインラインStorage Efficiency機能が通常どおり適用されます。

次の表に、いずれかの処理を実行した場合のソースボリュームとデスティネーションボリュームの動作を示します。

ソースボリュームの効率化	デスティネーションボリュームのデフォルトの動作			手動でTSSEを有効にしたあとのデフォルトの動作（SnapMirrorの解除後）		
	* Storage Efficiencyタイプ*	新規書き込み	コールドデータ圧縮	* Storage Efficiencyタイプ*	新規書き込み	コールドデータ圧縮
Storage Efficiency機能なし（FASと思われる）	ファイル圧縮	新しく書き込まれたデータに対してインラインでファイル圧縮が試行される	コールドデータ圧縮なし、データはそのまま保持	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮がTSSE形式で試行される	ファイル圧縮データ：N/A *非圧縮データ*：しきい値の日数を経過したあとに32Kの圧縮が試行された新たに書き込まれたデータ：しきい値の日数を経過したあとに32Kの圧縮が試行された
Storage Efficiency機能なし（FASと思われる）	ONTAP 9 .11.1P10またはONTAP 9 .12.1P3を使用したCシリーズプラットフォームでのファイル圧縮	TSSE対応のコールドデータ圧縮機能なし	ファイル圧縮データ：N/A	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮	ファイル圧縮データ：N/A *非圧縮データ*：しきい値の日数を経過したあとに32Kの圧縮が試行された新たに書き込まれたデータ：しきい値の日数を経過したあとに32Kの圧縮が試行された

Storage Efficiency機能なし（FASと思われる）	ONTAP 9 .12.1P4以降またはONTAP 9 .13.1以降を使用するCシリーズプラットフォーム上のTSSE	8Kのインライン圧縮がTSSE形式で試行される	ファイル圧縮データ：N/A *非圧縮データ*：しきい値の日数を経過したあとに32Kの圧縮が試行された新たに書き込まれたデータ：しきい値の日数を経過したあとに32Kの圧縮が試行された	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮がTSSE形式で試行される	ファイル圧縮データ：N/A *非圧縮データ*：しきい値の日数を経過したあとに32Kの圧縮が試行された新たに書き込まれたデータ：しきい値の日数を経過したあとに32Kの圧縮が試行された
ファイル圧縮グループ	ソースと同じ	新しく書き込まれたデータに対してインラインでファイル圧縮が試行される	コールドデータ圧縮なし、データはそのまま保持	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮がTSSE形式で試行される	ファイル圧縮データ：圧縮されていない+非圧縮データ：しきい値の日数に達したあとに32Kの圧縮が試行される+新規に書き込まれたデータ：しきい値の日数に達したあとに32Kの圧縮が試行される
TSSEコールドデータスキャン	ソースボリュームと同じ圧縮アルゴリズムを使用するTSSE（LZOPro → LZOProおよびZSTD → ZSTD）	TSSE形式で8Kのインライン圧縮が試行されました	既存データと新しく書き込まれたデータの両方で、しきい値日数ベースの寒さが満たされた後、LzoProで32Kの圧縮が試行されます。	TSSEが有効。注：LZOProコールドデータスキャンアルゴリズムはZSTDに変更できます。	8Kのインライン圧縮がTSSE形式で試行される	既存データと新規書き込まれたデータの両方が寒さをしきい値日数に達したあとに、32Kの圧縮が試行されます。

ボリューム作成時の**Storage Efficiency**モードの設定

ONTAP 9.10.1 以降では、新しい AFF ボリュームの作成時に Storage Efficiency モードを設定できます。

タスクの内容

新しいAFFボリュームに対するStorage Efficiencyモードは、パラメータを使用して制御できます `-storage-efficiency-mode`。Storage Efficiencyモードは、またはの `efficient`2つのオプションから選択できます `default`。どのStorage Efficiencyモードを選択するかは、ボリュームでパフォーマンスを向上させるかストレージ効率を向上させるかによって異なります。注：このパラメータは `-storage-efficiency-mode`、AFF以外のボリュームやデータ保護ボリュームではサポートされません。

"温度に基づくStorage EfficiencyモードとStorage Efficiencyモードの詳細"です。

手順

このタスクは、ONTAPシステムマネージャまたはONTAP CLIを使用して実行できます。

System Manager

ONTAP 9 .10.1以降では、温度の影響を受けやすいストレージ効率化機能を使用して、System Managerを使用してストレージ効率を向上させることができます。パフォーマンスベースのStorage Efficiencyはデフォルトで有効になります。

1. [ストレージ]>[ボリューム]*をクリックします。
2. Storage Efficiencyを有効または無効にするボリュームを選択し、をクリックします。
3. [編集]>[ボリューム]をクリックし、[Storage Efficiency]*までスクロールします。
4. Enable Higher Storage Efficiency * を選択します。

CLI

効率化モードを使用した新しいボリュームの作成

新しいボリュームの作成時に温度に基づくStorage Efficiencyモードを設定するには、パラメータをに指定し `efficient`ます `-storage-efficiency-mode`。

1. 効率化モードを有効にして新しいボリュームを作成します。

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode efficient
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1
-storage-efficiency-mode efficient -size 10g
```

パフォーマンスモードを使用した新しいボリュームの作成

パフォーマンスモードは、Storage Efficiencyを使用して新しいAFFを作成するとデフォルトで設定されます。必須ではありませんが、新しいAFFボリュームを作成するときにパラメータに値を `-storage-efficiency-mode`指定することもできます `default`。

1. パフォーマンスStorage Efficiencyモード「default」を使用して新しいボリュームを作成します。

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode default

volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage
-efficiency-mode default -size 10g
```

ボリュームの非アクティブデータ圧縮しきい値を**ONTAP**で変更する

ONTAPがコールドデータスキャンを実行する頻度を変更するには、温度の影響を受けやすいStorage Efficiencyを使用してボリュームのコールドしきい値を変更します。

開始する前に

クラスタ管理者またはSVM管理者であり、ONTAP CLIのadvanced権限レベルを使用する必要があります。

タスクの内容

寒さのしきい値は1～60日です。デフォルトのしきい値は14日です。

手順

1. 権限レベルを設定します。

   ```
   set -privilege advanced
   ```

2. ボリュームのアクセス頻度が低いデータの圧縮を変更します。

   ```
   volume efficiency inactive-data-compression modify -vserver <vserver_name>
   -volume <volume_name> -threshold-days <integer>
   ```

の詳細については `volume efficiency inactive-data-compression modify`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化モードを確認

AFFに対してコマンドを使用すると、効率化が設定されているかどうかを確認したり、現在の効率化モードを表示したりできます `volume-efficiency-show`。

ステップ

1. ボリュームの効率化モードを確認します。

   ```
   volume efficiency show -vserver <vserver name> -volume <volume name> -fields
   storage-efficiency-mode
   ```

の詳細については `volume efficiency show`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化モードの変更

ONTAP 9 .10.1以降では、ボリュームレベルのStorage Efficiencyモード_DEFAULT_AND_Efficient_がAFFシステムでのみサポートされます。これらのモードでは、新しいAFFボリュームを作成する際のデフォルトモードであるファイル圧縮（デフォルト）と、温度に基づくストレージ効率化（効率的）のどちらかを選択できます。`volume efficiency modify`コマンドを使用して、AFFのStorage Efficiencyモード `default`をからに変更できます `efficient`。ボリューム効率化がまだ設定されていない場合は、効率化モードを設定できます。

手順

1. ボリューム効率化モードを変更します。

   ```
   volume efficiency modify -vserver <vserver name> -volume <volume name>
   -storage-efficiency-mode <default|efficient>
   ```

の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

温度の影響を受けやすい**Storage Efficiency**の有無にかかわらず、ボリュームのフットプリント削減量を表示

ONTAPのリリースに応じて、各ボリュームでの物理的なスペース削減量を表示できます。これは、管理プロセスの有効性を評価するため、またはキャパシティプランニングの一環として実行できます。

タスクの内容

ONTAP 9 .11.1以降では、コマンドを使用して `volume show-footprint`、Temperature-Sensitive Storage Efficiency（TSSE）が有効になっているボリュームでの物理的なフットプリントによる削減量を表示できます。TSSE 13.1以降でONTAP 9は、同じコマンドを使用して、TSSEが有効になっていないボリュームでの物理的なフットプリントによる削減量を表示できます。

手順

1. ボリュームのフットプリントによる削減量を表示します。

```
volume show-footprint
```

TSSEが有効な場合の出力例

```
      Vserver : vs0
      Volume  : vol_tsse_75_per_compress

      Feature                                     Used       Used%
      --------------------------------          ----------    -----
      Volume Data Footprint                       10.15GB      13%
      Volume Guarantee                                0B       0%
      Flexible Volume Metadata                    64.25MB       0%
      Delayed Frees                               235.0MB       0%
      File Operation Metadata                         4KB       0%

      Total Footprint                             10.45GB      13%

      Footprint Data Reduction                     6.85GB       9%
           Auto Adaptive Compression               6.85GB       9%
      Effective Total Footprint                    3.59GB       5%
```

TSSEが有効でない場合の出力例

```
      Vserver : vs0
      Volume  : vol_file_cg_75_per_compress

      Feature                                        Used       Used%
      --------------------------------           ----------     -----
      Volume Data Footprint                           5.19GB        7%
      Volume Guarantee                                   0B        0%
      Flexible Volume Metadata                       32.12MB        0%
      Delayed Frees                                  90.17MB        0%
      File Operation Metadata                            4KB        0%

      Total Footprint                                 5.31GB        7%

      Footprint Data Reduction                        1.05GB        1%
           Data Compaction                            1.05GB        1%
      Effective Total Footprint                       4.26GB        5%
```

関連情報

- "ボリューム作成時のStorage Efficiencyモードの設定"

ボリュームでデータ圧縮を有効にする

コマンドを使用すると、FlexVol volumeでデータ圧縮を有効にしてスペースを削減できます `volume efficiency modify`。デフォルトの圧縮形式を使用しない場合は、ボリュームに圧縮形式を割り当てることもできます。の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

ボリュームで重複排除を有効にしておく必要があります。

- 重複排除は有効にさえなっていれば、実行されている必要はありません。
- AFFプラットフォーム内のボリューム上の既存のデータは、圧縮スキャナを使用して圧縮する必要があります。

"ボリュームでの重複排除の有効化"

タスクの内容

- HDDアグリゲートとFlash Poolアグリゲートでは、ボリュームに対してインライン圧縮とポストプロセス圧縮の両方を有効にすることも、ポストプロセス圧縮のみを有効にすることもできます。

  両方を有効にする場合は、ポストプロセス圧縮を有効にしてからインライン圧縮を有効にする必要があります。

- AFFプラットフォームでは、インライン圧縮のみがサポートされます。

ボリュームのインライン圧縮を有効にする前にポストプロセス圧縮を有効にしておく必要があります。ただし、AFFプラットフォームではポストプロセス圧縮がサポートされないため、ボリュームではポストプロセス圧縮は実行されず、ポストプロセス圧縮がスキップされたことを通知するEMSメッセージが生成されます。

- ONTAP 9では、温度に基づくストレージ効率化が導入されています。8.この機能を使用すると、データがホットかコールドかに応じてストレージ効率が適用されます。コールドデータの場合は大容量のデータブロックが圧縮され、頻繁に上書きされるホットデータの場合は小さいデータブロックが圧縮されるため、プロセスが効率化されます。新しく作成したシンプロビジョニングAFFでは、温度に基づくStorage Efficiencyが自動的に有効になります。
- 圧縮形式は、アグリゲートのプラットフォームに基づいて自動的に割り当てられます。

プラットフォーム / アグリゲート	圧縮形式
AFF	適応圧縮
Flash Poolアグリゲート	適応圧縮
HDDアクリケト	二次圧縮

選択肢

- コマンドを使用して `volume efficiency modify`、デフォルトの圧縮形式でデータ圧縮を有効にします。

  次のコマンドは、SVM vs1のボリュームVolAでポストプロセス圧縮を有効にします。

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true
  ```

  次のコマンドは、SVM vs1のボリュームVolAでポストプロセス圧縮とインライン圧縮の両方を有効にします。

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true -inline
  -compression true
  ```

- コマンドをadvanced権限レベルで使用して `volume efficiency modify`、特定の圧縮形式でデータ圧縮を有効にします。

  a. コマンドを使用し `set -privilege advanced`て、権限レベルをadvancedに変更します。

  b. コマンドを使用し `volume efficiency modify`て、ボリュームに圧縮形式を割り当てます。

     次のコマンドは、SVM vs1のボリュームVolAでポストプロセス圧縮を有効にして適応圧縮形式を割り当てます。

     ```
     volume efficiency modify -vserver vs1 -volume VolA -compression true
     -compression-type adaptive
     ```

     次のコマンドは、SVM vs1のボリュームVolAでポストプロセス圧縮とインライン圧縮の両方を有効にして、適応圧縮形式を割り当てます。

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
```

```
-compression-type adaptive -inline-compression true
```

a. コマンドを使用し `set -privilege admin`て、権限レベルをadminに変更します。

二次圧縮と適応圧縮の切り替え

データの読み取り量に応じて、二次圧縮と適応圧縮を切り替えることができます。ランダムリードの量が多く、高いパフォーマンスが要求されるシステムには、適応圧縮が適しています。データがシーケンシャルに書き込まれ、圧縮で多くの量を削減することが要求される場合は、二次圧縮が適しています。

タスクの内容

デフォルトの圧縮形式は、使用するアグリゲートとプラットフォームに基づいて選択されます。

手順

1. ボリュームの効率化を無効にします。

   ```
   volume efficiency off
   ```

   たとえば、次のコマンドは、ボリュームvol1の効率化を無効にします。

   ```
   volume efficiency off -vserver vs1 -volume vol1
   ```

2. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

3. 圧縮データを解凍します。

   ```
   volume efficiency undo
   ```

   たとえば、次のコマンドは、ボリュームvol1上の圧縮データを解凍します。

   ```
   volume efficiency undo -vserver vs1 -volume vol1 -compression true
   ```

   圧縮データを格納するための十分なスペースがボリュームにあることを確認する必要があります。

4. admin権限レベルに切り替えます。

   ```
   set -privilege admin
   ```

5. 処理のステータスがアイドルであることを確認します。

   ```
   volume efficiency show
   ```

   たとえば、次のコマンドは、ボリュームvol1に対する効率化処理のステータスを表示します。

   ```
   volume efficiency show -vserver vs1 -volume vol1
   ```

6. ボリュームの効率化を有効にします。

   `volume efficiency on` たとえば、次のコマンドは、ボリュームvol1で効率化を有効にします。

   ```
   volume efficiency on -vserver vs1 -volume vol1
   ```

7. データ圧縮を有効にして、圧縮形式を設定します。

   ```
   volume efficiency modify
   ```

   たとえば、次のコマンドは、ボリュームvol1でデータ圧縮を有効にし、圧縮形式を二次圧縮に設定します。

   ```
   volume efficiency modify -vserver vs1 -volume vol1 -compression true
   -compression-type secondary
   ```

   この手順では、ボリュームで二次圧縮が有効になるだけで、ボリューム上のデータは圧縮されません。

   - AFF システムで既存のデータを圧縮するには、バックグラウンド圧縮スキャナを実行する必要があります。
   - Flash Pool アグリゲートまたは HDD アグリゲートで既存のデータを圧縮するには、バックグラウンド圧縮を実行する必要があります。

8. オプション：インライン圧縮を有効にします。

   ```
   volume efficiency modify
   ```

   たとえば、次のコマンドは、ボリュームvol1でインライン圧縮を有効にします。

   ```
   volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true
   ```

ボリュームのデータ圧縮を無効にする

コマンドを使用して、ボリュームでのデータ圧縮を無効にできます `volume efficiency modify`。の詳細については `volume efficiency modify`、を"ONTAP コマンド リファレンス"参照してください。

タスクの内容

ポストプロセス圧縮を無効にする場合は、まずボリュームのインライン圧縮を無効にする必要があります。

手順

1. ボリューム上で現在アクティブになっているボリューム効率化処理を停止します。

   ```
   volume efficiency stop
   ```

2. データ圧縮を無効にします。

   ```
   volume efficiency modify
   ```

圧縮済みの既存のデータは、ボリューム上で圧縮されたままになります。圧縮されないのは、ボリュームへの新規の書き込みだけです。

例

次のコマンドは、ボリュームVolAでインライン圧縮を無効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

次のコマンドは、ボリューム VolA でポストプロセス圧縮とインライン圧縮の両方を無効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline
-compression false
```

の詳細については `volume efficiency stop`、を"ONTAPコマンド リファレンス"参照してください。

AFFシステムのインラインデータコンパクションを管理します。

AFFシステムでインラインデータコンパクションをボリュームレベルで制御するには、コマンドを使用し `volume efficiency modify`ます。AFF システム上のすべてのボリュームでは、データコンパクションがデフォルトで有効になっています。

開始する前に

データコンパクションを使用するには、ボリュームのスペースギャランティをに設定する必要があり `none`ます。これは AFF システムのデフォルトです。

AFF以外のデータ保護ボリュームのスペースギャランティは、デフォルトでnoneに設定されます。

手順

1. ボリュームのスペースギャランティ設定を確認するには、次の手順を実行します。

   ```
   volume show -vserver vserver_name -volume volume_name -fields space-guarantee
   ```

2. データコンパクションを有効にするには：

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction true
   ```

3. データコンパクションを無効にするには：

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction false
   ```

4. データコンパクションのステータスを表示するには：

   ```
   volume efficiency show -instance
   ```

例

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction
```

```
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data
-compaction false
```

FASシステムのインラインデータコンパクションを有効にする

Flash Pool（ハイブリッド）アグリゲートまたはHDDアグリゲートを使用するFASシステムでは、cluster shellコマンドを使用して、ボリュームレベルでインラインデータコンパクションを有効にできます `volume efficiency`。FASシステムで作成されたボリュームでは、データコンパクションはデフォルトで無効になっています。の詳細については `volume efficiency`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

ボリュームでインラインデータコンパクションを有効にするには、 `-space-guarantee`オプションをに設定する必要があります `none`。HDDアグリゲートのボリュームでデータコンパクションを有効にすると、追加のCPUリソースが使用されます。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

   の詳細については `set`、を"ONTAPコマンド リファレンス"参照してください。

2. 目的のノードのボリュームおよびアグリゲートのデータコンパクションの状態を確認します。

   ```
   volume efficiency show -volume <volume_name>
   ```

   の詳細については `volume efficiency show`、を"ONTAPコマンド リファレンス"参照してください。

3. ボリュームでデータコンパクションを有効にします。

   ```
   volume efficiency modify -volume <volume_name> -data-compaction true
   ```

   の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

   > アグリゲートまたはボリュームのいずれかでデータコンパクションがに設定されている場合 `false` 、コンパクションは失敗します。コンパクションを有効にしても既存のデータに対しては実行されず、システムへの新規の書き込みに対してのみ実行されます。コマンドには、 `volume efficiency start`既存のデータを圧縮する方法の詳細が含まれています。の詳細については `volume efficiency start`、を"ONTAPコマンド リファレンス"参照してください。

4. コンパクションの統計を表示します。

```
volume efficiency show -volume <volume_name>
```

AFFシステムテノインラインノ**Storage Efficiency**ノテフオルトユウコウカ

Storage Efficiency機能は、AFFシステムに新規に作成するすべてのボリュームでデフォルトで有効になります。すべてのインライン ストレージ効率機能は、すべてのAFFシステム上の既存および新しく作成されたすべてのボリュームでデフォルトで有効になっています。

Storage Efficiency 機能には、インライン重複排除、インラインのボリューム間重複排除、インライン圧縮があります。次の表に示すように、 AFF システムではこれらの機能がデフォルトで有効になっています。

AFFボリューム上のデータ圧縮動作はデフォルトで有効になっています。

ボリュームの状態	ストレージ効率化機能がデフォルトで有効		
	インライン重複排除	インラインのボリューム間重複排除	インライン圧縮
クラスタのアップグレード	○	○	○
ONTAP 7-Mode から clustered ONTAP への移行	○	○	○
ボリューム移動	○	○	○
シックプロビジョニングされたボリューム	○	いいえ	○
暗号化されたボリューム	○	いいえ	○

次の例外は、 1 つ以上のインラインの Storage Efficiency 機能に該当します。

- デフォルトのインラインの Storage Efficiency 機能がサポートされるのは、読み書き可能なボリュームだけです。
- 圧縮による削減が設定されたボリュームでは、インライン圧縮は有効になりません。
- ポストプロセスの重複排除が有効になっているボリュームでは、インライン圧縮は有効になりません。
- ボリューム効率化が無効になっているボリュームでは、既存のボリューム効率化ポリシーの設定が上書きされ、インラインのみのポリシーを有効にするように設定されます。

使用 `storage aggregate show-efficiency`システム内のすべてのアグリゲートのストレージ効率に関する情報を表示するコマンド。

`storage aggregate show-efficiency`コマンドには、コマンドオプションを渡すことで呼び出すことができる3つの異なるビューがあります。

詳細はこちら `storage aggregate show-efficiency`の中で"ONTAPコマンド リファレンス" 。

デフォルトビュー

デフォルトビューには、各アグリゲートの総削減率が表示されます。

```
cluster1::> storage aggregate show-efficiency
```

詳細ビュー

コマンドオプションを使用して詳細ビューを表示し `-details`ます。このビューには次の情報が表示されます。

- 各アグリゲートの総削減率
- Snapshotを含まない総削減率。
- 次の効率化テクノロジに対する比率のスプリット（ボリューム重複排除、ボリューム圧縮、Snapshot、クローン、データコンパクション、アグリゲートのインライン重複排除）。

```
cluster1::> storage aggregate show-efficiency -details
```

アドバンスト ビュー

アドバンスト ビューは詳細ビューと似ていますが、使用済みの論理容量と物理容量の詳細がどちらも表示されます。

このコマンドは、advanced権限レベルで実行する必要があります。コマンドを使用してadvanced権限に切り替えます `set -privilege advanced`。

コマンドプロンプトがに変わります `cluster::*>`。

```
cluster1::> set -privilege advanced
```

コマンドオプションを使用して、アドバンストビューを呼び出し `-advanced`ます。

```
cluster1::*> storage aggregate show-efficiency -advanced
```

単一のアグリゲートの削減比率を個別に表示するには、コマンドを実行し `-aggregate *aggregate_name*`ます。このコマンドは、advanced権限レベルだけでなく、adminレベルでも実行できます。

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

の詳細については `set -privilege advanced`、を"ONTAPコマンド リファレンス"参照してください。

効率化処理を実行するボリューム効率化ポリシーを作成します。

ボリューム効率化ポリシーを作成します。

コマンドを使用して、ボリュームに対して重複排除、またはデータ圧縮とそれに続く重複排除を特定の期間実行するボリューム効率化ポリシーを作成し、ジョブのスケジュールを指定できます `volume efficiency policy create`。

開始する前に

コマンドを使用して、cronスケジュールを作成しておく必要があります `job schedule cron create`。cronスケジュールの管理の詳細については、を参照して"システムアドミニストレーションリファレンス"ください。の詳細については `job schedule cron create`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

事前定義されたデフォルトのロールを持つSVM管理者は、重複排除ポリシーを管理できません。ただし、クラスタ管理者は、カスタマイズした任意のロールを使用して、SVM管理者に割り当てられているPrivilegesを変更できます。SVM管理者の権限の詳細については、を参照してください"カンリシヤニンシヨウトRBAC"。

> 重複排除またはデータ圧縮処理は、スケジュールした時間に実行するか、特定の期間を指定したスケジュールを作成するか、しきい値を指定して実行できます。しきい値は、新しいデータがしきい値を超えてから重複排除またはデータ圧縮処理をトリガーします。このしきい値は、ボリューム内で使用されている合計ブロック数に対する割合です。たとえば、ボリュームで使用されているブロックの合計数が50%のときにボリュームのしきい値を20%に設定した場合、ボリュームに書き込まれた新しいデータが10%（使用されているブロックの20%）に達すると、データの重複排除またはデータ圧縮が自動的に実行されます。必要に応じて、コマンド出力から使用されているブロックの総数を確認できます `df`。

手順

1. コマンドを使用し `volume efficiency policy create`て、ボリューム効率化ポリシーを作成します。

例

次のコマンドは、効率化処理を毎日実行するpol1という名前のボリューム効率化ポリシーを作成します。

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

次のコマンドは、しきい値が20%に達したときに効率化処理を実行するpol2という名前のボリューム効率化ポリシーを作成します。

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start
-threshold-percent 20%
```

の詳細については `volume efficiency policy create`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化ポリシーをボリュームに割り当てる

`volume efficiency modify`コマンドを使用して、ボリュームに効率化ポリシーを割り当て、重複排除またはデータ圧縮処理を実行できます。

開始する前に

ボリュームに割り当てる前に、必ずボリュームを割り当てるようにし"ボリューム効率化ポリシーを作成する"てください。

タスクの内容

効率化ポリシーが SnapVault セカンダリボリュームに割り当てられている場合は、ボリューム効率化処理の実行時に考慮される属性はボリューム効率化優先度のみです。ジョブスケジュールは無視され、重複排除処理はSnapVaultセカンダリボリュームに差分更新が行われたときに実行されます。

ステップ

1. コマンドを使用し `volume efficiency modify`て、ボリュームにポリシーを割り当てます。

例

次のコマンドは、という名前のボリューム効率化ポリシーをボリュームに `VolA`割り当て `new_policy`ます。

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化ポリシーを変更します。

コマンドを使用して、ボリューム効率化ポリシーを変更して別の期間で重複排除やデータ圧縮を実行したり、ジョブスケジュールを変更したりできます `volume efficiency policy modify`。の詳細については `volume efficiency policy modify`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用し `volume efficiency policy modify`て、ボリューム効率化ポリシーを変更します。

例

次のコマンドは、policy1という名前のボリューム効率化ポリシーを変更して、1時間ごとに実行するようにします。

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

次のコマンドは、pol2という名前のボリューム効率化ポリシーをしきい値30%に変更します。

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start
-threshold-percent 30%
```

ONTAPのボリューム効率化ポリシーを表示する

名前、スケジュール、期間、説明を含むボリューム効率化ポリシーを表示できます。

タスクの内容

コマンドは、 `volume efficiency policy show`ボリューム効率化ポリシーを表示します。クラスタ内でコマンドを実行した場合、クラスタを対象としたポリシーは表示されません。ただし、SVMコンテキストでは、クラスタを対象としたポリシーを表示できます。の詳細については `volume efficiency policy show`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用して `volume efficiency policy show`、ボリューム効率化ポリシーに関する情報を表示します。

   出力される内容は指定するパラメータによって異なります。の詳細については `volume efficiency policy show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドを実行すると、SVM vs1用に作成されたポリシーに関する情報が表示されます。
`volume efficiency policy show -vserver vs1`

次のコマンドは、期間が10時間に設定されているポリシーを表示します。
`volume efficiency policy show -duration 10`

ボリュームからボリューム効率化ポリシーの関連付けを解除する

ボリュームからボリューム効率化ポリシーの割り当てを解除して、そのボリュームに対してスケジュールされている以降の重複排除またはデータ圧縮処理を中止できます。ボリューム効率化ポリシーの関連付けを解除したら、手動でトリガーする必要があります。

ステップ

1. コマンドを使用し `volume efficiency modify`て、ボリュームからボリューム効率化ポリシーの関連付けを解除します。

例

次のコマンドは、ボリュームVolAからボリューム効率化ポリシーの関連付けを解除します。 `volume efficiency modify -vserver vs1 -volume VolA -policy -`

の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化ポリシーを削除します。

コマンドを使用して、ボリューム効率化ポリシーを削除できます `volume efficiency policy delete`。

開始する前に

削除するポリシーが関連付けられているボリュームがないことを確認しておく必要があります。

inline-only および _default_predefined 効率化ポリシーは削除できません。

ステップ

1. コマンドを使用し `volume efficiency policy delete`て、ボリューム効率化ポリシーを削除します。

例

次のコマンドは、policy1という名前のボリューム効率化ポリシーを削除します。 `volume efficiency policy delete -vserver vs1 -policy policy1`

の詳細については `volume efficiency policy delete`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化処理を手動で管理します。

手動によるボリューム効率化処理の管理の概要

効率化処理を手動で実行することで、ボリュームに対する効率化処理の実行方法を管理できます。

また、次の条件に基づいて効率化処理の実行方法を制御することもできます。

- チェックポイントを使用するかどうか
- 既存データまたは新規データのみに対して効率化処理を実行
- 必要に応じて効率化処理を停止する

コマンドでオプションの値をに `-fields`指定する `schedule`と、ボリュームに割り当てられているスケジュールを表示できます `volume efficiency show`。

の詳細については `volume efficiency show`、を"ONTAPコマンド リファレンス"参照してください。

効率化処理を手動で実行する

ボリュームに対して効率化処理を手動で実行できます。この処理は、効率化処理のスケジュールが適切でない場合に実行できます。

開始する前に

手動で実行する効率化処理に応じて、重複排除またはデータ圧縮と重複排除の両方をボリュームで有効にしておく必要があります。

タスクの内容

この処理は、 `volume efficiency start`コマンドを使用して実行します。温度に基づくStorage Efficiencyをボリュームで有効にすると、最初に重複排除が実行され、続けてデータ圧縮が実行されます。

重複排除は、実行中にシステムリソースを消費するバックグラウンドプロセスです。ボリューム内のデータの変更頻度が高くない場合は、重複排除の実行頻度を低くすることを推奨します。ストレージシステムで同時に複数の重複排除処理が実行されると、システムリソースの消費量が増加します。

ノードあたり、最大8つの重複排除またはデータ圧縮処理を同時に実行できます。これより多くの効率化処理がスケジュール設定されている場合、処理はキューに登録されます。

ONTAP 9 .13.1以降では、温度に基づくストレージ効率化がボリュームで有効になっている場合、既存データに対してvolume efficiencyを実行することで、シーケンシャルパッキングを利用してストレージ効率をさらに向上させることができます。

効率化を手動で実行

手順

1. ボリュームで効率化処理を開始します。 `volume efficiency start`

例

+次のコマンドを使用すると、重複排除のみを手動で開始し、続けて論理圧縮とコンテナ圧縮をボリュームVolAに対して実行できます。

+

```
volume efficiency start -vserver vs1 -volume VolA
```

既存データの再パック

温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームで、ONTAP 9 .13.1で導入されたシーケンシャルデータパッキングを利用するには、既存データを再パックします。このコマンドを使用するには、advanced権限モードにする必要があります。

手順

1. 権限レベルを設定します。 `set -privilege advanced`
2. 既存データの再パック： `volume efficiency inactive-data-compression start -vserver` *`vserver_name`* `-volume` *`volume_name`* `-scan-mode extended_recompression`

例

```
volume efficiency inactive-data-compression start -vserver vs1 -volume
vol1 -scan-mode extended_recompression
```

関連情報

- "既存データに対して効率化処理を手動で実行"

チェックポイントと効率化処理

チェックポイントは、効率化処理の実行プロセスを記録するために内部的に使用されます。何らかの理由（システムの停止、システムの中断、リブート、前回の効率化処理の失敗や停止など）で効率化処理が停止した場合にチェックポイントデータが存在すると、最新のチェックポイントファイルから効率化処理を再開できます。

チェックポイントが作成されます。

- 処理の各段階またはサブ段階
- コマンドの実行時 `sis stop`
- 有効期間が終了したとき

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

い。

停止した効率化処理を再開します。

システムの停止、システムの停止、リブートのために効率化処理が停止した場合は、停止した時点から効率化処理を再開できます。これにより、最初から操作を再開する必要がなくなるため、時間とリソースを節約できます。

タスクの内容

ボリュームで重複排除のみを有効にした場合は、データに対して重複排除が実行されます。ボリュームで重複排除とデータ圧縮の両方を有効にした場合は、データ圧縮が先に実行され、そのあとに重複排除が実行されます。

ボリュームのチェックポイントの詳細は、コマンドを使用して表示できます `volume efficiency show`。の詳細については `volume efficiency show`、を"ONTAPコマンド リファレンス"参照してください。

デフォルトでは、効率化処理はチェックポイントから再開されます。ただし、前回の効率化処理（-scan-old-data'コマンドが実行されるフェーズ）に対応するチェックポイントから24時間以上が経過している場合 `volume efficiency start`、効率化処理は前回のチェックポイントから自動的には再開されません。この場合、効率化処理は最初から開始されます。ただし、前回のスキャン以降にボリュームで重要な変更が行われていないことがわかっている場合は、オプションを使用して強制的に前回のチェックポイントから続行できます `-use-checkpoint`。

手順

1. `volume efficiency start`コマンドにオプションを指定し `-use-checkpoint`て、効率化処理を再開します。

   次のコマンドは、ボリュームVolA上の新しいデータに対して効率化処理を再開します。

   ```
   volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
   ```

   次のコマンドは、ボリュームVolA上の既存データに対して効率化処理を再開します。

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use
   -checkpoint true
   ```

   の詳細については `volume efficiency start`、を"ONTAPコマンド リファレンス"参照してください。

既存データに対して効率化処理を手動で実行する

重複排除、データ圧縮、またはデータコンパクションを有効にする前に、温度の影響を受けないStorage Efficiencyボリュームにあるデータに対して効率化処理を手動で実行できます。これらの処理は、ONTAP 9より前のバージョンのONTAPで実行できます。8.

タスクの内容

この処理は `volume efficiency start`、コマンドで `-scan-old-data`パラメータを指定して実行します。この `-compression` オプションは、温度の影響を受けやすいStorage Efficiencyボリュームでは機能しません `-scan-old-data` 。ONTAP 9.8以降では、温度の影響を受けやすいStorage Efficiencyボリュームの既存データに対して、非アクティブデータ圧縮が自動的に実行されます。

ボリュームで重複排除のみを有効にすると、データに対して重複排除が実行されます。ボリュームで重複排除、データ圧縮、データコンパクションを有効にすると、まずデータ圧縮が実行され、そのあとに重複排除とデータコンパクションが実行されます。

既存データに対してデータ圧縮を実行すると、デフォルトでは、重複排除で共有されているデータブロックとSnapshotでロックされているデータブロックはデータ圧縮処理によってスキップされます。共有ブロックに対してデータ圧縮を実行することを選択した場合、最適化が無効になり、フィンガープリント情報が取得されて再度共有するために使用されます。既存データを圧縮する際には、データ圧縮のデフォルトの動作を変更できます。

ノードあたり最大8つの重複排除、データ圧縮、またはデータコンパクション処理を同時に実行できます。残りの処理はキューに登録されます。

AFFプラットフォームでは、ポストプロセス圧縮は実行されません。この処理がスキップされたことを通知するEMSメッセージが生成されます。

の詳細については `volume efficiency start`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用して `volume efficiency start -scan-old-data`、既存データに対して重複排除、データ圧縮、またはデータコンパクションを手動で実行します。

   次のコマンドは、これらの処理をボリュームVolAの既存データに対して手動で実行します。

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-
   compression | -dedupe | -compaction ] true
   ```

関連情報

- "効率化処理を手動で実行"

スケジュールを使用したボリューム効率化処理の管理

書き込まれた新規データの量に基づいて効率化処理を実行する

効率化処理スケジュールを変更して、前回の効率化処理後にボリュームに書き込まれた新しいブロック数が指定したしきい値を超えたときに重複排除またはデータ圧縮を実行できます。これは、前回の効率化処理が手動で実行されたかスケジュールされていたかに

タスクの内容

この `schedule`オプションをに設定 `auto`すると、スケジュールされた効率化処理は、新しいデータの量が指定した割合を超えたときに実行されます。デフォルトのしきい値は 20% です。このしきい値は、すでに効率化処理によって処理された総ブロック数に対する割合です。

手順

1. しきい値の値を変更するには、オプションを指定してコマンドを `auto@num`使用し `volume efficiency modify`ます。

   `num`は、パーセンテージを指定する2桁の数値です。

例

次のコマンドは、ボリューム VolA のしきい値を 30% に変更します。

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

関連情報

- "スケジュールを使用した効率化処理の実行"
- "volume efficiency modify"

スケジュールを使用して効率化処理を実行します。

ボリュームに対する重複排除またはデータ圧縮処理のスケジュールを変更できます。スケジュールとボリューム効率化ポリシーの設定オプションを同時に指定することはできません。

タスクの内容

この処理は、 `volume efficiency modify`コマンドを使用して実行します。の詳細については `volume efficiency modify`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用して `volume efficiency modify`、ボリュームに対する重複排除またはデータ圧縮処理のスケジュールを変更します。

例

次のコマンドは、 VolA の効率化処理が月曜日から金曜日の午後 11 時に実行されるようにスケジュールを変更します。

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

関連情報

- "書き込まれた新規データの量に応じて効率化処理を実行"

ボリューム効率化処理の監視

効率化処理とステータスの表示

ボリュームで重複排除またはデータ圧縮が有効になっているかどうかを確認できます。また、ボリュームに対する効率化処理のステータス、状態、圧縮形式、および進捗状況を表示することもできます。

使用できるタスクは2つあります。どちらもコマンドを使用し `volume efficiency show`ます。

効率化ステータスの表示

手順

1. ボリュームに対する効率化処理のステータスを表示します。 `volume efficiency show`

   次のコマンドは、適応圧縮形式が割り当てられたボリュームVolAに対する効率化処理のステータスを表示

します。

```
volume efficiency show -instance -vserver vs1 -volume VolA
```

効率化処理がボリュームVolAに対して有効になっていて、処理がアイドルの場合、次のシステム出力が表示されます。

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

  Vserver Name: vs1
   Volume Name: VolA
   Volume Path: /vol/VolA
         State: Enabled
        Status: Idle
      Progress: Idle for 00:03:20
```

ボリュームにシーケンシャルにパックされたデータがあるかどうかを確認する

シーケンシャルパッキングが有効になっているボリュームのリストを表示できます。たとえば、9.13.1より前のONTAPリリースにリバートする必要がある場合などです。このコマンドを使用するには、advanced権限モードにする必要があります。

手順

1. 権限レベルを設定します。 `set -privilege advanced`
2. シーケンシャル パッキングが有効になっているボリュームを表示します。

   ```
   volume efficiency show -extended-auto-adaptive-compression true
   ```

効率化によるスペース削減量の表示

ボリュームで重複排除およびデータ圧縮によって達成されたスペース削減量を表示できます。これは、管理プロセスの有効性を評価するため、またはキャパシティプランニングの一環として実行できます。

タスクの内容

`volume show`ボリュームでのスペース削減量を表示するには、コマンドを使用する必要があります。`Snapshot`でのスペース削減量は、ボリュームで達成されたスペース削減量の計算には含まれません。重複排除を使用しても、ボリュームのクォータに影響しません。クォータは論理レベルで報告され、変更されません。

手順

1. コマンドを使用して `volume show`、重複排除とデータ圧縮を使用してボリュームで達成されたスペース削減を表示します。

例

次のコマンドを使用すると、ボリュームVolAで重複排除およびデータ圧縮を使用して達成されたスペース削減量を表示できます。 `volume show -vserver vs1 -volume VolA`

```
cluster1::> volume show -vserver vs1 -volume VolA

                                  Vserver Name: vs1
                                   Volume Name: VolA

...
            Space Saved by Storage Efficiency: 115812B
       Percentage Saved by Storage Efficiency: 97%
                  Space Saved by Deduplication: 13728B
            Percentage Saved by Deduplication: 81%
                Space Shared by Deduplication: 1028B
                   Space Saved by Compression: 102084B
        Percentage Space Saved by Compression: 97%

...
```

の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

FlexVol volumeの効率性に関する統計の表示

FlexVol volumeに対して実行される効率化処理の詳細を表示できます。これは、管理プロセスの有効性を評価するため、またはキャパシティプランニングの一環として実行できます。

手順

1. コマンドを使用して `volume efficiency stat`、FlexVol volumeに対する効率化処理の統計を表示します。

例

次のコマンドを使用すると、ボリュームVolAに対する効率化処理の統計を表示できます。
`volume efficiency stat -vserver vs1 -volume VolA`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

               Vserver Name: vs1
                Volume Name: VolA
                Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

の詳細については `volume efficiency stat`、を"ONTAPコマンド リファレンス"参照してください。

ボリューム効率化処理を停止します。

重複排除またはポストプロセス圧縮処理を停止できます。

タスクの内容

この処理では、コマンドを使用し `volume efficiency stop`ます。このコマンドではチェックポイントが自動的に生成されます。

手順

1. コマンドを使用して `volume efficiency stop`、アクティブな重複排除またはポストプロセス圧縮処理を停止します。

   オプションを指定する `-all`と、アクティブな効率化処理とキューに登録されている効率化処理が中止されます。

例

次のコマンドは、ボリュームVolAで現在アクティブな重複排除処理またはポストプロセス圧縮処理を停止します。

```
volume efficiency stop -vserver vs1 -volume VolA
```

次のコマンドは、ボリュームVolAのアクティブな重複排除処理またはポストプロセス圧縮処理とキューに登録されている重複排除処理またはポストプロセス圧縮処理を中止します。

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

の詳細については `volume efficiency stop`、を"ONTAPコマンド リファレンス"参照してください。

ボリュームのスペース削減取り消しに関する詳細情報

ボリュームに対する効率化処理によって達成されたスペース削減を取り消すことができます。ただし、反転に対応できる十分なスペースが必要です。

スペース削減の取り消しを計画、実装するのに役立つ関連リソースがいくつか用意されています。

関連情報

- "ONTAP 9での重複排除、圧縮、およびコンパクションによるスペース削減効果の確認方法"
- "ONTAP でのStorage Efficiencyによる削減効果を取り消す方法"

あるSVMから別のSVMにボリュームをリホストする

あるSVMから別のSVMにボリュームをリホストする準備

ボリュームのリホスト処理を使用すると、NASまたはSANボリュームをあるSVMから別のSVMに再割り当てできます。SnapMirrorコピーは必要ありません。具体的なリホスト手順は、使用するクライアントアクセスプロトコルとボリュームのタイプによって異なります。ボリュームのリホストはシステム停止を伴う処理であり、データアクセスとボリューム管理のために実行されます。

ボリュームをあるSVMから別のSVMにリホストするには、次の条件を満たしている必要があります。

- ボリュームはオンラインである必要があります。
- ボリュームプロトコルはSANまたはNASである必要があります。
  - NASプロトコルボリュームの場合、ボリュームをjunction-pathに含めることはできず、アンマウントする必要があります。
- ボリュームがSnapMirror関係にある場合は、関係を削除してから関係情報のみを解放するか、ボリュームをリホストする前に解除する必要があります。
  - ボリュームのリホスト処理後にSnapMirror関係を再同期できます。
- vserverサブタイプはソースとデスティネーションの両方のSVMで同じである必要があります
  - ボリュームは、同じサブタイプのSVM間でのみリホストできます
- FlexCloneまたはFlexCloneの親をボリュームにすることはできません
  - 親ボリュームまたはクローンボリュームをリホストする前にFlexCloneをスプリットする必要がある

SMBボリュームをリホストする

SMBプロトコルを使用してデータを提供するボリュームをリホストできます。リホスト処理後もクライアントが引き続きデータにアクセスできるようにするには、ポリシーと関連するルールを手動で設定する必要があります。

タスクの内容

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームポリシーと関連ルールの再設定が必要になることがあります。
- ソース SVM とデスティネーション SVM の Active Directory ドメインが異なる場合は、ボリューム上のオブジェクトへのアクセスが失われる可能性があります。
- ONTAP 9.8以降では、NetApp Volume Encryption（NVE）を使用するボリュームのリホストがサポートされます。オンボードキーマネージャを使用している場合は、リホスト処理中に暗号化されたメタデータが変更されます。ユーザデータは変更されません。

  ONTAP 9.8以前を使用している場合は、リホスト処理を実行する前にボリュームの暗号化を解除する必要があります。

- ソース SVM にローカルユーザとローカルグループが含まれている場合、ファイルとディレクトリに対して設定された権限（ ACL ）はボリュームのリホスト処理後に無効になります。

  監査ACL（SACL）についても同様です。

- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホストしたボリュームで手動で再設定する必要があります。
  - ボリュームとqtreeのエクスポートポリシー
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service （ QoS ；サービス品質）ポリシー

- Snapshotポリシー
- クォータルール
- ns-switch とネームサービスの設定のエクスポートポリシーとルール
- ユーザ ID とグループ ID

開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム管理処理（ボリュームの移動やLUNの移動など）を実行していないことを確認してください。
- リホストするボリュームへのデータアクセスを停止する必要があります。
- リホストするボリュームのデータアクセスをサポートするようにターゲット SVM の ns-switch とネームサービスを設定する必要があります。
- ソース SVM とデスティネーション SVM の Active Directory ドメインと DNS ドメインが同じであることが必要です。
- ボリュームのユーザ ID とグループ ID をターゲット SVM で使用可能であるか、またはホストするボリュームで変更する必要があります。

ローカルユーザとローカルグループが設定されていて、それらのユーザまたはグループに対して権限が設定されているボリューム上にファイルとディレクトリがある場合、それらの権限は無効になります。

手順

1. ボリュームのリホスト処理が失敗した場合にCIFS共有の情報が失われないように、CIFS共有に関する情報を記録します。
2. 親ボリュームからボリュームをアンマウントします。

   ```
   volume unmount
   ```

3. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

4. デスティネーション SVM でボリュームをリホストします。

   ```
   volume rehost -vserver source_svm -volume vol_name -destination-vserver
   destination_svm
   ```

5. デスティネーションSVMの適切なジャンクションパスにボリュームをマウントします。

   ```
   volume mount
   ```

6. リホストしたボリューム用のCIFS共有を作成します。

   ```
   vserver cifs share create
   ```

7. ソース SVM とデスティネーション SVM で DNS ドメインが異なる場合は、新しいユーザとグループを作成します。

8. 新しいデスティネーション SVM の LIF とリホストしたボリュームへのジャンクションパスで、 CIFS クライアントを更新します。

終了後

ポリシーおよび関連するルールをリホストしたボリュームに手動で再設定する必要があります。

"SMBの設定"

"SMBオヨヒNFSノマルチフロトコルセツテイ"

NFSボリュームをリホストする

NFSプロトコルを使用してデータを提供するボリュームをリホストできます。リホスト処理後もクライアントが引き続きデータにアクセスできるようにするには、ボリュームをSVMのエクスポートポリシーに関連付け、ポリシーと関連ルールを手動で設定する必要があります。

タスクの内容

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームポリシーと関連ルールの再設定が必要になることがあります。
- ONTAP 9.8以降では、NetApp Volume Encryption（NVE）を使用するボリュームのリホストがサポートされます。オンボードキーマネージャを使用している場合は、リホスト処理中に暗号化されたメタデータが変更されます。ユーザデータは変更されません。

  ONTAP 9.8以前を使用している場合は、リホスト処理を実行する前にボリュームの暗号化を解除する必要があります。

- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホストしたボリュームで手動で再設定する必要があります。
  - ボリュームとqtreeのエクスポートポリシー
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service （ QoS ；サービス品質）ポリシー
  - Snapshotポリシー
  - クォータルール
  - ns-switch とネームサービスの設定のエクスポートポリシーとルール
  - ユーザ ID とグループ ID

開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム管理処理（ボリュームの移動やLUNの移動など）を実行していないことを確認してください。
- リホストするボリュームへのデータアクセスを停止する必要があります。
- リホストするボリュームのデータアクセスをサポートするようにターゲット SVM の ns-switch とネーム

サービスを設定する必要があります。

- ボリュームのユーザ ID とグループ ID をターゲット SVM で使用可能であるか、またはホストするボリュームで変更する必要があります。

手順

1. ボリュームのリホスト処理が失敗した場合に NFS ポリシーの情報が失われないように、 NFS エクスポートポリシーに関する情報を記録します。
2. 親ボリュームからボリュームをアンマウントします。

   ```
   volume unmount
   ```

3. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

4. デスティネーション SVM でボリュームをリホストします。

   ```
   volume rehost -vserver source_svm -volume volume_name -destination-vserver
   destination_svm
   ```

   デスティネーション SVM のデフォルトのエクスポートポリシーがリホストしたボリュームに適用されます。

5. エクスポートポリシーを作成します。

   ```
   vserver export-policy create
   ```

6. リホストしたボリュームのエクスポートポリシーをユーザ定義のエクスポートポリシーに更新します。

   ```
   volume modify
   ```

7. デスティネーションSVMの適切なジャンクションパスにボリュームをマウントします。

   ```
   volume mount
   ```

8. デスティネーション SVM で NFS サービスが実行されていることを確認します。
9. リホストしたボリュームへのNFSアクセスを再開します。
10. NFS クライアントのクレデンシャルと LIF の構成を更新して、デスティネーション SVM の LIF を反映させます。

    これは、ボリュームのアクセスパス（LIFとジャンクションパス）が変更されているためです。

終了後

ポリシーおよび関連するルールをリホストしたボリュームに手動で再設定する必要があります。詳細については、を参照してください "NFSの設定" 。

SANボリュームをリホストする

マッピングされたLUNを介してデータを提供するSANボリュームをリホストできます。

デスティネーションSVMでイニシエータグループ（igroup）を再作成したあと、ボリュームのリホスト処理で同じSVMでボリュームを自動的に再マッピングできます。

タスクの内容

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームポリシーと関連ルールの再設定が必要になることがあります。
- ONTAP 9.8以降では、NetApp Volume Encryption（NVE）を使用するボリュームのリホストがサポートされます。オンボードキーマネージャを使用している場合は、リホスト処理中に暗号化されたメタデータが変更されます。ユーザデータは変更されません。

  ONTAP 9.8以前を使用している場合は、リホスト処理を実行する前にボリュームの暗号化を解除する必要があります。

- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホストしたボリュームで手動で再設定する必要があります。
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service （ QoS ；サービス品質）ポリシー
  - Snapshotポリシー
  - ns-switch とネームサービスの設定のエクスポートポリシーとルール
  - ユーザ ID とグループ ID

開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム管理処理（ボリュームの移動やLUNの移動など）を実行していないことを確認してください。
- ボリュームまたはLUNにアクティブなI/Oがないことを確認します。
- デスティネーション SVM に同じ名前でイニシエータが異なる igroup がないことを確認しておく必要があります。

  igroupの名前が同じ場合は、いずれかのSVM（ソースまたはデスティネーション）でigroupの名前を変更しておく必要があります。

- オプションを有効にしておく必要があり `force-unmap-luns`ます。
  - このオプションのデフォルト値 `force-unmap-luns`はです `false`。
  - このオプションをに `true`設定しても、警告メッセージや確認メッセージは表示されません `force-unmap-luns`。

手順

1. ターゲットボリュームの LUN マッピング情報を記録します。

   `lun mapping show volume` *`volume`* `vserver` *`source_svm`*

   これは、ボリュームのリホストが失敗した場合にLUNマッピングに関する情報が失われないようにするた

めの予防的な手順です。

の詳細については `lun mapping show volume`、を"ONTAPコマンド リファレンス"参照してください。

2. ターゲットボリュームに関連付けられているigroupを削除します。
3. デスティネーションSVMにターゲットボリュームをリホストします。

   `volume rehost -vserver` *`source_svm`* `-volume` *`volume_name`* `-destination-vserver` *`destination_svm`*

4. ターゲットボリュームのLUNを適切なigroupにマッピングします。
   - ボリュームのリホストではターゲットボリュームにLUNが保持されますが、LUNのマッピングは解除されたままです。
   - LUN のマッピングにはデスティネーション SVM のポートセットを使用します。
   - この `auto-remap-luns`オプションをに設定する `true`と、リホスト後にLUNが自動的にマッピングされます。

SnapMirror関係にあるボリュームをリホストする

SnapMirror関係の一部として定義されているボリュームをリホストできます。関係をリホストする前に考慮する必要があるいくつかの問題があります。

タスクの内容

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームポリシーと関連ルールの再設定が必要になることがあります。
- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホストしたボリュームで手動で再設定する必要があります。
  - ボリュームとqtreeのエクスポートポリシー
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service （ QoS ；サービス品質）ポリシー
  - Snapshotポリシー
  - クォータルール
  - ns-switch とネームサービスの設定のエクスポートポリシーとルール
  - ユーザ ID とグループ ID

開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム管理処理（ボリュームの移動やLUNの移動など）を実行していないことを確認してください。
- リホストするボリュームへのデータアクセスを停止する必要があります。
- リホストするボリュームのデータアクセスをサポートするようにターゲット SVM の ns-switch とネーム

サービスを設定する必要があります。

- ボリュームのユーザ ID とグループ ID をターゲット SVM で使用可能であるか、またはホストするボリュームで変更する必要があります。

手順

1. SnapMirror関係のタイプを記録します。

   ```
   snapmirror show
   ```

   これは、ボリュームのリホストが失敗した場合にSnapMirror関係タイプに関する情報が失われないようにするための予防的な手順です。

2. デスティネーションクラスタから、SnapMirror関係を削除します。

   ```
   snapmirror delete
   ```

   SnapMirror関係を解除しないでください。解除しないと、デスティネーションボリュームのデータ保護機能が失われ、リホスト処理後に関係を再確立できなくなります。

3. ソースクラスタから、SnapMirror関係の情報を削除します。

   ```
   snapmirror release -relationship-info-only true
   ```

   パラメータをに `true`設定する `-relationship-info-only`と、Snapshotは削除されずにソースの関係情報が削除されます。

4. ボリュームがマウントされている場合は、アンマウントします。

   ```
   volume unmount -vserver <source_svm> -volume <vol_name>
   ```

5. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

6. デスティネーション SVM でボリュームをリホストします。

   ```
   volume rehost -vserver <source_svm> -volume <vol_name> -destination-vserver
   <destination_svm>
   ```

7. SVMピア関係が存在しない場合は、ソースSVMとデスティネーションSVMの間にSVMピア関係を作成します。

   ```
   vserver peer create
   ```

8. ソースボリュームとデスティネーションボリューム間にSnapMirror関係を作成します。

   ```
   snapmirror create
   ```

   DPボリュームをホストしているSVMからコマンドを実行する必要があり `snapmirror create`ます。リホストしたボリュームは、SnapMirror関係のソースまたはデスティネーションにすることができます。

9. SnapMirror関係を再同期します。

関連情報

- "設定"
- "SnapMirror"
- "ホリユウムノリホスト"
- "ボリュームのアンマウント"
- "vserver peer create"

ONTAPでボリュームのリホストでサポートされない機能

ONTAPには、ボリュームのリホストをサポートしない機能がいくつかあります。リホスト処理を実行する前に、これらの機能について理解しておく必要があります。

次の機能は、ボリュームのリホストではサポートされません。

- SVM DR
- MetroClusterコウセイ

> MetroCluster構成では、ボリュームをFlexCloneボリュームとして別のSVMにクローニングすることもできません。

- SnapLockボリューム
- NetApp Volume Encryption（NVE）ボリューム（ONTAP 9.8より前のバージョン）

  ONTAP 9.8より前のリリースでは、ボリュームをリホストする前に暗号化を解除する必要があります。ボリュームの暗号化キーはSVMキーによって異なります。ボリュームを別のSVMに移動した場合に、ソースまたはデスティネーションのSVMでマルチテナント キーの設定が有効になっていると、ボリュームとSVMのキーが一致しなくなります。

  ONTAP 9.8以降では、NVEを使用してボリュームをリホストできます。

- FlexGroupホリユウム
- クローンボリューム

推奨されるボリュームとファイルまたは**LUN**の設定の組み合わせ

推奨されるボリュームとファイルまたは**LUN**の設定の組み合わせの概要

使用可能な FlexVol の設定とファイルまたは LUN の設定の組み合わせは、使用するアプリケーションと管理要件によって異なります。これらの組み合わせのメリットとコストを理解しておくと、環境に適した構成を判断するのに役立ちます。

推奨されるボリュームと LUN の設定の組み合わせは次のとおりです。

- スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング
- スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリュームプロビジョニング

- スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

これらのいずれかの設定の組み合わせとともに、 LUN で SCSI シンプロビジョニングを使用できます。

スペースリザーブファイルまたはスペースリザーブ **LUN** とシックボリュームプロビジョニング

- 利点 :*
- スペースリザーブファイルでのすべての書き込み処理が保証されます。スペース不足のために失敗することはありません。
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- コストと制限： *
- シックプロビジョニングボリュームをサポートするための十分なスペースをアグリゲートから事前に確保しておく必要があります。
- LUN 作成時に、 LUN の 2 倍のサイズのスペースがボリュームから割り当てられます。

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンボリュームプロビジョニング

- 利点 :*
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- スペースは使用時に初めて割り当てられます。
- 費用および制限 :*
- 書き込み処理は保証されず、ボリュームの空きスペースが不足すると失敗する場合があります。
- アグリゲートの空きスペースを効果的に管理して、空きスペースが不足しないようにする必要があります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニング

- 利点 :*

事前に確保されるスペースがシックボリュームプロビジョニングの場合よりも少なく、ベストエフォートの書き込み保証も提供されます。

- 費用および制限 :*
- このオプションを指定すると、書き込み処理が失敗することがあります。

  このリスクは、ボリュームの空きスペースとデータの揮発性の適切なバランスを維持することで軽減できます。

- Snapshot、FlexCloneファイル、LUNなどのデータ保護オブジェクトは保持されません。
- 重複排除、圧縮、 ODX / コピーオフロードなど、自動で削除できない ONTAP のブロック共有ストレージ効率化機能は使用できません。

ニーズに合ったボリュームと**LUN**の構成を特定する

環境に関するいくつかの基本的な質問に答えることで、環境に最適なFlexVol volumeとLUNの設定を決定できます。

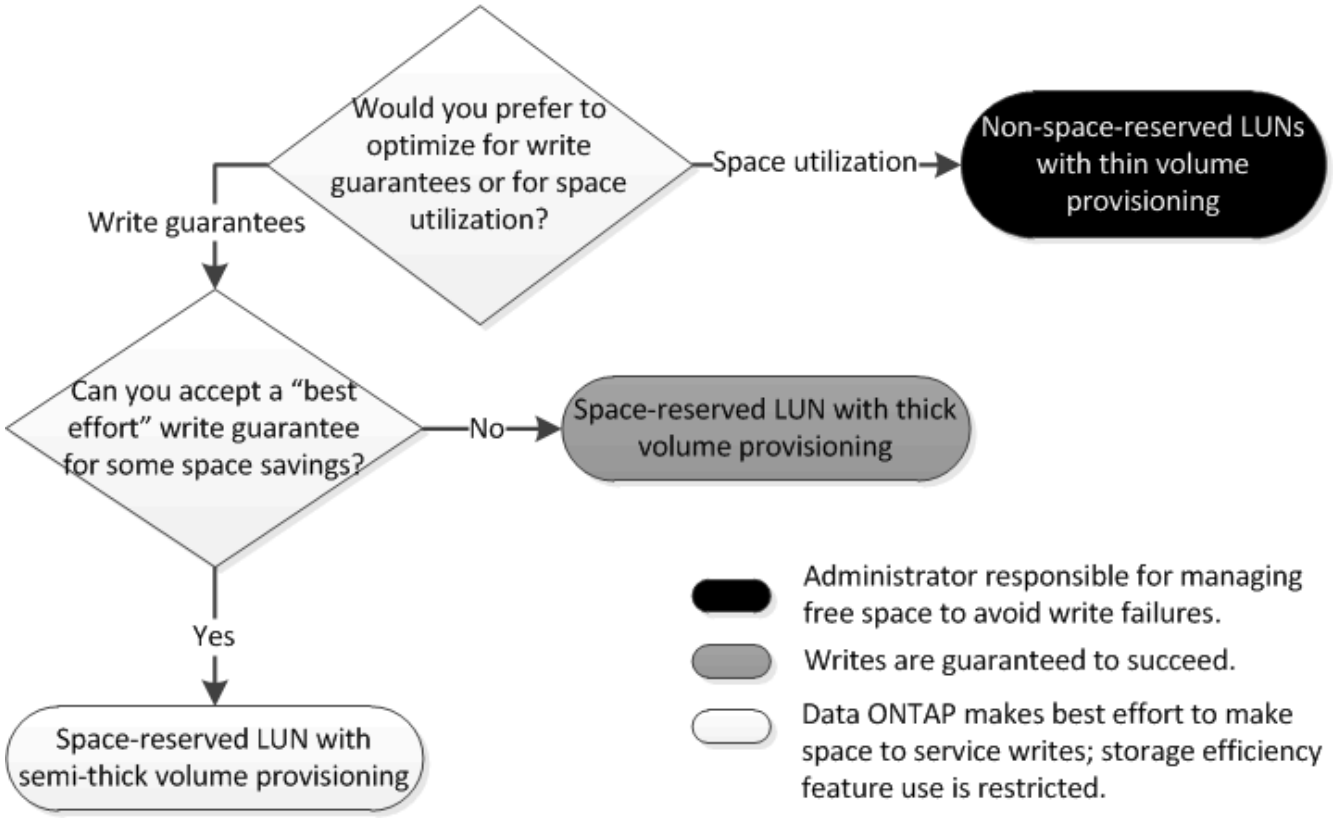
タスクの内容

LUNおよびボリュームの設定を最適化して、ストレージ利用率を最大限に高めたり、書き込みを保証したりすることができます。ストレージ利用要件、および空きスペースを監視して迅速に補充できるかどうかに基づいて、ご使用の環境に適したFlexVol volumeボリュームとLUNボリュームを決定する必要があります。

LUNごとに個別のボリュームを作成する必要はありません。

ステップ

1. 次のデシジョンツリーを使用して、環境に最適なボリュームとLUNの設定の組み合わせを決定してください。



スペースリザーブファイルまたはスペースリザーブ**LUN**とシックプロビジョニングボリュームを組み合わせた場合の構成設定

FlexVol volumeとファイルまたはLUNの設定には、いくつかの設定の組み合わせがあります。シックプロビジョニングボリュームをベースとするこの組み合わせではStorage Efficiencyテクノロジを使用できます。事前に十分なスペースが割り当てられるため、空きスペースを能動的に監視する必要はありません。

シックプロビジョニングを使用するボリュームでスペースリザーブファイルまたはスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	値
保証	ボリューム

音量設定	値
フラクショナルリザーブ	100
Snapshotリザーブ	任意
Snapshotの自動削除	オプション
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは **LUN** の設定	値
スペースリザベーション	有効

関連情報

- "推奨されるボリュームとファイルまたはLUNの設定の組み合わせの概要"

スペースリザーブなしのファイルまたはスペースリザーブなしの**LUN**とシンプロビジョニングボリュームを組み合わせた場合の設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、事前に割り当てられるストレージの量が最小になりますが、スペース不足によるエラーを回避するために空きスペースを能動的に管理する必要があります。

シンプロビジョニングボリュームでスペースリザーブなしのファイルまたはスペースリザーブなしの LUN を設定するには、次の設定が必要です。

音量設定	値
保証	なし
フラクショナルリザーブ	0
Snapshotリザーブ	任意
Snapshotの自動削除	オプション
自動拡張	オプション

ファイルまたは **LUN** の設定	値
スペースリザベーション	無効にする

その他の考慮事項

ボリュームまたはアグリゲートのスペースが不足すると、ファイルまたは LUN への書き込み処理が失敗する場合があります。

ボリュームとアグリゲートの両方の空きスペースを能動的に監視しない場合は、ボリュームの自動拡張を有効にして、ボリュームの最大サイズをアグリゲートのサイズに設定してください。この設定では、アグリゲートの空きスペースを能動的に監視する必要がありますが、ボリュームの空きスペースを監視する必要はありません。

スペースリザーブファイルまたはスペースリザーブ**LUN**とセミシックボリュームプロビジョニングを組み合わせた場合の構成設定

FlexVol volumeとファイルまたはLUNの設定には、いくつかの設定の組み合わせがあります。セミシックボリュームプロビジョニングに基づくこの組み合わせでは、フルプロビジョニングの組み合わせに比べて、事前に割り当てるストレージが少なくて済みます。ただし、ボリュームに使用できる効率化テクノロジに制限が適用されます。この設定の組み合わせでは、上書きがベストエフォートベースで行われます。

セミシックプロビジョニングを使用するボリュームでスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	値
保証	ボリューム
フラクショナルリザーブ	0
Snapshotリザーブ	0
Snapshotの自動削除	オン。この場合、コミットメントレベルを destroy に設定し、削除リストにすべてのオブジェクトを追加し、トリガーを volume に設定し、すべての FlexClone LUN と FlexClone ファイルの自動削除を有効にします。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは **LUN** の設定	値
スペースリザベーション	有効

テクノロジの制限事項

この設定の組み合わせでは、次のボリュームの Storage Efficiency テクノロジを使用できません。

- 圧縮

- 重複排除
- ODX コピーオフロードと FlexClone コピーオフロード
- 自動削除の対象としてマークされていない FlexClone LUN と FlexClone ファイル（アクティブクローン）
- FlexClone サブファイル
- ODX / コピーオフロード

その他の考慮事項

この設定の組み合わせを使用する場合は、次の点を考慮する必要があります。

- そのLUNをサポートするボリュームのスペースが不足すると、保護データ（FlexClone LUN、ファイル、Snapshot）が破棄されます。
- ボリュームの空きスペースが不足すると、書き込み処理がタイムアウトして失敗することがあります。

AFF プラットフォームではデフォルトで圧縮が有効になります。AFF プラットフォームのセミシックプロビジョニングを使用するボリュームに対しては、明示的に圧縮を無効にする必要があります。

関連情報

- "推奨されるボリュームとファイルまたはLUNの設定の組み合わせの概要"

ファイルおよびディレクトリの容量を変更する際の注意事項および考慮事項

ONTAPの**FlexVol**ボリュームに許可されるファイルのデフォルト数と最大数

FlexVolボリュームには、保存できるファイルのデフォルト数と最大数があります。データに多数のファイルが必要な場合は、ボリューム上でユーザーが表示できるファイルの数を最大値まで増やすことができます。続行する前に、制限事項と注意事項を理解しておく必要があります。

ボリュームに含めることができるユーザーに表示されるファイルの数は、ボリュームで使用可能な inode 容量によって決まります。 inode は、ファイルに関する情報を含むデータ構造です。

ONTAP は、ボリュームのサイズに基づいて、新しく作成されたボリュームの使用可能な inode のデフォルト数と最大数を次のように自動的に設定します。

デフォルトのiノード数	最大iノード数
ボリュームサイズ32KBごとに1つ	ボリュームサイズ4KBごとに1つ

ボリュームのサイズが管理者によって手動で、または ONTAP の自動サイズ設定機能によって自動的に増加されると、 ONTAP は、ボリュームのサイズが約 680 GB に達するまで、ボリューム サイズ 32 KB あたり少なくとも 1 つの inode が存在するように、使用可能な inode の数も（必要に応じて）増加します。

ONTAP 9.12.1 以前では、新しいボリュームを作成したり、サイズが 680 GB を超える既存のボリュームのサイズを変更したりしても、inode 容量が自動的に追加されることはありません。ボリュームのサイズに応じてデフォルトの数よりも多くのファイルが必要な場合は、 `volume modify`ボリュームの使用可能な inode の数を最大値まで増やすコマンド。

ONTAP 9.13.1 以降では、新しいボリュームを作成するか、既存のボリュームのサイズを変更すると、ボリュームが 680 GB より大きい場合でも、使用可能な inode のデフォルト数がボリューム スペース 32 KB あたり 1 inode に設定されます。この比率は、ボリュームが絶対的な inode 最大値 2,040,109,451 に達するまで持続します。

使用可能な inode の数を減らすこともできます。これにより、inode に割り当てられるスペースの量は変更されませんが、パブリック inode ファイルが消費できるスペースの最大量は削減されます。inode用にいったん割り当てられたスペースがボリュームに戻されることはありません。したがって、現在割り当てられている inode の数よりも最大 inode の数を減らすことはできません。

詳細情報

- ボリュームのファイルとinodeの使用量を確認する
- "NetAppナレッジベース: FAQ - ONTAP のデフォルトおよび最大ファイル数 (inode)"

FlexVolの最大ディレクトリサイズ

特定のFlexVol volumeのデフォルトの最大ディレクトリサイズを増やすには、 `-maxdir-size`オプションの `volume modify`コマンドを実行できますが、システムのパフォーマンスに影響する可能性があります。参照"NetAppナレッジベース: maxdirsize とは何ですか?"。

FlexVolボリュームのモデル別の最大ディレクトリサイズの詳細については、を参照してください"NetApp Hardware Universe"。

の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

ノードのルートボリュームとルートアグリゲートに関する制限

ノードのルートボリュームとルートアグリゲートに関する制限事項に注意する必要があります。

ノードのルートボリュームには、そのノードの特別なディレクトリとファイルが格納されています。ルートボリュームはルートアグリゲートに含まれています。

ノードのルートボリュームは、工場出荷時またはセットアップソフトウェアによってインストールされたFlexVol volumeです。システムファイル、ログファイル、コアファイル用に予約されています。ディレクトリ名はで `/mroot`、テクニカルサポートからのみシステムシェルからアクセスできます。ノードのルートボリュームの最小サイズは、プラットフォームモデルによって異なります。

- ノードのルートボリュームには次のルールが適用されます。
  - テクニカルサポートから指示がないかぎり、ルートボリュームの構成またはコンテンツを変更しないでください。
  - ユーザデータはルートボリュームに格納しないでください。

    ユーザデータをルートボリュームに格納すると、HAペアのノード間でのストレージのギブバックに時間がかかります。

  - ルートボリュームを別のアグリゲートに移動できます。

"新しいアグリゲートへのルートボリュームの再配置"

- ルートアグリゲートは、ノードのルートボリューム専用です。

  ONTAPでは、ルートアグリゲートに他のボリュームを作成することはできません。

"NetApp Hardware Universe"

新しいアグリゲートへのルートボリュームの再配置

ルートの交換手順では、現在のルートアグリゲートを、システムを停止することなく別のディスクセットに移行します。これは、ディスク交換または予防的メンテナンスプロセスの一環として実行する必要がある場合があります。

タスクの内容

次のシナリオでは、ルートボリュームの場所を新しいアグリゲートに変更できます。

- ルートアグリゲートが希望するディスク上にない場合
- ノードに接続されているディスクの配置を変更する場合
- EOSディスクシェルフを交換する場合

手順

1. ルートアグリゲートを再配置します。

   ```
   system node migrate-root -node node_name -disklist disk_list -raid-type
   raid_type
   ```

   - * -node *

     移行するルートアグリゲートを所有しているノードを指定します。

   - *-disklist *

     新しいルートアグリゲートを作成するディスクのリストを指定します。すべてのディスクはスペアであり、同じノードが所有している必要があります。必要なディスクの最小数は、RAIDタイプによって異なります。

   - * -raid-type *

     ルートアグリゲートのRAIDタイプを指定します。デフォルト値はです `raid-dp`。advanced モードでは、このタイプのみがサポートされます。

2. ジョブの進捗状況を監視します。

   ```
   job show -id jobid -instance
   ```

結果

すべての事前確認に成功すると、ルートボリューム交換ジョブが開始されてコマンドが終了します。

FlexCloneファイルとFlexClone LUNでサポートされる機能

FlexCloneファイルとFlexClone LUNでサポートされる機能

FlexCloneファイルとFlexClone LUNは、重複排除、Snapshot、クォータ、Volume SnapMirrorなど、さまざまなONTAP機能と連携します。

FlexCloneファイルとFlexClone LUNでサポートされる機能は次のとおりです。

- 重複排除
- スナップショット
- アクセス制御リスト
- クォータ
- FlexCloneボリューム
- NDMP
- ボリュームSnapMirror
- コマンド `volume move`
- スペースリザベーション
- HA構成

FlexCloneファイルおよびFlexClone LUNでの重複排除

重複排除が有効なボリューム内にファイルおよび親LUNのFlexCloneファイルまたはFlexClone LUNを作成することで、データブロックの物理ストレージスペースを効率的に使用できます。

FlexClone ファイルおよび FlexClone LUN で使用されるブロック共有メカニズムは、重複排除でも使用されます。ボリュームで重複排除を有効にし、重複排除が有効になったボリュームをクローニングすると、FlexVol で最大限のスペースを節約できます。

> 重複排除が有効なボリュームに対してコマンドを実行する `sis undo`場合、そのボリュームに存在する親ファイルおよび親LUNのFlexCloneファイルおよびFlexClone LUNを作成することはできません。

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

SnapshotとFlexCloneファイルおよびFlexClone LUNとの連携

SnapshotとFlexCloneファイルおよびFlexClone LUNとの間には相乗効果があります。これらのテクノロジを使用する場合は、可能なことと関連する制限事項を把握しておく必要があります。

FlexCloneファイルおよびLUNの作成

既存のSnapshotからFlexCloneファイルまたはFlexClone LUNを作成できます。このコピーは、FlexVol

volumeに含まれる親ファイルおよび親LUNに基づいています。

Snapshot を削除しています

FlexCloneファイルまたはFlexClone LUNの作成元であるSnapshotは、手動で削除できません。Snapshotは、バックグラウンドのブロック共有プロセスが完了するまでロックされたままです。ロックされているスナップショットを削除しようとすると、しばらくしてから操作を再試行するように求めるメッセージが表示されます。この場合は、削除処理を再試行する必要があります。ブロック共有が完了すると、スナップショットを削除できます。

FlexCloneファイルおよび**FlexClone LUN**によるアクセス制御リストの継承

FlexClone ファイルと FlexClone LUN は、親ファイルおよび親 LUN のアクセス制御リストを継承します。

親ファイルにWindows NTストリームが含まれている場合、FlexCloneファイルもストリーム情報を継承します。ただし、6つ以上のストリームを含む親ファイルはクローニングできません。

FlexCloneファイルおよび**FlexClone LUN**でのクォータの処理

クォータを使用する前に、FlexCloneファイルおよびFlexClone LUNでクォータがどのように処理されるかを理解しておく必要があります。

クォータ制限は、 FlexClone ファイルまたは FlexClone LUN の合計論理サイズに適用されます。ブロック共有がクォータを超過する場合でも、クローニング処理でブロック共有が停止されることはありません。

FlexClone ファイルまたは FlexClone LUN を作成した場合、クォータではスペース削減量が認識されません。たとえば、 10GB の親ファイルの FlexClone ファイルを作成した場合、使用される物理スペースは 10GB だけですが、クォータ利用率は 20GB （親は 10GB 、 FlexClone ファイルは 10GB ）と記録されます。

FlexClone ファイルまたは FlexClone LUN を作成するとグループクォータまたはユーザクォータを超過する場合、 FlexVol にクローンのメタデータを保管できるだけの十分なスペースがあれば、クローンの操作は成功します。ただし、そのユーザまたはグループのクォータはオーバーサブスクライブになります。

FlexCloneボリュームと関連する**FlexClone**ファイルおよび**FlexClone LUN**

FlexClone ファイルおよび FlexClone LUN とその親ファイルまたは親 LUN の両方を含む FlexVol ボリュームの、 FlexClone ボリュームを作成できます。

FlexClone ボリューム内に存在する FlexClone ファイルまたは FlexClone LUN とそれらの親ファイルまたは親 LUN は、親 FlexVol ボリューム内と同じ方法で引き続きブロックを共有します。実際、すべての FlexClone エンティティとそれらの親は、基盤となる同じ物理データブロックを共有するため、物理ディスクスペース使用量が最小限に抑えられます。

FlexClone ボリュームを親ボリュームからスプリットすると、 FlexClone ファイルまたは FlexClone LUN とそれらの親ファイルまたは親 LUN は、 FlexClone ボリュームのクローン内のブロックを共有しなくなります。以降は独立したファイルまたは LUN となります。つまり、ボリュームのクローンはスプリット前よりも多くのスペースを使用します。

NDMPによる**FlexClone**ファイルおよび**FlexClone LUN**の処理

NDMP は、論理レベルで FlexClone ファイルおよび FlexClone LUN に影響を与えます。

すべての FlexClone ファイルまたは FlexClone LUN は、独立したファイルまたは LUN としてバックアップされます。

NDMP サービスを使用して FlexClone ファイルまたは FlexClone LUN を含む qtree または FlexVol をバックアップする場合、親エンティティとクローンエンティティの間のブロック共有は維持されず、クローンエンティティは独立したファイルまたは LUN としてテープにバックアップされます。スペースの削減は失われます。したがって、バックアップ先のテープには、拡張された分のデータを格納できるだけの十分なスペースが必要です。リストア時には、すべての FlexClone ファイルおよび FlexClone LUN は独立した物理ファイルおよび LUN としてリストアされます。ボリュームで重複排除を有効にすると、ブロック共有のメリットを復元できます。

FlexVol volumeの既存のSnapshotからFlexCloneファイルとFlexClone LUNを作成している場合は、バックグラウンドで実行されるブロック共有プロセスが完了するまでボリュームをテープにバックアップすることはできません。ブロック共有プロセスの進行中にボリューム上の NDMP を使用すると、しばらくしてから処理を再試行するように求めるメッセージが表示されます。その場合、再試行を繰り返して、ブロック共有が完了した時点でテープバックアップ処理が実行されるようにする必要があります。

Volume SnapMirrorと**FlexClone**ファイルおよび**FlexClone LUN**との相互運用性

Volume SnapMirrorとFlexCloneファイルおよびFlexClone LUNを併用すると、クローンエンティティは一度だけレプリケートされるため、引き続きスペースを節約できます。

FlexVol ボリュームが Volume SnapMirror ソースで、 FlexClone ファイルまたは FlexClone LUN を含んでいる場合、 Volume SnapMirror は共有物理ブロックと少量のメタデータのみを Volume SnapMirror デスティネーションに転送します。デスティネーションでは物理ブロックのコピーが 1 つだけ保存され、このブロックが親エンティティとクローニングされたエンティティとの間で共有されます。したがって、デスティネーションボリュームはソースボリュームの正確なコピーであり、デスティネーションボリューム上のすべてのクローンファイルまたはクローン LUN は同じ物理ブロックを共有します。

スペースリザベーションと**FlexClone**ファイルおよび**FlexClone LUN**との相互運用性

FlexCloneファイルとFlexClone LUNを使用する場合は、スペースリザベーション属性の仕組みを理解しておく必要があります。

デフォルトでは、FlexCloneファイルおよびLUNは親ファイルおよび親LUNのスペースリザベーション属性をそれぞれ継承します。ただし、FlexVol volumeにスペースがない場合は、スペースリザベーションを無効にしてFlexCloneファイルおよびFlexClone LUNを作成できます。これは、それぞれの親の属性が有効になっている場合でも可能です。

親と同じスペースリザベーションが設定されたFlexCloneファイルまたはFlexClone LUNを作成するための十分なスペースがFlexVol volumeにない場合、クローニング処理は失敗します。

HA構成と**FlexClone**ファイルおよび**FlexClone LUN**との連携

FlexClone ファイルと FlexClone LUN の操作は、 HA 構成でサポートされています。

HAペアの場合、テイクオーバー処理またはギブバック処理の実行中は、パートナーにFlexCloneファイルまたはFlexClone LUNを作成することはできません。パートナー上の保留されたブロック共有処理はすべて、テイクオーバー処理またはギブバック処理が完了したあと再開されます。

FlexGroupボリユウムノカンリ

CLIを使用したONTAP FlexGroupボリューム管理の詳細

拡張性とパフォーマンスを確保するために、FlexGroupボリュームをセットアップ、管理、保護することができます。FlexGroupボリュームは、ハイパフォーマンスと自動負荷分散を実現するスケールアウトボリュームです。

FlexGroupボリュームは、次の条件に該当する場合に設定できます。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- SVM管理者Privilegesではなく、クラスタ管理者Privilegesが必要です。

ONTAP 9.5以降では、ONTAP 9.5以降のリリースではサポートされていないInfinite VolumeがFlexGroupボリュームに置き換えられます。

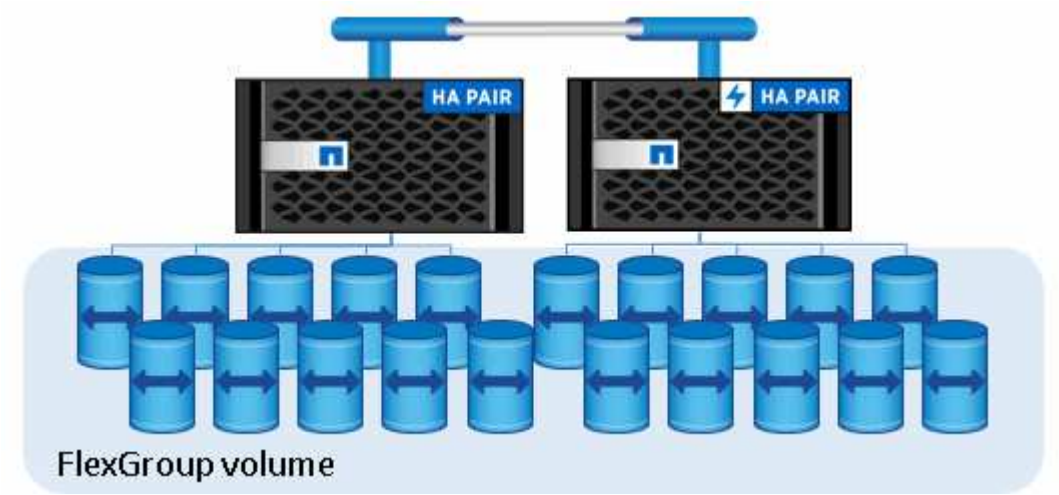
詳細については、"FlexGroupボリュームでサポートされる構成とサポートされない構成"を参照してください。

関連情報

FlexVolの概念はFlexGroupにも適用されます。FlexVolボリュームとONTAPテクノロジの情報については、ONTAPリファレンスライブラリおよびテクニカルレポート（TR）を参照してください。

ONTAP FlexGroupボリュームの詳細

FlexGroupボリュームは、ハイパフォーマンス、自動負荷分散、拡張性を提供するスケールアウトNASコンテナです。FlexGroupボリュームには、自動的かつ透過的にトラフィックを共有する複数のメンバーボリューム（コンスティチュエント）が含まれます。_メンバーボリューム_は、FlexGroupボリュームを構成する基盤となるFlexVolボリュームです。



FlexGroupには次の利点があります。

- 高い拡張性

  メンバーボリュームの数がノードまたはクラスタの制限を超えないかぎり、複数のFlexGroupボリュームを1つのクラスタにプロビジョニングできます。

  ONTAP 9.12.1P2以降では、単一のFlexGroupボリュームの最大容量は60PBで、10ノードのクラスタに4、000億個のファイルを"大容量ボリュームのサポートが有効"格納する場合に使用できます。大容量ボリュームをサポートしない場合、単一のFlexGroupボリュームの最大容量は20PBです。

  > 単一のFlexGroupボリュームの最大容量は60PB（メンバーボリューム200 x 300TB = 60PB）ですが、メンバーボリュームの使用容量が80%を下回る場合（メンバーボリューム200 x 240TB = 48PB）、最適なパフォーマンスが得られます。

- パフォーマンスの向上

  FlexGroupボリュームは、クラスタのリソースを使用して、高スループットと低レイテンシのワークロードを提供できます。

- 管理の簡易化

  FlexGroupボリュームは、FlexVolボリュームと同様の方法で管理できる単一のネームスペースコンテナです。

ONTAP FlexGroupボリュームでサポートされる構成とサポートされない構成

ONTAPの機能のうち、ONTAP 9のFlexGroupでサポートされる機能とサポートされない機能を確認しておく必要があります。

ONTAP 9.16.1以降でサポートされる機能

- 高度な容量分散

ONTAP 9.15.1以降でサポートされる機能

- 自動プロビジョニングの機能拡張

ONTAP 9.14.1以降でサポートされる機能

- Snapshotタギング：コマンドを使用した、FlexGroupボリュームでのSnapshotのSnapshotタグ（SnapMirrorラベルとコメント）の作成、変更、削除がサポートされ `volume snapshot`ます。

ONTAP 9.13.1以降でサポートされる機能

- 自律型ランサムウェア防御（ARP）FlexGroupボリュームの場合：次の機能がサポートされます。
  - FlexGroupの拡張処理：新しいメンバーボリュームは、Autonomous Ransomware Protectionの属性を継承します。
  - FlexVolからFlexGroupへの変換：自律型ランサムウェア対策が有効なFlexVolを変換できます。
  - FlexGroupのリバランシング：自律型ランサムウェア対策は、システムの停止を伴うリバランシング処理と無停止のリバランシング処理でサポートされます。

- 単一のFlexGroupリバランシング処理をスケジュールします。
- SnapMirrorファンアウトFlexGroupボリューム上のSVM DRとの関係。8つのサイトへのファンアウトをサポートします。

ONTAP 9.12.1以降でサポートされる機能

- FlexGroupリバランシング
- SnapLock for SnapVault
- SnapMirrorクラウド
- FabricPool、FlexGroup、SVM DRの連携（ONTAP 9.12.1より前のリリースでは、これらの機能のうち2つを同時に使用できましたが、3つすべてを同時に使用することはできませんでした）。
- 大容量のサポートFlexGroupボリュームのメンバーサイズが最大100TBから最大300TBに拡張されます。

ONTAP 9.11.1以降でサポートされる機能

- SnapLockボリューム

  SnapLockでは、FlexGroupボリュームで次の機能はサポートされません。

  - リーガルホールド
  - イベントベースの保持
  - SnapLock for SnapVault

SnapLockはFlexGroupレベルで設定します。SnapLockはメンバーボリュームレベルでは設定できません。

- クライアントによる非同期ディレクトリの削除

ONTAP 9.10.1以降でサポートされる機能

- SVM DR関係内のFlexVol volumeからFlexGroupボリュームへの変換
- SVM DR FlexCloneによるFlexGroupボリュームのサポート

ONTAP 9.9.1以降でサポートされる機能

- SVMディザスタリカバリ

  SVM DR関係の一部であるFlexGroupボリュームのクローニングはサポートされていません。

- 2つ以上（AからB、AからC）のSnapMirrorファンアウト関係（最大8つのファンアウトレッグ）。

  FlexGroupのSnapMirrorカスケード/ファンアウト関係の作成に関する考慮事項

- 最大2レベル（A→B→C）のSnapMirrorカスケード関係

  FlexGroupのSnapMirrorカスケード/ファンアウト関係の作成に関する考慮事項

ONTAP 9.8以降でサポートされる機能

- FlexGroupのSnapMirrorバックアップまたはUDPデスティネーションからの単一ファイルのリストア
  - 任意のジオメトリのFlexGroupボリュームから任意のジオメトリのFlexGroupボリュームへのリストアが可能
  - 1つのリストア処理でサポートされるファイルは1つだけです。
- 7-Modeシステムから移行したボリュームのFlexGroupボリュームへの変換

  詳細については、"NetAppナレッジベース: 移行したFlexVol をFlexGroupに変換する方法" 。
- NFSv4.2
- ファイルとディレクトリの非同期削除
- ファイルシステム分析（FSA）
- FlexGroupをVMware vSphereデータストアとして使用
- NDMPを使用したテープ バックアップ / リストアで次の機能を追加でサポート
  - NDMPのRestartable Backup Extension（RBE）とSnapshot Management Extension（SSME）
  - 環境変数EXCLUDEおよびMULTI_SUBTREE_NAMESはFlexGroupバックアップをサポート
  - FlexGroupバックアップ用のIGNORE_CTIME_MTIME環境変数の導入
  - 拡張機能 0x2050 ダンプセッションとリストアセッションの一部である NDMP_SNAP_RECOVER メッセージを使用した FlexGroup 内の個々のファイルのリカバリは、アップグレードまたはリバート中に中止されます。

ONTAP 9.7以降でサポートされる機能

- FlexCloneボリューム
- NFSv4とNFSv4.1
- pNFS
- NDMPを使用したテープバックアップおよびリストア

  FlexGroupでのNDMPのサポートについて、次の点に注意する必要があります。
  - 拡張クラス0x2050のNDMP_SNAP_RECOVERメッセージは、FlexGroupボリューム全体のリカバリにのみ使用できます。

    FlexGroupボリューム内の個 々 のファイルはリカバリできません。
  - NDMPのRestartable Backup Extension（RBE）はFlexGroupではサポートされません。
  - FlexGroupボリュームでは、環境変数EXCLUDEおよびMULTI_SUBTREE_NAMESはサポートされません。
  - `ndmpcopy`コマンドは、FlexVolボリュームとFlexGroupボリュームの間のデータ転送に対応しています。

    Data ONTAP 9.7から以前のバージョンにリバートした場合、以前の転送の差分転送情報は保持されないため、リバート後にベースラインコピーを実行する必要があります。

- VMware vStorage APIs for Array Integration（VAAI）
- FlexVol volumeからFlexGroupボリュームへの変換
- FlexGroupボリュームをFlexCache元のボリュームとして使用

ONTAP 9.6以降でサポートされる機能

- 継続的可用性を備えたSMB共有
- "MetroClusterコウセイ"
- FlexGroup volumeコマンドの名前変更(`volume rename`)
- FlexGroup volumeコマンドのサイズの縮小(`volume size`)
- エラスティックサイジング
- NetAppアグリゲート暗号化（NAE）
- Cloud Volumes ONTAP

ONTAP 9.5以降でサポートされる機能

- ODXコピー オフロード
- ストレージレベルのアクセス保護
- SMB共有の変更通知の機能拡張

  変更通知は、プロパティが設定されている親ディレクトリに対する変更と、その親ディレクトリ内のすべてのサブディレクトリに対する変更について送信され `changenotify`ます。

- FabricPool
- クォータの適用
- qtreeの統計
- FlexGroupボリューム内のファイルに対するアダプティブQoS
- FlexCache（キャッシュのみ。ONTAP 9.7ではFlexGroupを元のボリュームとしてサポート）

ONTAP 9.4以降でサポートされる機能

- FPolicy
- ファイルノカンサ
- FlexGroupのスループットの下限（最小QoS）とアダプティブQoS
- FlexGroupボリューム内のファイルに対するスループットの上限（最大QoS）と下限（最小QoS）

  ファイルに関連付けられているQoSポリシーグループを管理するには、コマンドを使用し `volume file modify`ます。

- SnapMirrorの制限を緩和
- SMB 3.xマルチチャネル

ONTAP 9.3以前でサポートされる機能

- ウイルス対策の設定
- SMB共有の変更通知

  通知は、プロパティが設定されている親ディレクトリに対する変更についてのみ送信され `changenotify` ます。親ディレクトリのサブディレクトリに対する変更については送信されません。

- qtree
- スループットの上限（最大QoS）
- SnapMirror関係にあるソースFlexGroupボリュームとデスティネーションFlexGroupボリュームの拡張
- SnapVaultのバックアップとリストア
- 一元化されたデータ保護関係
- 自動拡張オプションと自動縮小オプション
- 取り込みで考慮されるinode数
- ボリューム暗号化
- アグリゲートのインライン重複排除（ボリューム間重複排除）
- NetAppボリューム暗号化（NVE）
- SnapMirrorテクノロジ
- スナップショット
- Digital Advisor
- インラインアダプティブ圧縮
- インライン重複排除
- インラインデータコンパクション
- AFF
- クォータレポート
- NetAppのSnapshotテクノロジ
- SnapRestoreソフトウェア（FlexGroupレベル）
- ハイブリッドアグリゲート
- コンスティチュエントまたはメンバーボリュームの移動
- ポストプロセス重複排除
- NetApp RAID-TECテクノロジ
- アグリゲートごとの整合ポイント
- 同じSVMにあるFlexVolとのFlexGroupの共有

ONTAP 9でサポートされない**FlexGroup**ボリューム構成

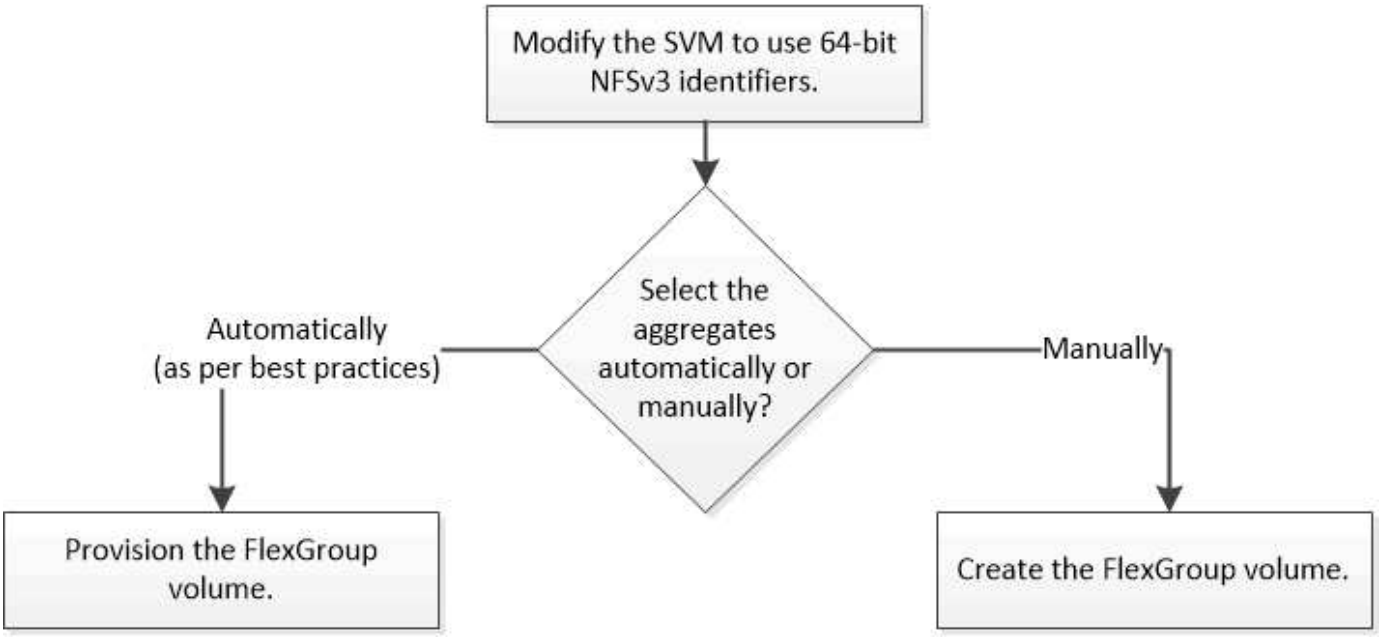
サポートされないプロトコル	サポートされないデータ保護機能	サポートされないその他のONTAP機能

• pNFS（ONTAP 9 .6以前） • SMB 1.0 • SMBの透過的フェイルオーバー（ONTAP 9 .5以前） • SAN	• SnapLockボリューム（ONTAP 9 .10.1以前） • SMTape • SnapMirror同期 • FabricPoolを含むFlexGroupボリュームを使用したSVM DR（ONTAP 9.11.1以前）	• リモートのボリュームシャドウコピーサービス（VSS） • SVMのデータ移動

FlexGroupボリュームのセットアップ

ONTAP FlexGroupボリュームのセットアップワークフロー

最適なパフォーマンスになるようにベストプラクティスに基づいてアグリゲートがONTAP で自動的に選択されるように FlexGroup ボリュームをプロビジョニングするか、アグリゲートを手動で選択してデータアクセスを設定することで FlexGroup ボリュームを作成することができます。



開始する前に

SVMを作成し、SVMで許可されるプロトコルの一覧にNFSとSMBを追加しておく必要があります。

タスクの内容

FlexGroup ボリュームの自動プロビジョニングは、 4 ノード以下のクラスタでのみ実行できます。ノード数がそれより多いクラスタでは、 FlexGroup ボリュームを手動で作成する必要があります。

FlexGroups を備えた ONTAP SVM で 64 ビット NFSv3 識別子を有効にする

FlexGroup ボリュームの大量のファイルをサポートし、ファイル ID の競合を防ぐためには、 FlexGroup ボリュームを作成する必要がある SVM で 64 ビットのファイル ID を有

効にします。

手順

1. advanced権限レベルにログインします。 `set -privilege advanced`
2. 64ビットのNFSv3 FSIDとファイルIDを使用するようにSVMを変更します。 `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
         FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
         result in older client software no longer working with the
volumes
         owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
         "vs0", it is highly recommended that you remount all NFSv3
clients
         connected to it after the command completes.
Do you want to continue? {y|n}: y
```

終了後

すべてのクライアントを再マウントする必要があります。これは、ファイルシステム ID が変わるため、クライアントが NFS 処理を試みたときに stale file handle メッセージが表示される可能性があるためです。

ONTAP FlexGroupボリュームを自動的にプロビジョニングする

FlexGroupボリュームを作成するときに、使用するローカル階層（アグリゲート）を選択してONTAPでFlexGroupを自動的にプロビジョニングするように選択できます。パフォーマンスと容量を最適化するためのベストプラクティスに基づいてローカル階層が選択されます。

開始する前に

クラスタ内の各ノードに少なくとも1つのローカル階層が必要です。

アクセス頻度の低いデータを階層化するFlexGroupボリュームを作成する場合は、各ノードでFabricPoolが有効になっているローカル階層が少なくとも1つ必要です。

タスクの内容

ONTAPは、各ノードの使用可能なスペースが最も多い2つのローカル階層を選択してFlexGroupボリュームを作成します。使用可能なローカル階層が2つない場合、ONTAPはノードごとに1つのローカル階層を選択し

てFlexGroupボリュームを作成します。

ONTAP 9.15.1以降では、FlexGroupボリュームを自動的にプロビジョニングする際に、ONTAPで分散配置（BP）を使用してローカル階層とFlexGroupメンバー（コンスティチュエント）ボリュームのレイアウトを選択します。BPの1つの側面として、保証された（シンプロビジョニングされた）FlexGroupボリュームを作成する際にローカル階層のオーバープロビジョニングを制限する方法があります。FlexGroupボリューム全体のサイズはローカル階層の空きスペースの量によって制限されますが、この制限は「volume」で保証された（シックプロビジョニングされた）FlexGroupボリュームの制限よりも高くなります。REST APIまたはONTAP CLIを使用してFlexGroupボリュームを作成する場合 `auto-provision-as` 、スペース不足が原因でプロビジョニングに失敗することがあります。これを回避するには、FlexGroupボリュームのサイズを小さくするか、"FlexGroupボリュームの作成とローカル階層の手動選択" パラメータを使用し `aggr-list` ます。

手順

1. FlexGroupボリュームをプロビジョニングします。

   ```
   volume create -vserver svm_name -volume fg_vol_name -auto-provision-as
   flexgroup -size fg_size [-encrypt true] [-qos-policy-group
   qos_policy_group_name] [-support-tiering true] [-granular-data advanced]
   ```

   ONTAP 9.16.1以降では、 (`-granular-data advanced`CLIでを有効にすることができます）。ファイルが10GBを超える場合に、複数のFlexGroupメンバーボリュームにデータを書き込むことができます"高度な容量分散"。

   ONTAP 9.5以降では、FabricPoolが有効なローカル階層にFlexGroupボリュームを作成できます。FabricPoolが有効なローカル階層にFlexGroupボリュームを自動的にプロビジョニングするには、パラメータをに `true`設定する必要があります `-support-tiering`。FabricPoolのボリュームギャランティは常にに設定する必要があります `none`。FlexGroupボリュームに対して階層化ポリシーと階層化の最小クーリング期間を指定することもできます。

   "ディスクおよびアグリゲートの管理"

   FlexGroupボリュームにはスループットの上限（最大QoS）を指定できます。これにより、FlexGroupボリュームで消費できるパフォーマンスリソースが制限されます。ONTAP 9.4以降では、FlexGroupボリュームにスループットの下限（最小QoS）とアダプティブQoSを指定できます。

   "パフォーマンス管理"

   FlexGroupボリュームで暗号化を有効にする場合は、パラメータをに `true`設定し `-encrypt`ます。暗号化されたボリュームを作成するには、ボリューム暗号化ライセンスとキー管理ツールをインストールしておく必要があります。

   暗号化はFlexGroupボリュームの作成時に有効にする必要があります。既存のFlexGroupボリュームで暗号化を有効にすることはできません。

   "保存データの暗号化"

   パラメータは `size`、FlexGroupボリュームのサイズ（KB、MB、GB、TB、またはPB）を指定します。

   次の例は、400TBのFlexGroupボリュームをプロビジョニングする方法を示しています。

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

次の例は、スループットの上限を設定するQoSポリシーグループを作成してFlexGroupボリュームに適用する方法を示しています。

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

次の例は、FabricPoolが有効なローカル階層で400TBのFlexGroupボリュームをプロビジョニングする方法を示しています。

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

クラスタ内の各ノードに8個のメンバーボリュームで構成されるFlexGroupボリュームが作成されます。メンバーボリュームは、各ノード上の最も大きい2つのローカル階層に均等に分散されます。

デフォルトでは、AFFシステムの場合を除き、FlexGroupボリュームはスペースギャランティ設定で作成され `volume`ます。AFFシステムの場合、デフォルトではスペースギャランティが設定されてFlexGroupボリュームが作成され `none`ます。

2. ジャンクションパスを使用してFlexGroupボリュームをマウントします。

   ```
   volume mount -vserver vserver_name -volume vol_name -junction-path
   junction_path
   ```

   ```
   cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
   ```

終了後

FlexGroupボリュームはクライアントからマウントする必要があります。

ONTAP 9 .6以前を実行していて、Storage Virtual Machine（SVM）でNFSv3とNFSv4の両方が設定されている場合、クライアントからのFlexGroupボリュームのマウントが失敗することがあります。その場合は、クライアントからFlexGroupボリュームをマウントする際に、NFSバージョンを明示的に指定する必要があります。

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

関連情報

- "QoSポリシーグループの作成"

ONTAP FlexGroupボリュームの作成

FlexGroupボリュームを作成するには、FlexGroupボリュームを作成するローカル階層（アグリゲート）を手動で選択し、各ローカル階層のメンバーボリューム（コンスティチュエント）の数を指定します。

また、ローカル階層を選択し、パフォーマンスと容量が最適化されるようにベストプラクティスに基づいてONTAPでメンバーボリュームの数を設定することで、FlexGroupボリュームをONTAPにすることもでき"自動でプロビジョニング"ます。

タスクの内容

FlexGroupボリュームを作成するためにローカル階層に必要なスペースを確認しておく必要があります。

FlexGroupボリュームを作成するときは、FlexGroupボリュームのパフォーマンスを最大限に高めるために、次のガイドラインを考慮する必要があります。

- FlexGroupボリュームでは、同一のハードウェアシステム上のローカル階層を使用する必要があります。

  使用されているハードウェア システムのモデルが同じであれば、FlexGroupボリューム全体のパフォーマンスを容易に予測できます。注意: C シリーズ r1 および C シリーズ r2 システムは同一のシステムではありません。たとえば、 AFF C80 r1 とAFF C80 r2 は同一ではありません。

- FlexGroupボリュームは、同じディスクタイプおよびRAIDグループ構成を使用するローカル階層で構成されている必要があります。

一貫したパフォーマンスを実現するには、すべてのローカル階層がSSD、HDD、またはオールFlash Pool（ハイブリッド）ローカル階層で構成されていることを確認する必要があります。また、ローカル階層のドライブ数とRAIDグループ数がFlexGroupボリューム全体で同じである必要があります。

- FlexGroupボリュームは、クラスタの一部にまたがることができます。

  FlexGroupボリュームをクラスタ全体にまたがるように設定する必要はありませんが、その場合、使用可能なハードウェアリソースをより有効に活用できます。

- FlexGroupボリュームを作成する際は、FlexGroupボリュームを導入するローカル階層に次の特性を設定することを推奨します。
  - 特にシンプロビジョニングを使用する場合は、複数のローカル階層間でほぼ同じ量の空きスペースを確保する必要があります。
  - FlexGroupボリュームの作成後に、空きスペースの約3%をローカル階層のメタデータ用にリザーブする必要があります。
- FASシステムの場合は、ノードごとに2つのローカル階層を使用することを推奨します。AFFシステムの場合は、FlexGroupボリュームのノードごとに1つのローカル階層を使用する必要があります。
- FlexGroupボリュームごとに少なくとも8個のメンバーボリュームを作成し、FASシステムの場合は2つ以上のローカル階層に、AFFシステムの場合は1つ以上のローカル階層に分散します。
- ONTAP 9 .9.1以降では、2つ以上のFlexGroupのSnapMirrorファンアウト関係（最大8つのファンアウトレッグ）がサポートされます。System Managerでは、SnapMirrorカスケードFlexGroupボリューム関係はサポートされません。
- System Manager を使用してFlexGroupボリュームを作成すると、 ONTAPFlexGroupボリュームの作成に必要なローカル階層が自動的に選択されます。
- ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。

開始する前に

- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

System Manager

System Manager を使用して、FlexGroup ボリュームを作成できます。

手順

1. *ストレージ > ボリューム*に移動して選択 + Add 。
2. *ボリュームの追加*ウィンドウで、ボリュームの名前とサイズを入力し、*その他のオプション*を選択します。
3. *ストレージと最適化*セクションで、*ボリューム データをクラスター全体に分散する (FlexGroup)*を選択します。

   ONTAP 9.8以降を実行していて、QoSを無効にするかカスタムQoSポリシーを選択する場合は、**[その他のオプション]***をクリックし、[ストレージと最適化]で[パフォーマンスサービスレベル]*を選択します。

4. ボリュームの残りの情報を入力し、「保存」を選択します。

CLI

1. FlexGroup ボリュームを作成します。

```
volume create -vserver <svm_name> -volume <flexgroup_name> -aggr
-list aggr1,aggr2,.. -aggr-list-multiplier <constituents_per_aggr>
-size <fg_size> [-encrypt true] [-qos-policy-group
qos_policy_group_name] [-granular-data advanced]
```

   - パラメータは `-aggr-list`、FlexGroupメンバーボリュームに使用するローカル階層のリストを指定します。

     FlexGroupボリューム全体で一貫したパフォーマンスを実現するには、すべてのローカル階層でディスクタイプとRAIDグループ構成を同じにする必要があります。

   - パラメータは `-aggr-list-multiplier`、パラメータで指定した各ローカル階層に作成されるメンバーボリュームの数を指定します `-aggr-list`。

     パラメータのデフォルト値 `-aggr-list-multiplier`は4です。

   - パラメータは `size`、FlexGroupボリュームのサイズ（KB、MB、GB、TB、またはPB）を指定します。
   - ONTAP 9.16.1以降では、（`-granular-data advanced`CLIでを有効にすることができます）。ファイルが10GBを超える場合に、複数のFlexGroupメンバーボリュームにデータを書き込むことができます"高度な容量分散"。
   - ONTAP 9.5以降では、FabricPoolが有効なローカル階層を使用してFlexGroupボリュームを作成できます。

     FabricPool用のFlexGroupボリュームを作成するには、パラメータで指定するすべてのローカル階層 `-aggr-list`でFabricPoolを有効にする必要があります。FabricPoolを使用する場合は、ボリュームギャランティを常にに設定する必要があります `none`。FlexGroupボリュームに

対して階層化ポリシーと階層化の最小クーリング期間を指定することもできます。

ディスクおよびアグリゲートの管理

- ONTAP 9 .4以降では、FlexGroupボリュームにスループットの下限（最小QoS）とアダプティブQoSを指定できます。

"パフォーマンス管理"

- FlexGroupボリュームのスループット上限 (QoS Max) を指定して、 FlexGroupボリュームが消費できるパフォーマンス リソースを制限できます。
- FlexGroupボリュームで暗号化を有効にする場合は、パラメータをに `true`設定し `-encrypt`ます。

  暗号化されたボリュームを作成するには、ボリューム暗号化ライセンスとキー管理ツールをインストールしておく必要があります。

  暗号化はFlexGroupボリュームの作成時に有効にする必要があります。既存のFlexGroupボリュームで暗号化を有効にすることはできません。

"保存データの暗号化"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number
of constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

この例では、FabricPoolのFlexGroupボリュームを作成する場合、すべてのローカル階層（aggr1、aggr2、aggr3）でFabricPoolを有効にする必要があります。ジャンクションパスを使用してFlexGroupボリュームをマウントします。 `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

終了後

FlexGroupボリュームはクライアントからマウントする必要があります。

ONTAP 9 .6以前を実行していて、Storage Virtual Machine（SVM）でNFSv3とNFSv4の両方が設定されている場合、クライアントからのFlexGroupボリュームのマウントが失敗することがあります。その場合は、クライアントからFlexGroupをマウントするときに、NFSのバージョンを明示的に指定する必要があります。

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

関連情報

"NetAppテクニカルレポート4571：『NetApp FlexGroupベストプラクティスおよび実装ガイド』"

FlexGroupボリュームを管理します。

ONTAP FlexGroupボリュームのスペース使用量の監視

FlexGroupボリュームとそのコンスティチュエントを表示し、FlexGroupボリュームで使用されているスペースを監視できます。

タスクの内容

ONTAP 9 .6以降では、エラスティックサイジングがサポートされます。FlexGroupボリュームのコンスティチュエントは、空きスペースがあるFlexGroup内の他のコンスティチュエントを同じ量だけ縮小することで、スペースが不足している場合に自動的に拡張されますONTAP。エラスティックサイジングを使用すると、1つ以上のFlexGroupコンスティチュエントボリュームのスペース不足が原因で発生するスペース不足エラーを回避できます。

ONTAP 9 .9.1以降では、FlexGroupボリュームに対して論理スペースのレポートと適用も使用できます。詳細については、を参照してください "ボリュームの論理スペースのレポートと適用"。

ステップ

1. FlexGroupボリュームとそのコンスティチュエントで使用されているスペースを表示します。 `volume show -vserver vserver_name -volume-style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1          -            online     RW        500GB
207.5GB   56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1__0001    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0002    aggr1        online     RW      31.25GB
12.98GB   56%
vs1       fg1__0003    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0004    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0005    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0006    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0007    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0008    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0009    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0010    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0011    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0012    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0013    aggr3        online     RW      31.25GB
12.95GB   56%
vs1       fg1__0014    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0015    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0016    aggr1        online     RW      31.25GB
13.01GB   56%
16 entries were displayed.
```

使用可能なスペースと使用済みスペースの割合を使用して、FlexGroupボリュームのスペース使用量を監視できます。

ONTAP FlexGroupボリュームのサイズを拡張する

FlexGroupボリュームのサイズを増やすには、 FlexGroupボリュームの既存のすべてのメンバー ボリューム (構成要素) に容量を追加するか、新しいメンバー ボリュームでFlexGroupボリュームを拡張します。 FlexGroupボリュームには 200 を超えるメンバー ボリュームを含めることはできません。

必要に応じて、 FlexGroupボリューム内の個々のボリュームのサイズを増やすこともできます。

開始する前に

アグリゲートに十分なスペースが必要です。

タスクの内容

スペースを追加する場合は、FlexGroupボリューム全体のサイズを増やすことができます。FlexGroupボリュームのサイズを拡張すると、FlexGroupボリュームの既存のメンバーボリュームのサイズが変更されます。

パフォーマンスの向上が必要な場合は、FlexGroupボリュームを拡張できます。FlexGroupボリュームの拡張と新しいメンバーボリュームの追加が必要になる状況は次のとおりです。

- クラスタに新しいノードが追加された。
- 既存のノードに新しいローカル階層（アグリゲート）が作成されています。
- FlexGroupボリュームの既存のメンバーボリュームがハードウェアの最大FlexVolサイズ（有効になっている場合は100TBまたは300TB）に達している"大容量のサポート"ため、メンバーボリュームを追加しないとFlexGroupボリュームのサイズを変更できません。

> FlexGroupボリュームにメンバーを追加するように変更すると、以前に作成されたスナップショットは「部分的」とみなされ、クライアントはFlexGroupボリュームからのみアクセスできるようになります。 `.snapshot`ディレクトリまたは*以前のバージョン*タブ。
>
> スナップショットが「部分的」とみなされる場合、SnapRestore操作では使用できません。ただし、部分的なスナップショットは、個々のファイルを復元するために使用できます。 `.snapshot`ディレクトリまたは*以前のバージョン*タブ。

ONTAP 9.3より前のリリースでは、SnapMirror関係の確立後にFlexGroupボリュームを拡張しないでください。ONTAP 9.3よりも前のリリースでSnapMirror関係の解除後にソースFlexGroupボリュームを拡張した場合は、デスティネーションFlexGroupボリュームへのベースライン転送をもう一度実行する必要があります。ONTAP 9.3以降では、SnapMirror関係にあるFlexGroupボリュームを拡張できます。

手順

1. 必要に応じて、FlexGroupボリュームの容量またはパフォーマンスを増やしてFlexGroupボリュームのサイズを拡張します。

追加する項目	操作
FlexGroupボリュームの容量	FlexGroupボリュームのすべてのメンバー ボリュームのサイズを変更します。 `volume modify -vserver <svm_name> -volume <fg_name> -size <new_size>`

FlexGroupボリュームのパフォーマンス	新しいメンバーボリューム（コンスティチュエント）を追加してFlexGroupボリュームを拡張します。 `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]` パラメータのデフォルト値 `-aggr-list-multiplier`は1です。 を使用してFlexGroupボリュームを拡張する場合"FabricPool"は、すべてのローカル階層（アグリゲート）を同じクラウド階層に接続する必要があります。

既存のアグリゲート（ローカル階層）またはメンバーボリュームが最大容量（それぞれ100/300TBまたは20億個のファイル）に達していない場合は、メンバーボリュームを追加するのではなく、FlexGroupボリュームの全体的なサイズを増やすことを推奨します。

ボリューム拡張は、既存のボリュームサイズまたはファイル数を増やすことができない場合、またはFlexGroupを新しいハードウェアに拡張する場合にのみ使用してください。一貫したパフォーマンスを確保するためには、すべてのノードに同じ数のメンバーボリュームを追加する必要があります。たとえば、既存のFlexGroupボリュームに8個のメンバーボリュームがあり、ノードあたり4個のメンバーボリュームがある場合、ノードあたり2個のメンバーボリュームを追加すると、12個のメンバーボリューム（ノードあたり6個のメンバーボリューム）になります。

新しいノードに新しいメンバーを追加する場合は、ノードあたりのメンバーボリュームの数を既存のノードと同じにするようにしてください。たとえば、既存のFlexGroupボリュームに8個のメンバーボリュームがあり、各ノードに4個のメンバーボリュームがある場合、FlexGroupボリュームを新しいノードに拡張するには、4個のメンバーボリュームを追加する必要があります。その結果、12個のメンバーFlexGroupボリュームになります。

FlexGroupボリュームに新しいメンバーを追加すると、新しい空のメンバーボリュームが優先されるように取り込みのヒューリスティックが変更されます。新しいメンバーボリュームが既存のメンバーボリュームと分散されるまで、新しいデータの取り込みの全体的なシステムパフォーマンスに影響する可能性があります。

例

既存のメンバーボリュームの容量拡張の例

次の例は、FlexGroupボリュームvolXに20TBのスペースを追加する方法を示しています。

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

FlexGroupに16個のメンバーボリュームがある場合、各メンバーボリュームのスペースは1.25TB増加します。

新しいメンバーボリュームの追加によるパフォーマンス向上の例

次の例は、FlexGroupボリュームの基盤となるローカル層（アグリゲート）のそれぞれに2つずつ、合計4つの

メンバーボリュームを追加する方法を示しています。 `fg1` ：

```
cluster1::> volume expand -vserver svm1 -volume fg1 -aggr-list aggr1,aggr2
-aggr-list-multiplier 2
```

新しいメンバーボリュームのサイズは、既存のメンバーボリュームのサイズと同じです。

個々のボリュームのサイズを増やす

FlexGroupボリューム内の個々のメンバーボリュームのサイズを増やす場合は、 `volume resize`指示。

ステップ

1. 単一のFlexGroupメンバー ボリュームのサイズを増やす:

   ```
   volume size -volume <volume_name> -vserver <svm1> -new-size <new_size>
   ```

   次の例では、 FlexGroupメンバー ボリューム FG_0003 のサイズを 3.7 GB に増やします。

   ```
   volume size -volume FG__0003 -vserver svm1 -new-size 3.7GB
   vol size: Volume "svm1:FG__0003" size set to 3.70g.
   ```

ONTAP FlexGroupボリュームのサイズを縮小する

ONTAP 9 .6以降では、FlexGroupボリュームのサイズを現在のサイズよりも小さい値に変更して、ボリュームから未使用スペースを解放できます。FlexGroupボリュームのサイズを縮小すると、すべてのFlexGroupコンスティチュエントのサイズがONTAPによって自動的に変更されます。

ステップ

1. 現在のFlexGroup ボリュームサイズを確認します。「volume size -vserver _vserver_name _-volume_fg_name _」
2. FlexGroupボリュームのサイズを縮小します。 `volume size -vserver` *`vserver_name`* `-volume` *`fg_name new_size`*

   新しいサイズを指定するときは、現在のサイズよりも小さい値を指定するか、マイナス記号（-）を使用してFlexGroupボリュームの現在のサイズが縮小される負の値を指定できます。

   > volumeコマンドに対して自動縮小が有効になっている場合(`volume autosize`）、最小オートサイズはボリュームの新しいサイズに設定されます。

   次の例は、volXという名前のFlexGroupボリュームの現在のボリュームサイズを表示し、ボリュームのサイズを10TBに変更します。

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

次の例は、volXという名前のFlexGroupボリュームの現在のボリュームサイズを表示し、ボリュームのサイズを5TBだけ縮小します。

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

ONTAP FlexGroupボリュームのサイズを自動的に拡張および縮小するように設定する

ONTAP 9 .3以降では、必要なスペースに応じてFlexGroupボリュームを自動的に拡張および縮小するように設定できます。

開始する前に

FlexGroupボリュームはオンラインである必要があります。

タスクの内容

FlexGroupボリュームのオートサイズは、次の2つのモードで実行できます。

- ボリュームのサイズを自動的に拡張する(`grow`モード）

  自動拡張を使用すると、FlexGroupボリュームがスペース不足になるのを防ぐことができます（アグリゲートが追加のスペースを提供できる場合）。ボリュームの最大サイズを設定できます。この拡張は、ボリュームに書き込まれるデータの量に基づいて、現在の使用済みスペースの量と設定されているしきい値に基づいて自動的にトリガーされます。

  デフォルトでは、ボリュームは自動拡張が有効になっているサイズの120%まで拡張できます。ボリュームをそれよりも大きく拡張できるようにする必要がある場合は、それに応じてボリュームの最大サイズを設定する必要があります。

- ボリュームのサイズを自動的に縮小(`grow_shrink`するモード）

  自動縮小では、ボリュームが必要以上に大きくなるのを防ぎ、アグリゲートのスペースを解放して他のボリュームで使用できるようにします。

自動縮小は、変化するスペース需要に対応するために自動拡張と組み合わせてのみ使用でき、単独で使用することはできません。自動縮小を有効にすると、自動拡張と自動縮小の処理が無限に繰り返されるのを防ぐために、ONTAPはボリュームの縮小動作を自動的に管理します。

ボリュームが拡張されると、格納できるファイルの最大数が自動的に増える可能性があります。ボリュームが縮小されても格納できるファイルの最大数は変わらず、ボリュームが縮小前のファイルの最大数に対応するサイズよりも小さくなることはありません。そのため、自動縮小でボリュームを最初のサイズまで縮小できるとは限りません。

手順

1. ボリュームのサイズを自動的に拡張および縮小するように設定します。 `volume autosize -vserver vserver_name -volume vol_name -mode [grow | grow_shrink]`

   ボリュームを拡張または縮小する最大サイズ、最小サイズ、およびしきい値を指定することもできます。

   、70% 使用された場合、最大サイズが 5 TB まで拡張されるように構成されています。

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

ONTAP FlexGroupボリュームからディレクトリを非同期的に削除する

ONTAP 9.8 以降では、Linux および Windows クライアント共有からディレクトリを非同期的に（つまり、バックグラウンドで）削除できます。クラスタ管理者とSVM管理者は、FlexVolとFlexGroupボリュームの両方で非同期削除処理を実行できます。

タスクの内容

高度な権限モードを使用するクラスタ管理者または SVM 管理者である必要があります。

ONTAP 9.8以降では、ONTAP CLIを使用して非同期削除機能を使用できます。ONTAP9.9.1以降では、System Managerを使用してこの機能を使用できます。このプロセスの詳細については、を参照してください"FSAのONTAP分析に基づいて是正措置を講じる"。

ONTAP 9 .11.1以降では、ストレージ管理者がボリュームに対する権限を付与して、NFSクライアントとSMBクライアントによる非同期削除処理を許可できます。詳細については、を参照してください "ディレクトリを非同期で削除するクライアント権限を管理します。"。

使用することができます `volume file async-delete show`進行中の非同期削除ジョブのステータスを確認するコマンドです。ONTAP 9.17.1 以降では、クライアントから発行された非同期削除ジョブのステータスも表示されます。

ディレクトリを非同期的に削除する

System Manager またはONTAP CLI を使用して、ディレクトリを非同期的に削除できます。

System Manager

ONTAP 9.10.1以降	ONTAP 9.9.1の場合
1. ストレージ > ボリューム を選択し、目的のボリューム名を選択します。 2. 個々のボリューム ページで、ファイル システム タブを選択し、エクスプローラー タブを選択します。 3. *エクスプローラー*ビューで、目的のディレクトリを選択します。 4. 削除するには、ファイルまたはフォルダの上にマウスを移動し、削除オプションが表示されます。 一度に削除できるオブジェクトは 1 つだけです。 ディレクトリとファイルを削除しても、新しいストレージ容量の値はすぐには表示されません。	1. Storage > Volumes （ストレージ）を選択します。 2. 目的のボリュームを選択し、* Explorer *を選択します。 3. *エクスプローラー*ビューで、目的のディレクトリを選択します。 4. 削除するには、ファイルまたはフォルダの上にマウスを移動し、削除オプションが表示されます。

CLI

- CLIを使用して非同期削除を実行*

1. advanced権限モードに切り替えます。

   ```
   set -privilege advanced
   ```

2. FlexVolまたはFlexGroupボリューム上のディレクトリを削除します。

   ```
   volume file async-delete start -vserver <SVM_name> -volume <volume_name>
   -path <file_path> -throttle <throttle>
   ```

   最小スロットル値は10、最大スロットル値は100000、デフォルトは5000です。スロットル値が低いほどリソースの使用量が少なくなり、削除速度が遅くなる可能性があります。一方、スロットル値が高いほどリソースの使用量が多くなりますが、削除速度は速くなります。

   次の例は、d1という名前のディレクトリにあるd2という名前のディレクトリを削除します。

   ```
   cluster::*> volume file async-delete start -vserver vs1 -volume
   vol1 -path d1/d2
   ```

3. (オプション) 進行中の非同期削除ジョブのステータスを確認します。

   ```
   volume file async-delete show
   ```

4. ディレクトリが削除されたことを確認します。

   ```
   event log show
   ```

   次の例は、ディレクトリが正常に削除された場合のイベント ログの出力を示しています。

```
cluster::*> event log show

Time                 Node              Severity      Event
-------------------- ---------------- -------------
--------------------------
7/7/2025 09:04:04    cluster-vsim      NOTICE
asyncDelete.message.success: Async delete job on path d1/d2 of
volume (MSID: 2162149232) was completed. Number of files deleted: 7,
Number of directories deleted: 5. Total number of bytes deleted:
135168.
```

+
の詳細については `event log show`、を"ONTAPコマンド リファレンス"参照してください。

ディレクトリ削除ジョブのキャンセル

1. advanced権限モードに切り替えます。

   ```
   set -privilege advanced
   ```

2. ディレクトリの削除が実行中であることを確認します。

   ```
   volume file async-delete show
   ```

   ディレクトリのSVM、ボリューム、ジョブID、およびパスが表示された場合は、ジョブをキャンセルできます。

3. ディレクトリの削除をキャンセルします。

   ```
   volume file async-delete cancel -vserver <SVM_name> -volume <volume_name>
   -jobid <job_id>
   ```

FlexGroupsを使用して**ONTAP**ディレクトリを非同期的に削除するためのクライアント権限を管理する

ONTAP 9.11.1 以降、ストレージ管理者はボリュームに対する権限を付与して、NFS および SMB クライアントが非同期削除操作を実行できるようにすることができます。クラスタで非同期削除が有効になっている場合、Linuxクライアントユーザーは `mv`コマンドとWindowsクライアントユーザーは、 `rename`指定されたボリューム上のディレクトリを、デフォルトで .ontaptrashbin という名前の隠しディレクトリに移動して削除するコマンド。

権利は巻ごとに付与されます。 NFS クライアント ユーザーには、NFS クライアントに対するルート アクセス権と、NFS エクスポートに対するスーパーユーザー アクセス権が必要です。

ディレクトリのみを移動できます。ファイルを .ontaptrashbin ディレクトリに移動することはできません。

"ONTAPを使用してFlexGroupボリュームからディレクトリを非同期的に削除する方法について説明します。"
。

クライアントの非同期ディレクトリ削除を有効にする

手順

1. クラスタCLIからadvanced権限モードに切り替えます。 `-privilege advance`
2. ボリュームのマウントポイントでクライアントの非同期削除を有効にし、必要に応じて、ゴミ箱ディレクトリの別名を指定します。

   `volume file async-delete client enable volume` *`volname`* `vserver` *`vserverName`* `trashbinname` *`name`*

   デフォルトのごみ箱名を使用する例：

   ```
   cluster1::*> volume file async-delete client enable -volume v1 -vserver
   vs0

   Info: Async directory delete from the client has been enabled on volume
   "v1" in
         Vserver "vs0".
   ```

   代替ゴミ箱名を指定する例：

   ```
   cluster1::*> volume file async-delete client enable -volume test
   -trashbin .ntaptrash -vserver vs1

   Success: Async directory delete from the client is enabled on volume
   "v1" in
         Vserver "vs0".
   ```

3. クライアントの非同期削除が有効であることを確認します。

   `volume file async-delete client show`

   例：

```
cluster1::*> volume file async-delete client show

Vserver Volume      async-delete client TrashBinName
------------ ------------ ---------------------- -------------
vs1          vol1         Enabled          .ntaptrash
vs2          vol2         Disabled          -

2 entries were displayed.
```

クライアントの非同期ディレクトリ削除を無効にする

手順

1. クラスタCLIから、クライアントの非同期ディレクトリ削除を無効にします。

   `volume file async-delete client disable volume *volname* vserver *vserverName*`

   例：

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

       Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. クライアントの非同期削除が無効であることを確認します。

   `volume file async-delete client show`

   例：

```
cluster1::*> volume file async-delete client show

Vserver      Volume      async-delete client      TrashBinName
------------ ------------ ---------------------- -------------
vs1          vol1         Disabled                -
vs2          vol2         Disabled                -

2 entries were displayed.
```

ONTAP FlexGroupで**qtree**を作成する

ONTAP 9 3以降では、FlexGroupボリュームを含むqtreeを作成できます。qtreeを使用すると、FlexGroupボリュームを小さなセグメントにパーティショニングして、個別に管

理できます。

タスクの内容

- ソースFlexGroupボリュームにSnapMirror関係が確立されたqtreeがある場合、デスティネーションクラスタでONTAP 9 .3以降（qtreeをサポートするONTAPソフトウェアのバージョン）が実行されている必要があります。
- ONTAP 9 .5以降では、FlexGroupボリュームでqtreeの統計がサポートされます。

手順

1. FlexGroup ボリュームにqtreeを作成します。

```
volume qtree create -vserver <vserver_name> -volume <volume_name> -qtree
<qtree_name>
```

必要に応じて、qtreeのセキュリティ形式、SMB oplock、UNIX権限、およびエクスポートポリシーを指定できます。

```
cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1
-security-style mixed
```

関連情報

"論理ストレージ管理"

ONTAP FlexGroupボリュームにクォータを使用する

ONTAP 9 .4以前では、クォータルールをFlexGroupボリュームに適用できますが、クォータ制限を適用することはできません。ONTAP 9 5以降では、FlexGroupボリュームに適用されるクォータルールに制限を適用できます。

タスクの内容

- ONTAP 9 5以降では、FlexGroupボリュームにハードリミット、ソフトリミット、およびしきい値制限のクォータを指定できます。

  これらの制限を指定すると、特定のユーザ、グループ、またはqtreeが作成できるスペースの量、ファイル数、またはその両方を制限できます。クォータ制限は、次の場合に警告メッセージを生成します。

  - 使用量が設定されたソフトリミットを超えると、ONTAPは警告メッセージを発行しますが、それ以上のトラフィックは許可されます。

    その後、使用量が設定されたソフトリミットを再び下回ると、すべてクリアのメッセージが表示されます。

  - 使用量が設定されたしきい値制限を超えると、ONTAPは2番目の警告メッセージを発行します。

    その後使用量がしきい値制限を下回っても、解決済みのメッセージは表示されません。

- 使用量が設定されているハード リミットに達した場合、トラフィックが拒否されて、それ以降はリソースを消費できなくなります。

- ONTAP 9.5では、SnapMirror関係のデスティネーションFlexGroupボリュームでクォータ ルールを作成またはアクティブ化することができません。
- クォータの初期化中はクォータは適用されず、クォータの初期化後に超過したクォータに関する通知が生成されることはありません。

  クォータの初期化中にクォータに違反がなかったかどうかを確認するには、コマンドを使用し `volume quota report`ます。

クォータのターゲットとタイプ

クォータにはユーザ、グループ、またはqtreeの3種類のタイプがあります。クォータ ターゲットは、クォータ制限が適用されるユーザ、グループ、またはqtreeを指定します。

次の表に、クォータ ターゲットの種類、各クォータ ターゲットに関連付けられているクォータのタイプ、および各クォータ ターゲットの指定方法を示します。

クォータターゲット	クォータタイプ	ターゲットの指定方法	脚注
ユーザ	ユーザ クォータ	UNIXユーザ名 UNIX UID Windows 2000より前の形式のWindowsユーザ名 Windows SID	ユーザ クォータは、特定のボリュームまたはqtreeに適用できます
グループ	グループ クォータ	UNIXグループ名 UNIX GID	グループ クォータは、特定のボリュームまたはqtreeに適用できます グループ クォータの適用にWindows IDは使用されません。
qtree	ツリー クォータ	qtree名	ツリー クォータは特定のボリュームに適用され、他のボリューム内のqtreeには影響しません

""	ユーザ クォータ□□グループ クォータ ツリー クォータ	二重引用符（""）	と表示されたクォータターゲットは、 a_default QUOTA_示さ れています。デフォルトクォータの場合、クォータタイプはtypeフィールドの値によって決まります。

クォータ制限を超えた場合の**FlexGroup**の動作

ONTAP 9 .5以降では、FlexGroupボリュームでクォータ制限がサポートされます。FlexGroupとFlexVol volumeでは、クォータ制限の適用方法にいくつかの違いがあります。

クォータ制限を超えた場合、FlexGroupボリュームは次のように動作することがあります。

- FlexGroupボリュームのスペースとファイルの使用量が設定されているハードリミットを最大で5%上回ると、クォータ制限が適用されて以降のトラフィックが拒否されることがあります。

  最高のパフォーマンスを実現するために、ONTAPでは、クォータの適用が開始される前に、スペース使用量が設定されたハードリミットを少しだけ超過することがあります。この追加のスペース消費量が、設定されているハードリミット（1GBまたは65536ファイル）の5%を超えることはありません。

- クォータ制限に達したあと、ユーザまたは管理者が一部のファイルまたはディレクトリを削除してクォータ使用量が制限値を下回ると、クォータを消費する後続のファイル処理が遅延（再開までに最大5秒かかることがあります）で再開されることがあります。
- FlexGroupボリュームのスペースとファイルの合計使用量が設定されたクォータ制限を超えた場合、イベントログメッセージのロギングがわずかに遅れることがあります。
- FlexGroup ボリュームの一部のコンスティチュエントがいっぱいになったにもかかわらず、クォータ制限に達していない場合は、「スペース不足」エラーが表示されます。
- クォータのハードリミットが設定されているクォータターゲットでのファイルまたはディレクトリの名前変更やqtree間のファイル移動などの処理は、FlexVolでの同様の処理に比べて時間がかかることがあります。

FlexGroupボリュームに対するクォータの適用例

以下の例を使用して、ONTAP 9 .5以降で制限を使用してクォータを設定する方法を理解できます。

例 **1** ：ディスク制限を指定してクォータルールを適用する

1. 現実的な値のディスクのソフトリミットとハードリミットを指定したタイプのクォータポリシールールを作成する必要があります `user`。

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. クォータポリシールールを表示できます。

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           1TB    800GB       -        -
-
```

3. 新しいクォータルールをアクティブ化するには、ボリュームのクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. クォータレポートを使用して、FlexGroupボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    root      50GB      -       1       -
FG                 user    *         800GB    1TB      0       -   *
2 entries were displayed.
```

ディスクのハードリミットに達すると、クォータポリシールールのターゲット（この場合はユーザ）はファイルへのデータの書き込みをブロックされます。

例 **2** ：複数のユーザにクォータルールを適用する

1. タイプがのクォータポリシールールを作成し `user`ます。クォータターゲットに複数のユーザ（UNIXユーザ、SMBユーザ、またはその両方の組み合わせ）を指定し、現実的な値のディスクのソフトリミットとハードリミットを指定します。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit  800GB
```

2. クォータポリシールールを表示できます。

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "rdavis,ABCCORP\RobertDavis"  "" off  1TB  800GB  -  -
```

3. 新しいクォータルールをアクティブ化するには、ボリュームのクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. クォータの状態がアクティブであることを確認できます。

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
                Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. クォータレポートを使用して、FlexGroupボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                       ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis,ABCCORP\RobertDavis
```

クォータ制限は、クォータターゲットにリストされているすべてのユーザに共有されます。

ディスクのハードリミットに達すると、クォータターゲットにリストされているユーザはファイルへのデータの書き込みをブロックされます。

例 **3** ：ユーザマッピングが有効なクォータを適用する

1. タイプのクォータポリシールールを作成し `user`、UNIXユーザまたはWindowsユーザをクォータターゲットとしてに指定し、をに設定して `on`、現実的な値のディスクのソフトリミットとディスクのハードリミットを指定 `user-mapping`します。

   UNIXユーザとWindowsユーザ間のマッピングは、コマンドを使用して事前に設定しておく必要があります `vserver name-mapping create`。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit  800GB -user-mapping on
```

2. クォータポリシールールを表示できます。

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                              Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   rdavis    ""      on           1TB    800GB       -        -
-
```

3. 新しいクォータルールをアクティブ化するには、ボリュームのクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. クォータの状態がアクティブであることを確認できます。

```
cluster1::> volume quota show -vserver vs0 -volume FG
               Vserver Name: vs0
                Volume Name: FG
                Quota State: on
                 Scan Status: -
           Logging Messages: on
           Logging Interval: 1h
           Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. クォータレポートを使用して、FlexGroupボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                      ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis
```

クォータ制限は、クォータターゲットにリストされているユーザと、それに対応するWindowsユーザまたはUNIXユーザの間で共有されます。

ディスクのハードリミットに達すると、クォータターゲットにリストされているユーザと、そのユーザに対応するWindowsユーザまたはUNIXユーザは、ファイルへのデータの書き込みをブロックされます。

例 **4** ：クォータが有効になっている場合に **qtree** のサイズを確認する

1. タイプがで、現実的な値のディスクのソフトリミットとハードリミットが設定されたクォータポリシールールを作成する必要があります `tree`。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. クォータポリシールールを表示できます。

```
cluster1::> quota policy rule show -vserver vs0

Vserver: vs0                Policy: default           Volume: FG

                                                 Soft              Soft
                          User          Disk     Disk    Files     Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit     Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree    tree_4118314302  "" -          48GB        -      20        -
```

3. 新しいクォータルールをアクティブ化するには、ボリュームのクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

   a. クォータレポートを使用して、FlexGroupボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
------- -------- ------ ------- ----- ----- ------ ------ ---------
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

   クォータ制限は、クォータターゲットにリストされているユーザと、それに対応するWindowsユーザまたはUNIXユーザの間で共有されます。

4. NFSクライアントから、コマンドを使用して、 `df`合計スペース使用量、使用可能なスペース、および使用済みスペースを表示します。

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

ハードリミットが指定されている場合、NFSクライアントでは次のようにスペース使用量が計算されます。

- 合計スペース使用量 = ツリーのハードリミット
- 空きスペース = ハードリミットから qtree のスペース使用量をハードリミットなしで引いた値は、NFS クライアントで次のようにスペース使用量が計算されます。
- スペース使用量 = クォータ使用量
- 合計スペース = ボリューム内のクォータ使用量と物理的な空きスペースの合計です

5. SMB共有から、エクスプローラを使用して、合計スペース使用量、使用可能なスペース、および使用済みスペースを表示します。

   SMB共有では、スペース使用量の計算に関する次の考慮事項に注意する必要があります。

   - 使用可能な合計スペースの計算では、ユーザおよびグループのユーザクォータのハードリミットが考慮されます。
   - ツリークォータルール、ユーザクォータルール、グループクォータルールの空きスペースの中で最も小さな値が、 SMB 共有の空きスペースと見なされます。
   - SMB では合計スペース使用量が一定ではなく、ツリー、ユーザ、グループの中で最も小さな空きスペースに対応するハードリミットによって決まります。

FlexGroupボリュームにルールと制限を適用する

手順

1. ターゲットのクォータルールを作成します。 `volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]`

   - FlexGroupボリュームのクォータターゲットのタイプは、、 `group`のいずれ `tree`かです `user`。
   - FlexGroup ボリュームのクォータルールを作成する際に、ターゲットとしてパスを指定することはできません。
   - ONTAP 9.5 以降では、 FlexGroup ボリュームに対して、ディスクのハードリミット、ファイルのハードリミット、ディスクのソフトリミット、ファイルのソフトリミット、しきい値制限の各クォータを指定できます。

     ONTAP 9 .4以前では、FlexGroupボリュームのクォータルールを作成するときに、ディスクリミット、ファイルリミット、ディスクリミットのしきい値、ディスクのソフトリミット、ファイルのソフトリミットを指定できません。

次の例は、ユーザターゲットタイプに対してデフォルトのクォータルールを作成します。

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

次の例は、qtree1という名前のqtreeにツリークォータルールを作成します。

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. 指定したFlexGroupボリュームのクォータをアクティブ化します。 `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. クォータの初期化状態を監視します。 `volume quota show -vserver svm_name`

FlexGroupボリュームの状態がと表示されることがあります `mixed`。これは、まだすべてのコンスティチュエントボリュームの状態が同じではないことを示しています。

```
cluster1::> volume quota show -vserver vs0
                                        Scan
Vserver    Volume        State          Status
---------  ------------  -------------- ------
vs0        fg1           initializing         95%
vs0        vol1          off                   -
2 entries were displayed.
```

1. アクティブなクォータがあるFlexGroupのクォータレポートを表示します。 `volume quota report -vserver svm_name -volume flexgroup_vol`

   FlexGroupの場合、コマンドでパスを指定することはできません `volume quota report`。

   次の例は、FlexGroupボリュームのユーザークォータを示しています。 `fg1` ：

```
cluster1::> volume quota report -vserver vs0 -volume fg1
  Vserver: vs0
                                       ----Disk----  ----Files-----
Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  fg1                user    *           0B      -       0       -   *
  fg1                user    root       1GB      -       1       -   *
  2 entries were displayed.
```

次の例は、FlexGroupボリュームのツリークォータを示しています。 `fg1` ：

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
fg1      qtree1  tree      1         68KB      -      18       -
qtree1
fg1              tree      *           0B      -       0       -   *
2 entries were displayed.
```

結果

クォータルールとクォータ制限がFlexGroupボリュームに適用されます。

ONTAPがそれ以上のトラフィックを拒否してクォータを適用する前に、設定されたハードリミットよりも最大5%高い使用量に達する可能性があります。

関連情報

- "ONTAPコマンド リファレンス"

ONTAP FlexGroupボリュームで**Storage Efficiency**を有効にする

FlexGroup に重複排除とデータ圧縮を一緒に、または個別に実行して、最善のスペース削減効果を得ることができます。

開始する前に

FlexGroupボリュームはオンラインである必要があります。

手順

1. FlexGroupボリュームでStorage Efficiencyを有効にします。 `volume efficiency on -vserver svm_name -volume volume_name`

   Storage Efficiency 処理は、 FlexGroup のすべてのコンスティチュエントで有効になります。

   ボリュームで Storage Efficiency を有効にしたあとに FlexGroup ボリュームを拡張した場合は、新しいコンスティチュエントでも Storage Efficiency が自動的に有効になります。

2. コマンドを使用して、FlexGroupボリュームで必要なStorage Efficiency処理を有効にします `volume efficiency modify`。

   FlexGroup ボリュームでは、インライン重複排除、ポストプロセス重複排除、インライン圧縮、およびポストプロセス圧縮を有効にすることができます。FlexGroup ボリュームに対して圧縮形式（二次圧縮またはアダプティブ圧縮）を設定し、スケジュールや効率化ポリシーを指定することもできます。

3. スケジュールや効率化ポリシーを使用せずにStorage Efficiency処理を実行する場合は、効率化処理を開始します。 `volume efficiency start -vserver svm_name -volume volume_name`

   重複排除とデータ圧縮が有効になっている場合は、最初にデータ圧縮が実行され、続けて重複排除が実行されます。FlexGroup ボリュームですでにいずれかの効率化処理がアクティブになっている場合、このコマンドは失敗します。

4. FlexGroupボリュームで有効になっている効率化処理を確認します。 `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
             Vserver Name: vs1
              Volume Name: fg1
              Volume Path: /vol/fg1
                    State: Enabled
                   Status: Idle
                 Progress: Idle for 17:07:25
                     Type: Regular
                 Schedule: sun-sat@0

...

             Compression: true
      Inline Compression: true
Incompressible Data Detection: false
      Constituent Volume: false
Compression Quick Check File Size: 524288000
           Inline Dedupe: true
         Data Compaction: false
```

Snapshotの作成を自動的に管理するSnapshotポリシーを作成したり、FlexGroupボリュームのSnapshotを手動で作成したりできます。FlexGroupボリュームの有効なSnapshotは、ONTAPがFlexGroupボリュームの各コンスティチュエントのSnapshotを正常に作成できるまで作成されません。

タスクの内容

- Snapshotポリシーに複数のFlexGroupを関連付ける場合は、FlexGroupのスケジュールが重ならないようにする必要があります。
- ONTAP 9.8以降では、FlexGroupボリュームでサポートされるSnapshotの最大数は1023です。

ONTAP 9.8以降では `volume snapshot show`、FlexGroupボリュームに対するコマンドで、最も若い所有ブロックが計算されるのではなく、論理ブロックを使用してSnapshotサイズが報告されます。この新しいサイズ計算方法では、以前のバージョンのONTAPでの計算よりもスナップショットサイズが大きく表示されることがあります。

手順

1. Snapshotポリシーを作成するか、手動でSnapshotを作成します。

作成する項目	入力するコマンド
Snapshotポリシー	`volume snapshot policy create` FlexGroupボリュームのSnapshotポリシーに関連付けるスケジュールは、間隔が30分を超える必要があります。 FlexGroupボリュームを作成すると、`default`SnapshotポリシーがFlexGroupボリュームに適用されます。
Snapshotを手動で作成	`volume snapshot create` FlexGroupのSnapshotを作成したあとで、Snapshotの属性を変更することはできません。属性を変更する場合は、Snapshotを削除してから再作成する必要があります。

Snapshotの作成時には、FlexGroupボリュームへのクライアントアクセスが一時的に休止されます。

1. FlexGroupボリュームの有効なSnapshotが作成されたことを確認します。 `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot               state
------- ------ ---------------------- -----
fg_vs   fg     hourly.2016-08-23_0505 valid
```

2. FlexGroupボリュームのコンスティチュエントのSnapshotを表示します。 `volume snapshot show -is-constituent true`

```
cluster1::> volume snapshot show -is-constituent true

---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
fg_vs    fg__0001
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0002
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0003
                  hourly.2016-08-23_0505                    72MB     0%
27%
...
         fg__0016
                  hourly.2016-08-23_0505                    72MB     0%
27%
```

ONTAP FlexGroupからのコンスティチュエントの移動

FlexGroupボリュームのコンスティチュエントをアグリゲート間で移動して、特定のコンスティチュエントのトラフィックが多い場合に負荷を分散することができます。コンスティチュエントを移動すると、既存のコンスティチュエントのサイズを変更するためにアグリゲートのスペースを解放することもできます。

開始する前に

SnapMirror関係にあるFlexGroupボリュームコンスティチュエントを移動する場合は、SnapMirror関係を初期化しておく必要があります。

タスクの内容

FlexGroupボリュームのコンスティチュエントの拡張中は、ボリューム移動処理を実行できません。

手順

1. 移動するFlexGroupボリュームコンスティチュエントを特定します。

   `volume show -vserver svm_name -is-constituent true`

```
cluster1::> volume show -vserver vs2 -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2       fg1          -            online     RW        400TB
15.12TB   62%
vs2       fg1__0001    aggr1        online     RW         25TB
8.12MB   59%
vs2       fg1__0002    aggr2        online     RW         25TB
2.50TB   90%
...
```

2. FlexGroupボリュームコンスティチュエントの移動先となるアグリゲートを特定します。

   `volume move target-aggr show -vserver svm_name -volume vol_constituent_name`

   使用可能なスペースが移動するFlexGroupボリュームコンスティチュエントのサイズよりも大きいアグリゲートを選択する必要があります。

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9TB          hdd
node12a_aggr3    100.34TB         hdd
node12a_aggr2    100.36TB         hdd
node12a_aggr1    100.36TB         hdd
node12a_aggr4    100.36TB         hdd
5 entries were displayed.
```

3. FlexGroupボリュームコンスティチュエントを目的のアグリゲートに移動できることを確認します。

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name -perform-validation-only true`

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

4. FlexGroupボリュームコンスティチュエントを移動します。

```
volume move start -vserver svm_name -volume vol_constituent_name -destination
-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]
```

ボリューム移動処理はバックグラウンドプロセスとして実行されます。

ONTAP 9 5以降では、パラメータをに `true`設定することで、FlexGroupボリュームコンスティチュエントをFabric Poolから非Fabric Poolに（またはその逆に）移動できます `-allow-mixed-aggr-types`。デフォルトでは、この `-allow-mixed-aggr-types`オプションはに設定されて `false`います。

FlexGroupでは、コマンドを使用して暗号化を有効にすることはできません `volume move`。

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```

アクティブなSnapMirror処理が原因でボリューム移動処理が失敗した場合は、コマンドを使用してSnapMirror処理を中止する必要があります `snapmirror abort -h`。場合によっては、SnapMirrorの中止処理も失敗することがあります。その場合は、ボリューム移動処理を中止してから再試行してください。の詳細については `snapmirror abort`、を"ONTAPコマンド リファレンス"参照してください。

5. ボリューム移動処理の状態を確認します。

```
volume move show -volume vol_constituent_name
```

次の例は、ボリューム移動処理のレプリケーションフェーズを完了し、カットオーバーフェーズにあるFlexGroupコンスティチュエントボリュームの状態を示しています。

```
cluster1::> volume move show -volume fg1_002
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       fg1_002    healthy  cutover     -                -
```

既存の**ONTAP FlexGroup**ボリュームに**FabricPool**内のアグリゲートを使用する

ONTAP 9 .5以降では、FlexGroupボリュームでFabricPoolがサポートされます。FabricPool内のアグリゲートを既存のFlexGroupボリュームに使用する場合は、FlexGroupボリュームが配置されているアグリゲートをFabricPool内のアグリゲートに変換するか、FlexGroupボリュームのコンスティチュエントをFabricPool内のアグリゲートに移行します。

開始する前に

- FlexGroupボリュームのスペースギャランティをに設定する必要があります `none`。

- FlexGroupボリュームが配置されているアグリゲートをFabricPool内のアグリゲートに変換する場合は、アグリゲートがSSDディスクのみを使用している必要があります。

タスクの内容

既存のFlexGroupボリュームがSSD以外のアグリゲートに配置されている場合は、FlexGroupボリュームのコンスティチュエントをFabricPool内のアグリゲートに移行する必要があります。

選択肢

- FlexGroupボリュームが配置されているアグリゲートをFabricPool内のアグリゲートに変換するには、次の手順を実行します。

  a. 既存のFlexGroupボリュームで階層化ポリシーを設定します。 `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. FlexGroupボリュームが配置されているアグリゲートを特定します。 `volume show -volume flexgroup_name -fields aggr-list`

  ```
  cluster-2::> volume show -volume fg1 -fields aggr-list
  vserver volume aggr-list
  ------- ------ -----------
  vs1     fg1    aggr1,aggr3
  ```

  c. アグリゲートリストに表示された各アグリゲートにオブジェクトストアを接続します。 `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

  すべてのアグリゲートをオブジェクトストアに接続する必要があります。

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- FlexGroupボリュームコンスティチュエントをFabricPoolのアグリゲートに移行するには、次の手順を実行します。

  a. 既存のFlexGroupボリュームで階層化ポリシーを設定します。 `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. FlexGroupボリュームの各コンスティチュエントを、同じクラスタ内のFabricPool内のアグリゲートに移動します。 `volume move start -volume constituent-volume -destination -aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

FlexGroupボリュームのすべてのコンスティチュエントをFabricPool内のアグリゲートに移動し（FlexGroupコンスティチュエントが異なるタイプのアグリゲートに配置されている場合）、すべてのコンスティチュエントをクラスタ内のノード間に分散させる必要があります。

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

関連情報

- "ディスクおよびアグリゲートの管理"
- "ストレージ集約オブジェクトストアアタッチ"

ファイルデータの再分散による**ONTAP FlexGroup**ボリュームのバランス調整

ONTAP 9 .16.1以降では、高度な容量分散を有効にして、大容量ファイルが拡張されて1つのメンバーボリュームのスペースが消費された場合に、FlexGroupメンバーボリューム間でデータを分散させることができます。

高度な容量バランシングにより、ONTAP 9 .12.1で導入されたきめ細かなデータ機能が拡張され、ONTAPはファイルを他のメンバーに移動できるようになり"FlexGroupボリュームのリバランシング"ます。ONTAP 9 .16.1以降では、オプションを使用して高度な容量バランシングを有効にすると、 `-granular-data advanced`「基本的な」ファイルリバランシング機能と高度な容量機能の両方がアクティブになります。

ファイルのリバランシングと高度な容量のバランシングは、どちらもデフォルトで無効になっています。これらの機能を有効にすると、無効にすることはできません。容量の分散を無効にする必要がある場合は、高度な容量の分散を有効にする前に作成されたSnapshotからリストアする必要があります。

高度な容量分散は、新しい書き込みが10GB（ボリュームの空きスペースの1%）に達するとトリガーされます。

ファイルの分散方法

ファイルが作成または拡張されて容量の高度な分散が行われるようになると、ファイルは1GB~10GBのストライプでメンバーFlexGroupボリュームに分散されます。

高度な容量バランシングを有効にすると、ONTAPは既存の大容量ファイルをさかのぼってストライプしません。高度な容量分散を有効にした後も既存の大容量ファイルが引き続き拡張される場合は、ファイルのサイズと使用可能なスペースに応じて、既存の大容量ファイルの新しいコンテンツがメンバーFlexGroupボリュームにストライピングされることがあります。

高度な容量バランシングによってストライプ幅が決定される1つの方法は、メンバーボリュームで使用可能な空きスペースの量を使用することです。高度な容量分散により、使用可能な空きスペースの1%のファイルストライプが作成されます。つまり、使用可能なスペースが増えるとストライプのサイズが大きくなり、FlexGroupがいっぱいになるとストライプのサイズが小さくなります。

サポートされるプロトコル

高度な容量分散は、次のプロトコルでサポートされます。

- NFSv3、NFSv4、NFSv4.1
- pNFS
- SMB

高度な容量分散を有効にする

デフォルトでは、高度な容量分散は無効になっています。FlexGroup容量を自動的に分散するには、高度な容量分散を有効にする必要があります。一度有効にするとこの機能を無効にすることはできませんが、高度な容量分散を有効にする前に作成されたSnapshotからリストアすることは可能です。

開始する前に

- クラスタ内のすべてのノードでONTAP 9 .16.1以降が実行されている必要があります。
- 高度な容量分散が有効になっている場合、ONTAP 9 16.1より前のリリースにリバートすることはできません。リバートが必要な場合は、高度な容量分散を有効にする前に作成されたSnapshotからリストアする必要があります。
- (`vserver nfs -vstorage enabled`SVMでNFSコピーオフロードが有効になっている場合）、FlexGroupボリュームで高度な容量分散を有効にすることはできません。同様に、SVM内のいずれかのFlexGroupボリュームで高度な容量バランシングを有効にしている場合、NFSコピーオフロードを有効にすることはできません。
- FlexCacheライトバックでは、高度な容量分散はサポートされていません。
- ONTAP 9.16.1以降を実行するクラスタのボリュームで高度な容量分散が有効になっている場合、ONTAP 9.16.1より前のバージョンのONTAPではSnapMirror転送がサポートされません。

タスクの内容

詳細なデータオプション（基本またはアドバンスト）を使用してDPデスティネーションボリュームを作成する場合、SnapMirror転送が完了するまでデスティネーションには設定が「disabled」と表示されます。転送が完了すると、DPデスティネーションに詳細なデータが「有効」と表示されます。

FlexGroupの作成時に高度な容量分散を有効にする

手順

System ManagerまたはONTAP CLIを使用して、新しいFlexGroupボリュームを作成するときに容量の高度な分散を有効にすることができます。

System Manager

1. [ストレージ]>[ボリューム]*に移動し、をクリックします

。
2. ウィンドウで、ボリュームの名前とサイズを入力します。次に[その他のオプション]*をクリックします。
3. で、[ボリュームデータをクラスタ全体に分散（FlexGroup）]*を選択します。
4. [Advanced capacity balancing]*を選択します。
5. ボリュームの設定を完了し、*[保存]*をクリックします。

CLI

1. 高度な容量バランシングを有効にしてボリュームを作成します。

```
volume create -vserver <svm name> -volume <volume name> -size <volume
size> -auto-provision-as flexgroup -junction-path /<path> -granular
-data advanced
```

例：

```
volume create -vserver vs0 -volume newvol -size 1TB -auto-provision
-as flexgroup -junction-path /newvol -granular-data advanced
```

既存の**FlexGroup**ボリュームで高度な容量分散を有効にする

手順

System ManagerまたはONTAP CLIを使用して、高度な容量分散を有効にすることができます。

System Manager

1. [ストレージ]>[ボリューム]に移動し、をクリックし⋮て[編集]>[ボリューム]*を選択します。
2. ウィンドウの[ストレージと最適化]で、[高度な容量バランシング]*を選択します。
3. [保存（ Save ）] をクリックします。

CLI

1. 既存のFlexGroupボリュームを変更して、高度な容量分散を有効にします。

```
volume modify -vserver <svm name> -volume <volume name> -granular
-data advanced
```

例：

```
volume modify -vserver vs0 -volume newvol  -granular-data advanced
```

ファイルの移動による**ONTAP FlexGroup**ボリュームのリバランシング

ONTAP 9 12.1以降では、FlexGroup内のあるコンスティチュエントから別のコンスティチュエントにファイルを無停止で移動することで、FlexGroupボリュームのリバランシングを実行できます。

FlexGroupのリバランシングは、新しいファイルの追加やファイルの増加によって不均衡が長期的に生じた場合に、容量を再配分するのに役立ちます。リバランシング処理を手動で開始すると、ONTAPによってファイルが選択され、システムを停止することなく自動的に移動されます。

> マルチパートinodeの作成により、1つのリバランシングイベントまたは複数のリバランシングイベントの一部として大量のファイルが移動された場合、FlexGroupのリバランシングではシステムパフォーマンスが低下することに注意してください。リバランシングイベントの一環として移動されたすべてのファイルには、そのファイルに2つのマルチパートinodeが関連付けられています。FlexGroup内のファイル総数に対するマルチパートinodeを持つファイル数の割合が大きいほど、パフォーマンスへの影響が大きくなります。FlexVolからFlexGroupへの変換など、特定のユースケースでは、大量のマルチパートinodeが作成される可能性があります。

リバランシングは、クラスタ内のすべてのノードでONTAP 9.12.1以降のリリースが実行されている場合にのみ使用できます。リバランシング処理を実行するFlexGroupボリュームでは、詳細データ機能を有効にする必要があります。一度有効にすると、このボリュームを削除するか、設定を有効にする前に作成されたSnapshotからリストアしないかぎり、ONTAP 9.11.1以前のバージョンに戻すことはできません。

ONTAP 9.14.1以降では、ONTAPに導入されたアルゴリズムにより、ユーザが操作しなくても、詳細データ機能が有効になっているボリューム内のファイルが、システムの停止を伴わずプロアクティブに移動されます。このアルゴリズムは、きわめて特殊な限られたシナリオで作動し、パフォーマンスのボトルネックを軽減します。このアルゴリズムが機能するシナリオには、クラスタ内の1つのノード上の特定のファイル セットに対する書き込み負荷が非常に高い場合や、非常にホットな親ディレクトリ内のファイルが継続的に増加している場合などがあります。

ONTAP 9 .16.1以降では、を有効にして、FlexGroupメンバーボリューム間で大容量ファイルのデータを再分散することもできます"高度な容量分散"。

FlexGroupリバランシングに関する考慮事項

FlexGroupリバランシングの仕組みおよび他のONTAP機能との連携を理解しておく必要があります。

- FlexVolからFlexGroupへの変換

  FlexVolからFlexGroupへの変換後は、 FlexGroup の自動再バランス調整を使用しないことをお勧めします。代わりに、既存のファイルを再配布するには、 `volume rebalance file-move start` ONTAP 9.10.1 以降で使用可能なコマンド。この操作はデフォルトで非中断です(`-is-disruptive false`）。ビジー状態のファイルの一部が移動できない場合は、中断モードでコマンドを再実行できます。(`-is -disruptive true`) を計画されたメンテナンス時間中に実行します。詳細はこちら `volume rebalance file-move start`の中で"ONTAPコマンド リファレンス" 。

  FlexGroupの自動リバランシング機能を使用したリバランシングでは、FlexVolからFlexGroupへの変換を実行し、FlexVol volume上のデータの50~85%が新しいコンスティチュエントに移動されるなど、多数のファイルを移動する際のパフォーマンスが低下する可能性があります。

- ファイルの最小サイズと最大サイズ

  自動リバランシングの対象となるファイルは、保存されているブロックに基づいて選択されます。デフォルトでは、リバランシング対象となる最小ファイル サイズは100MB（後述のmin-file-sizeパラメータを使用すると20MBまで低く設定可能）、最大ファイル サイズは100GBです。

- スナップショット内のファイル

  現在どのスナップショットにも存在しないファイルのみを移動対象として考慮するようにFlexGroupのリバランシングを設定できます。リバランシングが開始されると、リバランシング処理中にいつでもSnapshot処理がスケジュールされているかどうかが通知に表示されます。

  ファイルが移動中で、デスティネーションでフレーミング中の場合、スナップショットは制限されます。ファイルのリバランシングの実行中は、Snapshotのリストア処理は実行できません。

  ONTAP 9.11.1以前のバージョンではマルチパートinodeがサポートされないため、オプションを有効にしたあとに作成されたSnapshotは、 `granular-data`ONTAP 9.11.1以前のバージョンを実行するシステムにレプリケートできません。

- SnapMirrorの処理

  FlexGroupのリバランシングは、スケジュールされたSnapMirror処理間で実行する必要があります。SnapMirror処理を開始する前にファイルを再配置する場合、そのファイルの移動が24分以内に完了しないと、SnapMirror処理が失敗することがありますSnapMirror。SnapMirror転送の開始後に開始される新しいファイルの再配置は失敗しません。

- ファイルベースの圧縮によるストレージ効率化

  ファイルベースの圧縮によるStorage Efficiencyでは、デスティネーションに移動する前にファイルが解凍されるため、圧縮による削減効果は失われます。圧縮による削減効果は、リバランシング後に手動で開始したバックグラウンドスキャナをFlexGroupボリュームで実行したあとに回復します。ただし、いずれかのボリュームのSnapshotに関連付けられているファイルがある場合、そのファイルの圧縮は無視されます。

- 重複排除

  重複排除されたファイルを移動すると、FlexGroupボリュームの全体的な使用量が増加する可能性があります。ファイルのリバランシングでは、一意のブロックのみがデスティネーションに移動され、ソースの容量が解放されます。共有ブロックはソースに保持され、デスティネーションにコピーされます。これにより、ほぼフルのソース コンスティチュエントの使用済み容量を削減するという目標は達成できますが、新しいデスティネーションに共有ブロックがコピーされるため、FlexGroupボリュームの全体的な使用量が増加する可能性もあります。これは、スナップショットの一部であるファイルが移動された場合にも可能です。Snapshotスケジュールが再利用され、Snapshot内のファイルのコピーがなくなるまで、スペース削減は完全に認識されません。

- FlexCloneボリューム

  FlexCloneボリュームを作成したときにファイルのリバランシングが実行されていた場合、そのFlexCloneボリュームでリバランシングは実行されません。FlexCloneボリュームでのリバランシングは、ボリュームの作成後に実行する必要があります。

- ファイル移動

  FlexGroupリバランシング処理中にファイルが移動されると、ソースとデスティネーションの両方のコンスティチュエントでのクォータ計算で、そのファイル サイズが報告されます。移動が完了すると、クォータの計算は通常の状態に戻り、ファイル サイズは新しいデスティネーションでのみ報告されます。

- 自律型ランサムウェア対策

  ONTAP 9 .13.1以降では、システムの停止を伴うリバランシング処理と無停止のリバランシング処理で自律型ランサムウェア対策がサポートされます。

- オブジェクトストアボリューム

  ボリューム容量のリバランシングは、S3バケットなどのオブジェクトストアボリュームではサポートされていません。

FlexGroupリバランシングを有効にする

ONTAP 9 12.1以降では、無停止のFlexGroupボリュームの自動リバランシングを有効にして、FlexGroupコンスティチュエント間でファイルを再配分できます。

ONTAP 9 .13.1以降では、単一のFlexGroupリバランシング処理を将来の日時に開始するようにスケジュール設定できます。

開始する前に

FlexGroupのリバランシングを有効にする前に、FlexGroupボリュームでオプションを有効にしておく必要があります `granular-data`。有効にするには、次のいずれかの方法を使用します。

- コマンドを使用してFlexGroupボリュームを作成する場合 `volume create`
- コマンドを使用して既存のFlexGroupボリュームを変更して設定を有効にする `volume modify`
- コマンドを使用してFlexGroupのリバランシングが開始されたときに自動的に設定する `volume rebalance`

ONTAP 9 .16.1以降を使用していて、ONTAP CLIのオプションまたはSystem Managerを使用して有効にしている `granular-data advanced`場合は"FlexGroupの高度な容量分散"、FlexGroupのリバランシングも有効になります。

手順

FlexGroupのリバランシングは、ONTAPシステムマネージャまたはONTAP CLIを使用して管理できます。

System Manager

1. [ストレージ]>[ボリューム]に移動し、再バランスするFlexGroup ボリュームを探します。
2. を選択 ⌄ してボリュームの詳細を表示します。
3. FlexGroup Balance Status で Rebalance *を選択します。

   「リバランス」オプションは、FlexGroupステータスが残高不足の場合にのみ使用できます。

4. 「* Rebalance Volume *」（ボリュームの再バランス）ウィンドウで、必要に応じてデフォルト設定を変更します。
5. リバランシング処理をスケジュールするには、*[あとでリバランシング]*を選択して日時を入力します。

CLI

1. 自動リバランシングを開始します。

   ```
   volume rebalance start -vserver <SVM name> -volume <volume name>
   ```

   必要に応じて、次のオプションを指定できます。

   [[-max-runtime]<time interval>最大実行時間

   [-max-threshold <percent>]コンスティチュエントあたりの最大不均衡しきい値

   [-min-threshold <percent>]コンスティチュエントごとの最小不均衡しきい値

   [-max-file-moves <integer>]コンスティチュエントあたりの同時ファイル移動の最大数

   [-min-file-size ｛<integer>[KB|MB|GB|TB|PB]｝]最小ファイルサイズ

   [-start-time <mm/dd/yyyy-00:00:00>]再バランスの開始日時をスケジュールします

   [-exclude-snapshots ｛true|false｝] Snapshotでスタックしているファイルを除外する

   例：

   ```
   volume rebalance start -vserver vs0 -volume fg1
   ```

FlexGroupリバランシングの設定を変更します。

FlexGroupのリバランシング構成を変更して、不均衡しきい値、同時ファイル数移動の最小ファイルサイズ、最大ランタイムを更新し、スナップショットを含めるか除外することができます。FlexGroupリバランシングスケジュールを変更するオプションは、ONTAP 9.13.1以降で使用できます。

System Manager

1. [ストレージ]>[ボリューム]に移動し、再バランスするFlexGroup ボリュームを探します。
2. を選択 してボリュームの詳細を表示します。
3. FlexGroup Balance Status で Rebalance *を選択します。

   「リバランス」オプションは、FlexGroupステータスが残高不足の場合にのみ使用できます。

4. 「* Rebalance Volume *」（ボリュームの再バランス）ウィンドウで、必要に応じてデフォルト設定を変更します。

CLI

1. 自動リバランシングを変更します。

   ```
   volume rebalance modify -vserver <SVM name> -volume <volume name>
   ```

   次のオプションを1つ以上指定できます。

   [[-max-runtime]<time interval>最大実行時間

   [-max-threshold <percent>]コンスティチュエントあたりの最大不均衡しきい値

   [-min-threshold <percent>]コンスティチュエントごとの最小不均衡しきい値

   [-max-file-moves <integer>]コンスティチュエントあたりの同時ファイル移動の最大数

   [-min-file-size ｛<integer>[KB|MB|GB|TB|PB]｝]最小ファイルサイズ

   [-start-time <mm/dd/yyyy-00:00:00>]再バランスの開始日時をスケジュールします

   [-exclude-snapshots ｛true|false｝] Snapshotでスタックしているファイルを除外する

FlexGroupリバランシングの停止

FlexGroupのリバランシングを有効またはスケジュール設定したあとは、いつでも停止できます。

System Manager

1. [ストレージ]>[ボリューム]の順に選択し、FlexGroup ボリュームを探します。
2. を選択 してボリュームの詳細を表示します。
3. [Stop Rebalance]*を選択します。

CLI

1. FlexGroup のリバランシングを停止します。

```
volume rebalance stop -vserver <SVM name> -volume <volume name>
```

FlexGroupリバランシングステータスの表示

FlexGroupリバランシング処理のステータス、FlexGroupリバランシングの設定、リバランシング処理時間、およびリバランシングインスタンスの詳細を表示できます。

System Manager

1. [ストレージ]>[ボリューム]の順に選択し、FlexGroup ボリュームを探します。
2. FlexGroupの詳細を表示する場合に選択し ⌄ ます。
3. * FlexGroup Balance Status *は、詳細ペインの下部に表示されます。
4. 前回のリバランシング処理に関する情報を表示するには、*[前回のボリュームのリバランシングステータス]*を選択します。

CLI

1. FlexGroup のリバランシング処理のステータスを表示します。

```
volume rebalance show
```

リバランシング状態の例：

```
> volume rebalance show
Vserver: vs0
                                                                  Target
Imbalance
Volume       State                  Total      Used     Used
Size     %
------------ ------------------ --------- --------- ---------
--------- -----
fg1          idle                     4GB   115.3MB         -
8KB    0%
```

リバランシングの設定の詳細例：

```
> volume rebalance show -config
Vserver: vs0
                     Max            Threshold         Max
Min          Exclude
Volume               Runtime        Min     Max       File Moves
File Size    Snapshot
---------------      ------------   -----   -----     ----------
---------    ---------
fg1                  6h0m0s         5%      20%          25
4KB          true
```

リバランシング時間の詳細の例：

```
> volume rebalance show -time
Vserver: vs0
Volume               Start Time                    Runtime
Max Runtime
---------------     -------------------------     -----------
-----------
fg1                  Wed Jul 20 16:06:11 2022      0h1m16s
6h0m0s
```

リバランシング インスタンスの詳細の例：

```
    > volume rebalance show -instance
    Vserver Name: vs0
    Volume Name: fg1
    Is Constituent: false
    Rebalance State: idle
    Rebalance Notice Messages: -
    Total Size: 4GB
    AFS Used Size: 115.3MB
    Constituent Target Used Size: -
    Imbalance Size: 8KB
    Imbalance Percentage: 0%
    Moved Data Size: -
    Maximum Constituent Imbalance Percentage: 1%
    Rebalance Start Time: Wed Jul 20 16:06:11 2022
    Rebalance Stop Time: -
    Rebalance Runtime: 0h1m32s
    Rebalance Maximum Runtime: 6h0m0s
    Maximum Imbalance Threshold per Constituent: 20%
    Minimum Imbalance Threshold per Constituent: 5%
    Maximum Concurrent File Moves per Constituent: 25
    Minimum File Size: 4KB
    Exclude Files Stuck in snapshots: true
```

FlexGroupのデータ保護

ONTAP FlexGroupボリュームのデータ保護ワークフローの概要

FlexGroupのSnapMirrorディザスタリカバリ（DR）関係を作成できます。SnapVaultテクノロジを使用したFlexGroupのバックアップとリストアや、バックアップとDRに同じデスティネーションを使用する一元化されたデータ保護関係の作成も可能です。

タスクの内容

SnapMirror関係のタイプは、FlexGroupボリュームの場合は常にです `XDP`。SnapMirror関係によって提供されるデータ保護のタイプは、使用するレプリケーションポリシーによって決まります。作成するレプリケーション関係に必要なタイプのデフォルトポリシーまたはカスタムポリシーを使用できます。

1. クラスタと**SVM**のピアリング

クラスタとSVMのピア関係がまだ確立されていない場合は、とを作成し"クラスタピア""SVMピア"ます。

2. ジョブスケジュールを作成する

SnapMirrorの更新がいつ実行されるかを確認する必要があり"ジョブスケジュールを作成する"ます。

3. データ保護の種類に応じて、次のいずれかの手順を実行します。

- * SnapMirror DRの場合：*

  "SnapMirror関係を作成"関係を作成するときに、タイプがのデフォルトポリシーまたはカスタムポリシーを `async-mirror`選択できます `MirrorAllSnapshots`。

- * SnapMirrorボルトの場合：*

  "SnapMirrorバックアップ関係を作成"関係を作成するときに、タイプがのデフォルトポリシーまたはカスタムポリシーを `vault`選択できます `XDPDefault`。

- 統合データ保護の場合：

  "一元化されたデータ保護関係を作成"関係を作成するときに、タイプがのデフォルトポリシーまたはカスタムポリシーを `mirror-vault`選択できます `MirrorAndVault`。

ONTAP FlexGroupボリュームの**SnapMirror**関係を作成する

ディザスタリカバリ用にデータをレプリケートするために、ピア関係にあるSVMのソースFlexGroupボリュームとデスティネーションFlexGroupボリュームの間にSnapMirror関係を作成できます。災害発生時にFlexGroupボリュームのミラーコピーを使用してデータをリカバリできます。

開始する前に

クラスタピア関係とSVMピア関係を作成しておく必要があります。

"クラスタとSVMのピアリング"

タスクの内容

- ONTAP 9.9.1以降では、ONTAP CLIを使用してFlexGroupボリュームのSnapMirrorカスケード関係およびファンアウト関係を作成できます。詳細については、を参照してください "FlexGroupのSnapMirrorカスケード/ファンアウト関係の作成に関する考慮事項"。
- FlexGroupボリュームには、クラスタ間SnapMirror関係とクラスタ内SnapMirror関係の両方を作成できます。

- ONTAP 9 .3以降では、SnapMirror関係にあるFlexGroupボリュームを拡張できます。

  ONTAP 9.3より前のバージョンのONTAPを使用している場合は、SnapMirror関係の確立後にFlexGroupボリュームを拡張しないでください。ただし、FlexGroupボリュームの容量は、SnapMirror関係の確立後に拡張できます。ONTAP 9.3より前のリリースでSnapMirror関係の解除後にソースFlexGroupボリュームを拡張した場合は、デスティネーションFlexGroupボリュームへのベースライン転送を実行する必要があります。

手順

1. ソースFlexGroupと同じ数のコンスティチュエントで構成されるタイプのデスティネーションFlexGroupボリュームを作成し `DP`ます。

   a. ソースクラスタから、ソースFlexGroupボリュームのコンスティチュエントの数を確認します。
   `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

   b. デスティネーションクラスタから、ソースFlexGroupと同じ数のコンスティチュエントで構成されるタイプのデスティネーションFlexGroupボリュームを作成し `DP`ます。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. デスティネーションクラスタから、デスティネーションFlexGroupボリュームのコンスティチュエントの数を確認します。 `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume        Aggregate    State      Type       Size
Available  Used%
--------- ------------  ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     DP         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     DP         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     DP         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     DP         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     DP         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     DP         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     DP         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     DP         25TB
10.63TB   57%
...
```

2. ジョブスケジュールを作成します。 `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

`-month`オプション、 `-dayofweek`および `-hour`オプションでは、ジョブを毎月、毎日、および1時間ごとに実行するように指定できます `all`。

次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

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

3. SnapMirror関係のタイプがのカスタムポリシーを作成し `async-mirror`ます。 `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

   カスタムポリシーを作成しない場合は、SnapMirror関係にポリシーを指定する必要があります `MirrorAllSnapshots`。

4. デスティネーションクラスタから、ソースFlexGroupボリュームとデスティネーションFlexGroupボリュームの間のSnapMirror関係を作成します。 `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

   FlexGroupボリュームのSnapMirror関係のタイプはである必要があり `XDP`ます。

   FlexGroupのSnapMirror関係のスロットル値を指定した場合、各コンスティチュエントで使用されるスロットル値は同じです。スロットル値はコンスティチュエント間で分配されません。

   FlexGroupボリュームでは、SnapshotのSnapMirrorラベルは使用できません。

   ONTAP 9 .4以前では、コマンドでポリシーが指定されていない場合 `snapmirror create`、`MirrorAllSnapshots`デフォルトでポリシーが使用されます。`ONTAP 9 .5`では、コマンドでポリシーが指定されていない場合 `snapmirror create`、`MirrorAndVault`デフォルトでポリシーが使用されます。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly
Operation succeeded: snapmirror create for the relationship with
destination "vsd:dstFG".
```

5. デスティネーションクラスタから、ベースライン転送を実行してSnapMirror関係を初期化します。 `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   ベースライン転送の完了後は、SnapMirror関係のスケジュールに基づいて定期的にデスティネーションFlexGroupボリュームが更新されます。

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

ONTAP 9.3を実行しているソースクラスタとONTAP 9.2以前を実行しているデスティネーションクラスタの間にSnapMirror関係を作成した場合、ソースFlexGroup FlexGroupボリュームにqtreeを作成するとSnapMirrorの更新が失敗します。この状況からリカバリするには、FlexGroupボリューム内のデフォルト以外のqtreeをすべて削除し、FlexGroupボリュームのqtree機能を無効にしてから、qtree機能が有効になっているSnapshotをすべて削除する必要があります。

終了後

LIFやエクスポートポリシーなどの必要な設定を行って、デスティネーションSVMをデータアクセス用にセットアップする必要があります。

関連情報

- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror policy create"
- "snapmirror update"

ONTAP FlexGroupボリュームの**SnapVault**関係を作成する

SnapVault 関係を設定し、その関係に SnapVault ポリシーを割り当てて、 SnapVault バックアップを作成することができます。

開始する前に

FlexGroup ボリュームの SnapVault 関係の作成に関する考慮事項を確認しておく必要があります。

手順

1. ソースFlexGroupと同じ数のコンスティチュエントで構成されるタイプのデスティネーションFlexGroupボリュームを作成し `DP`ます。
   a. ソースクラスタから、ソースFlexGroupボリュームのコンスティチュエントの数を確認します。
      `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume src* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       src          -            online     RW         400TB
172.86GB  56%
vss       src__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       src__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       src__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       src__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       src__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       src__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       src__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. デスティネーションクラスタから、ソースFlexGroupと同じ数のコンスティチュエントで構成されるタイプのデスティネーションFlexGroupボリュームを作成し `DP`ます。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst

Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. デスティネーションクラスタから、デスティネーションFlexGroupボリュームのコンスティチュエントの数を確認します。 `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dst* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     RW         400TB
172.86GB  56%
vsd       dst__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dst__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dst__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dst__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dst__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dst__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dst__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. ジョブスケジュールを作成します。 `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

> `-dayofweek`、および `-hour`では `-month`、ジョブを毎月、曜日、および時間ごとに実行するように指定できます `all`。

次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

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

3. SnapVault ポリシーを作成し、 SnapVault ポリシーのルールを定義します。

   a. SnapVault関係のタイプがのカスタムポリシーを作成し `vault`ます。 `snapmirror policy create -vserver svm_name -policy policy_name -type vault`

   b. 初期化処理と更新処理の際にどのSnapshotを転送するかを決定するSnapVaultポリシーのルールを定義します。 `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

カスタムポリシーを作成しない場合は、SnapVault関係にポリシーを指定する必要があります

XDPDefault。

4. SnapVault関係を作成します。 `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

   ONTAP 9 .4以前では、コマンドでポリシーが指定されていない場合 `snapmirror create`、`MirrorAllSnapshots`デフォルトでポリシーが使用されます。`ONTAP 9 .5`では、コマンドでポリシーが指定されていない場合 `snapmirror create`、`MirrorAndVault`デフォルトでポリシーが使用されます。

   ```
   cluster2::> snapmirror create -source-path vss:srcFG -destination-path
   vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
   ```

   の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

5. デスティネーションクラスタから、ベースライン転送を実行してSnapVault関係を初期化します。 `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror initialize -destination-path vsd:dst
   Operation is queued: snapmirror initialize of destination "vsd:dst".
   ```

関連情報

- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror policy add-rule"
- "snapmirror policy create"

ONTAP FlexGroupボリュームの一元化されたデータ保護関係を作成する

ONTAP 9 3以降では、SnapMirrorの一元化されたデータ保護関係を作成して設定し、同じデスティネーションボリュームでディザスタリカバリとアーカイブを設定できます。

開始する前に

FlexGroupボリュームの一元化されたデータ保護関係の作成に関する考慮事項を確認しておく必要があります。

"FlexGroupのSnapVaultバックアップ関係および一元化されたデータ保護関係の作成に関する考慮事項"

手順

1. ソースFlexGroupと同じ数のコンスティチュエントで構成されるタイプのデスティネーションFlexGroupボリュームを作成し`DP`ます。

   a. ソースクラスタから、ソースFlexGroupボリュームのコンスティチュエントの数を確認します。
      `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume         Aggregate    State      Type       Size
Available  Used%
--------- ------------   ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. デスティネーションクラスタから、ソースFlexGroupと同じ数のコンスティチュエントで構成されるタイプのデスティネーションFlexGroupボリュームを作成し `DP`ます。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. デスティネーションクラスタから、デスティネーションFlexGroupボリュームのコンスティチュエントの数を確認します。 `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     RW         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. ジョブスケジュールを作成します。 `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   `-month`オプション、 `-dayofweek`および `-hour`オプションでは、ジョブを毎月、毎日、および1時間ごとに実行するように指定できます `all`。

   次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

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

3. タイプがのカスタムポリシーを作成し `mirror-vault`、ミラーとバックアップポリシーのルールを定義します。

   a. 一元化されたデータ保護関係用のタイプのカスタムポリシーを作成し `mirror-vault`ます。 `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`

   b. 初期化処理と更新処理の際にどのSnapshotを転送するかを決定する、ミラーとバックアップポリシーのルールを定義します。 `snapmirror policy add-rule -vserver svm_name -policy`

```
policy_for_rule - snapmirror-label snapmirror-label -keep retention_count
-schedule schedule
```

カスタムポリシーを指定しない場合、その `MirrorAndVault`ポリシーは一元化されたデータ保護関係に使用されます。

4. 一元化されたデータ保護関係を作成します。 `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

   ONTAP 9 .4以前では、コマンドでポリシーが指定されていない場合 `snapmirror create`、`MirrorAllSnapshots`デフォルトでポリシーが使用されます。`ONTAP 9 .5`では、コマンドでポリシーが指定されていない場合 `snapmirror create`、`MirrorAndVault`デフォルトでポリシーが使用されます。

   ```
   cluster2::> snapmirror create -source-path vss:srcFG -destination-path
   vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
   ```

   の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

5. デスティネーションクラスタから、ベースライン転送を実行して一元化されたデータ保護関係を初期化します。 `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror initialize -destination-path vsd:dstFG
   Operation is queued: snapmirror initialize of destination "vsd:dstFG".
   ```

関連情報

- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror policy add-rule"
- "snapmirror policy create"

ONTAP FlexGroupのSVMディザスタリカバリ関係を作成する

ONTAP 9.9.1以降では、FlexGroupボリュームを使用してSVMディザスタリカバリ（SVM DR）関係を作成できます。SVM DR関係は、SVMの設定とそのデータを同期およびレプリケートすることで冗長性を確保し、災害発生時にFlexGroupボリュームをリカバリする機能を提供します。SVM DRにはSnapMirrorライセンスが必要です。

開始する前に

次の条件に該当する場合は、FlexGroup SVM DR関係を作成できません。

- FlexClone FlexGroup構成が存在する
- FlexGroupボリュームがカスケード関係の一部である
- FlexGroupボリュームはファンアウト関係の一部であり、クラスタでONTAP 9よりも前のバージョン

のONTAPが実行されている。12.1（ONTAP 9.13.1以降では、ファンアウト関係がサポートされます）。

タスクの内容

- 両方のクラスタのすべてのノードで、ONTAP 9 DRがサポートされるノード（SVM.9.1以降）と同じバージョンのONTAPが実行されている必要があります。
- プライマリサイトとセカンダリサイトの間のSVM DR関係が健全であり、プライマリとセカンダリの両方のSVMにFlexGroupボリュームをサポートする十分なスペースが必要です。
- ONTAP 9 12.1以降では、FabricPool、FlexGroup、およびSVM DRを連動させることができます。ONTAP 9 12.1より前のリリースでは、これらの機能のいずれか2つが連携して動作しましたが、3つすべてが連携して動作するわけではありませんでした。
- ファンアウト関係の一部であるFlexGroup SVM DR関係を作成する場合FlexGroupは、次の要件に注意してください。
  - ソースクラスタとデスティネーションクラスタでONTAP 9 .13.1以降が実行されている必要があります。
  - FlexGroupを備えたSVM DRでは、8サイトへのSnapMirrorファンアウト関係がサポートされます。

SVM DR関係の作成については、を参照してください"SnapMirror SVMレプリケーションを管理します。"。

手順

1. SVM DR関係を作成するか、既存の関係を使用します。

   "SVMの設定全体をレプリケートする"

2. 必要な数のコンスティチュエントを含むFlexGroupボリュームをプライマリサイトに作成します。

   "FlexGroupボリュームの作成"です。

   FlexGroupとそのすべてのコンスティチュエントが作成されるまで待ってから、処理を続行してください。

3. FlexGroupボリュームをレプリケートするには、セカンダリサイトでSVMを更新します。 `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

   スケジュールされたSnapMirror更新がすでに存在するかどうかを確認するには、次のように入力します。 `snapmirror show -fields schedule`

4. セカンダリサイトで、SnapMirror関係が正常であることを確認します。 `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                  Idle           -         true    -
```

5. セカンダリサイトで、新しいFlexGroupボリュームとそのコンスティチュエントが存在することを確認します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                    Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                             Snapmirrored
                                    Idle           -         true    -
6 entries were displayed.
```

関連情報

- "snapmirror show"
- "snapmirror update"

ONTAP FlexGroup SnapMirror関係をSVM DRに移行

既存のFlexGroup SnapMirror関係を移行することで、FlexGroup SVM DR関係を作成できます。

開始する前に

- FlexGroup Volume SnapMirror関係は正常な状態です。
- ソースとデスティネーションのFlexGroupボリュームの名前が同じです。

手順

1. SnapMirrorデスティネーションから、FlexGroupレベルのSnapMirror関係を再同期します。 `snapmirror resync`
2. FlexGroup SVM DR SnapMirror関係を作成FlexGroup VolumeのSnapMirror関係に設定されているのと同じSnapMirrorポリシーを使用します。 `snapmirror create -destination-path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`

   > レプリケーション関係を作成するときは、コマンドのオプションを `snapmirror create`使用する必要があります `-identity-preserve true`。

   の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

3. 関係が解除されていることを確認します。 `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:


Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
fg_vs:        XDP  fg_vs1_renamed:     Broken-off
                                      Idle           -         true    -
```

4. デスティネーションSVMを停止します。 `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. SVM SnapMirror関係を再同期します。 `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. SVM DRレベルのSnapMirror関係が健全なアイドル状態になっていることを確認します。 `snapmirror`

`show -expand`

7. FlexGroup SnapMirror関係が健全な状態であることを確認します。 `snapmirror show`

関連情報

- "スナップミラー作成"
- "snapmirror resync"
- "snapmirror show"

ONTAP FlexVolボリュームを**SVM-DR**関係内の**FlexGroup**ボリュームに変換する

SVM.10.1以降でONTAP 9は、FlexVol volumeをSVM-DRソースのFlexGroupボリュームに変換できます。

開始する前に

- 変換するFlexVol volumeがオンラインになっている必要があります。
- FlexVol volumeの処理と設定は、変換プロセスと互換性がある必要があります。

  FlexVol volumeに互換性がない場合にボリュームの変換がキャンセルされると、エラーメッセージが生成されます。対処方法を実行してから変換を再試行できます。詳細については、を参照してください。"FlexVolボリュームをFlexGroupボリュームに変換する場合の考慮事項"

手順

1. advanced権限モードでログインします。 `set -privilege advanced`
2. デスティネーションから、SVM-DR関係を更新します。

```
snapmirror update -destination-path <destination_svm_name>: -source-path
<source_svm_name>:
```

   オプションで、SVM名のあとにコロン（：）を入力する必要があります `-destination-path` 。

3. SVM-DR関係がSnapMirrored状態であり、Broken-offになっていないことを確認します。

```
snapmirror show
```

4. デスティネーションSVMから、FlexVol volumeを変換する準備が完了していることを確認します。

```
volume conversion start -vserver <svm_name> -volume <vol_name> -check
-only true
```

   このコマンドで「This is a destination SVMDR volume」以外のエラーが生成された場合は、適切に対処してコマンドを再度実行し、変換を続行できます。

5. デスティネーションから、SVM-DR関係の転送を無効にします。

```
snapmirror quiesce -destination-path <dest_svm>:
```

> オプションで、SVM名のあとにコロン（：）を入力する必要があります `-destination-path` 。

6. ソースクラスタから、変換を開始します。

```
volume conversion start -vserver <svm_name> -volume <vol_name>
```

7. 変換が正常に完了したことを確認します。

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state    volume-style-extended
-------  ---------  ------   ---------------------
vs0      my_volume  online   flexgroup
```

8. デスティネーション クラスタから、関係の転送を再開します。

```
snapmirror resume -destination-path <dest_svm>:
```

> オプションで、SVM名のあとにコロン（：）を入力する必要があります `-destination-path` 。

9. デスティネーション クラスタから更新を実行して、デスティネーションに変換を反映します。

```
snapmirror update -destination-path <dest_svm>:
```

> オプションで、SVM名のあとにコロン（：）を入力する必要があります `-destination-path` 。

10. SVM-DR関係がSnapMirroredの状態で、解除されていないことを確認します。

```
snapmirror show
```

11. デスティネーションで変換が行われたことを確認します。

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state   volume-style-extended
-------  -------    ------  ---------------------
vs0_dst  my_volume  online  flexgroup
```

関連情報

- "snapmirror resume"
- "スナップミラーの静止"
- "snapmirror show"
- "snapmirror update"

ONTAP FlexGroupのSnapMirrorカスケード/ファンアウト関係の作成に関する考慮事項

FlexGroupボリュームのSnapMirrorカスケード/ファンアウト関係を作成するときは、サポートに関する考慮事項と制限事項に注意する必要があります。

カスケード関係の作成に関する考慮事項

- 各関係は、クラスタ間関係またはクラスタ内関係のいずれかになります。
- 両方の関係で、async-mirror、mirror-vault、vaultを含むすべての非同期ポリシータイプがサポートされます。
- サポートされる非同期ミラーポリシーは「MirrorAllSnapshots」のみで、「MirrorLatest」はサポートされません。
- 長期保存スナップショットはサポートされていません。

  詳細はこちら"長期保存スナップショット"。

- カスケードXDP関係の同時更新がサポートされます。
- AからBへ、BからCへの削除、およびAからCへの再同期、またはCからAへの再同期をサポートします。
- すべてのノードでONTAP 9 .9.1以降が実行されている場合、AとBのFlexGroupボリュームもファンアウトをサポートします。
- BまたはCのFlexGroupボリュームからのリストア処理がサポートされます。
- デスティネーションがリストア関係のソースである間は、FlexGroup関係を転送することはできません。
- FlexGroupリストアのデスティネーションを他のFlexGroup関係のデスティネーションにすることはできません。
- FlexGroupファイルのリストア処理には、通常のFlexGroupリストア処理と同じ制限事項があります。

- クラスタ内のBとCのFlexGroupボリュームが配置されているすべてのノードで、ONTAP 9 .9.1以降が実行されている必要があります。
- すべての拡張機能と自動拡張機能がサポートされています。
- A対B対Cのカスケード構成で、A対BとB対CのコンスティチュエントSnapMirror関係の数が異なる場合、B対CのSnapMirror関係でソースから中止処理を実行することはできません。
- System Managerでは、ONTAPのバージョンに関係なくカスケード関係はサポートされません。
- AからBへのFlexVol関係のセットをFlexGroup関係に変換する場合は、最初にBからCへのホップを変換する必要があります。
- RESTでサポートされるポリシータイプを使用する関係のすべてのFlexGroupカスケードFlexGroup構成は、REST APIでもサポートされます。
- FlexVol関係と同様に、FlexGroupカスケードはコマンドではサポートされません `snapmirror protect`。

ファンアウト関係の作成に関する考慮事項

- AからB、AからCなど、最大8つのFlexGroupファンアウト関係がサポートされます。
- 各関係には、クラスタ間またはクラスタ内のどちらかを設定できます。
- 2つの関係で同時更新がサポートされます。
- すべての拡張機能と自動拡張機能がサポートされています。
- ファンアウト関係でコンスティチュエントSnapMirror関係の数が異なる場合、AとBおよびAとCの関係でソースから中止処理を実行することはできません。
- クラスタ内のソースとデスティネーションのFlexGroupボリュームが格納されているすべてのノードで、ONTAP 9.9.1以降が実行されている必要があります。
- ファンアウト関係では、FlexGroup SnapMirrorで現在サポートされているすべての非同期ポリシータイプがサポートされます。
- BからCのFlexGroupボリュームへのリストア処理を実行できます。
- RESTでサポートされるポリシータイプを使用するすべてのファンアウト構成は、FlexGroupファンアウト構成のREST APIでもサポートされます。

関連情報

- "SnapMirror保護"

ONTAP FlexGroupの SnapVault**バックアップ関係および一元化されたデータ保護関係の作成に関する考慮事項**

FlexGroupボリュームのSnapVaultバックアップ関係と一元化されたデータ保護関係の作成に関する考慮事項を確認しておく必要があります。

- SnapVaultバックアップ関係および一元化されたデータ保護関係を再同期するには、最新の共通のSnapshotよりも新しいSnapshotをデスティネーションボリュームに保持するオプションを使用し `-preserve`ます。
- FlexGroupボリュームでは長期保持はサポートされません。

  長期保持を使用すると、ソースボリュームにSnapshotを格納することなく、デスティネーションボリュー

ムにSnapshotを直接作成できます。

- コマンド `expiry-time`オプションは `snapshot`FlexGroupボリュームではサポートされません。
- SnapVaultバックアップ関係および一元化されたデータ保護関係のデスティネーションFlexGroupでは、Storage Efficiencyを設定できません。
- FlexGroupボリュームのSnapVaultバックアップ関係および一元化されたデータ保護関係のSnapshotの名前は変更できません。
- 1つのFlexGroupボリュームをソースボリュームにできるのは、1つのバックアップ関係またはリストア関係だけです。

  2つのSnapVault関係、2つのリストア関係、またはSnapVaultバックアップ関係とリストア関係のソースにすることはできませんFlexGroup。

- ソースFlexGroupボリュームでSnapshotを削除して同じ名前のSnapshotを再作成した場合、デスティネーションFlexGroupボリュームに同じ名前のSnapshotがあると、デスティネーションボリュームへの次回の更新転送は失敗します。

  これは、FlexGroupボリュームのSnapshotの名前を変更できないためです。

ONTAP FlexGroupボリュームのSnapMirrorデータ転送の監視

FlexGroup Volume SnapMirror関係のステータスを定期的に監視して、デスティネーションFlexGroupボリュームが指定したスケジュールに従って定期的に更新されていることを確認する必要があります。

タスクの内容

このタスクはデスティネーションクラスタで実行する必要があります。

手順

1. すべてのFlexGroupボリューム関係のSnapMirror関係ステータスを表示します。 `snapmirror show -relationship-group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:d        Snapmirrored
                                 Idle           -         true    -
vss:s2      XDP  vsd:d2       Uninitialized
                                 Idle           -         true    -
2 entries were displayed.
```

関連情報

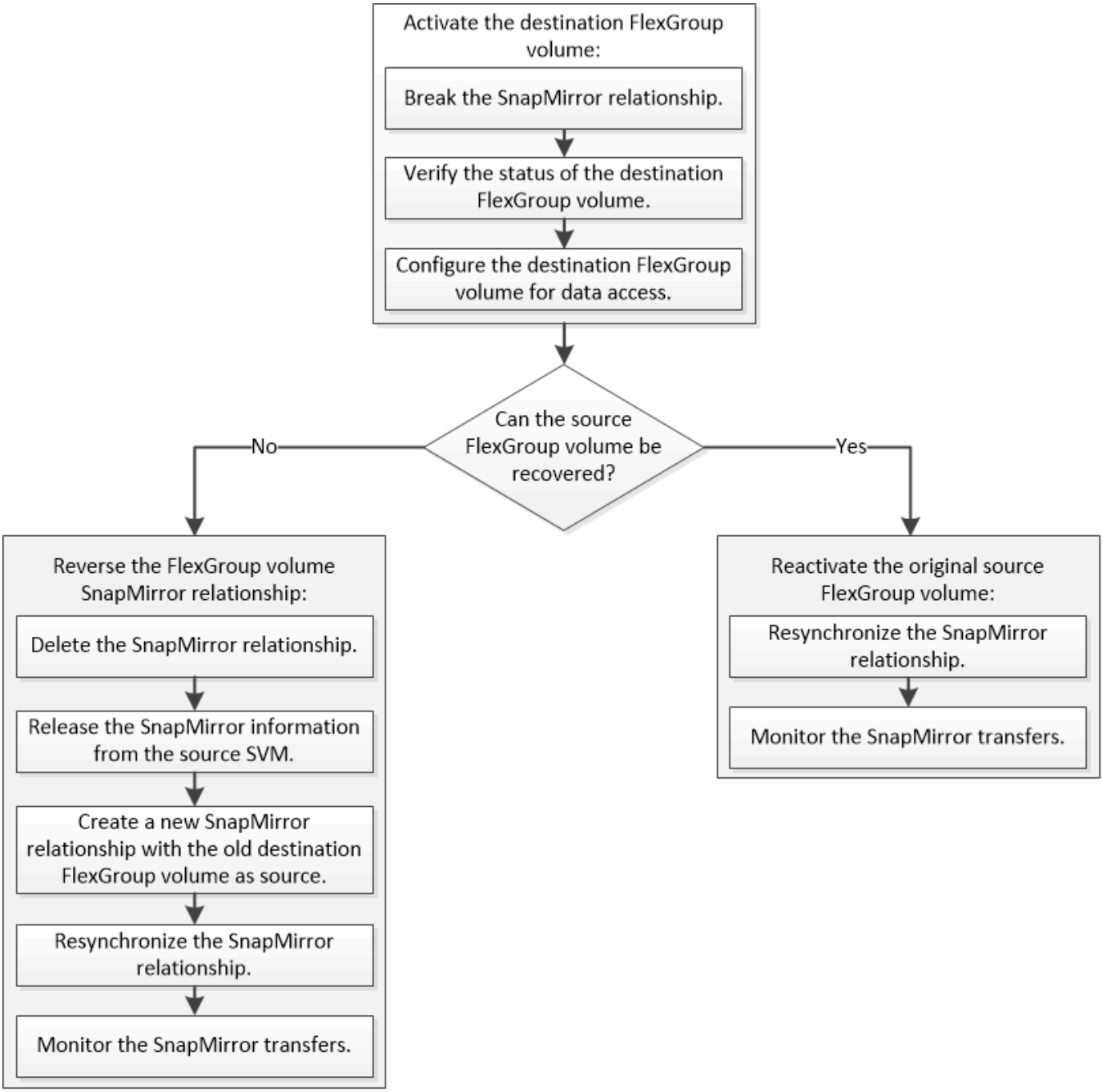
- "snapmirror show"

FlexGroupボリュームのデータ保護処理を管理します。

FlexGroupノテイサスタリカハリ

ONTAP FlexGroupノテイサスタリカハリノワクフロ

ソース FlexGroup ボリュームで災害が発生した場合は、デスティネーション FlexGroup をアクティブ化してクライアントアクセスをリダイレクトします。ソース FlexGroup ボリュームをリカバリできるかどうかに応じて、ソース FlexGroup ボリュームを再アクティブ化するか、 SnapMirror 関係を反転させる必要があります。



タスクの内容

SnapMirror の解除と再同期など、一部の SnapMirror 処理の実行中は、デスティネーション FlexGroup ボリュームへのクライアントアクセスが一時的にブロックされます。SnapMirror 処理に失敗した場合、一部のコンスティチュエントがその状態のまま残り、 FlexGroup ボリュームへのアクセスが拒否されることがあります。このような場合は、 SnapMirror 処理を再試行する必要があります。

デスティネーション**ONTAP FlexGroup**ボリュームをアクティブ化

データが破損した場合や誤って削除した場合、あるいはオフライン状態の場合など、データをソース FlexGroup から提供できないときは、ソース FlexGroup ボリュームのデータをリカバリするまでの間、デスティネーション FlexGroup ボリュームをアクティブ化してデータアクセスを提供する必要があります。アクティブ化には、以降の SnapMirror

データ転送の中止と、 SnapMirror 関係の解除が伴います。

タスクの内容

このタスクはデスティネーションクラスタで実行する必要があります。

手順

1. FlexGroup Volume SnapMirror関係の以降の転送を無効にします。 `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. FlexGroup Volume SnapMirror関係を解除します。 `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. SnapMirror関係のステータスを表示します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Broken-off
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Broken-off
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Broken-off
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Broken-off
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Broken-off
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Broken-off
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Broken-off
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Broken-off
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Broken-off
                                    Idle           -         true    -
...
```

各コンスティチュエントのSnapMirror関係のステータスはです `Broken-off`。

4. デスティネーションFlexGroupボリュームが読み取り/書き込み可能であることを確認します。 `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     **RW**          2GB
1.54GB   22%
vsd       d2           -            online     DP           2GB
1.55GB   22%
vsd       root_vs0     aggr1        online     RW         100MB
94.02MB    5%
3 entries were displayed.
```

5. デスティネーション FlexGroup ボリュームにクライアントをリダイレクトします。

関連情報

- "スナップミラーの破損"
- "スナップミラーの静止"
- "snapmirror show"

災害後の元のソース**ONTAP FlexGroup**ボリュームの再アクティブ化

ソース FlexGroup ボリュームが使用可能になったら、元のソース FlexGroup ボリュームと元のデスティネーション ボリュームを再同期できます。デスティネーション FlexGroup ボリュームの新しいデータはすべて失われます。

タスクの内容

再同期が実行される前に、デスティネーションボリュームのアクティブなクォータルールは非アクティブ化され、削除されます。

再同期処理の完了後に、コマンドと `volume quota modify`コマンドを使用してクォータルールを作成し、再アクティブ化できます `volume quota policy rule create`。

手順

1. デスティネーションクラスタから、FlexGroup Volume SnapMirror関係を再同期します。 `snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. SnapMirror関係のステータスを表示します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Snapmirrored
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Snapmirrored
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Snapmirrored
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Snapmirrored
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Snapmirrored
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Snapmirrored
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Snapmirrored
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Snapmirrored
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Snapmirrored
                                    Idle           -         true    -
...
```

各コンスティチュエントのSnapMirror関係のステータスはです `Snapmirrored`。

関連情報

- "snapmirror resync"
- "snapmirror show"

ディザスタリカバリ時の**ONTAP FlexGroup**ボリューム間の**SnapMirror**関係の反転

災害によって SnapMirror 関係のソース FlexGroup が機能しなくなった場合、ソース FlexGroup ボリュームの修理や交換を行う間、デスティネーション FlexGroup ボリュームを使用してデータを提供できます。ソース FlexGroup ボリュームがオンラインになったら、元のソース FlexGroup ボリュームを読み取り専用のデスティネーションにして、SnapMirror 関係を反転できます。

タスクの内容

再同期が実行される前に、デスティネーションボリュームのアクティブなクォータルールは非アクティブ化さ

れ、削除されます。

再同期処理の完了後に、コマンドと `volume quota modify`コマンドを使用してクォータルールを作成し、再アクティブ化できます `volume quota policy rule create`。

手順

1. 元のデスティネーションFlexGroupボリュームで、ソースFlexGroupボリュームとデスティネーションFlexGroupボリュームの間のデータ保護ミラー関係を削除します。 `snapmirror delete -destination-path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. 元のソースFlexGroupボリュームで、ソースFlexGroupボリュームから関係の情報を削除します。 `snapmirror release -destination-path svm_name:volume_name -relationship-info -only`

   SnapMirror 関係を削除したあと、再同期処理を実行する前に、ソース FlexGroup ボリュームから関係の情報を削除する必要があります。

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship -info-only true
```

3. 新しいデスティネーションFlexGroupで、ミラー関係を作成します。 `snapmirror create -source -path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path vss:src -type XDP -policy MirrorAllSnapshots
```

   の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

4. 新しいデスティネーションFlexGroupボリュームで、ソースFlexGroupを再同期します。 `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. SnapMirror転送を監視します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vsd:dst       XDP  vss:src        Snapmirrored
                                      Idle           -         true    -
vss:dst__0001 XDP  vss:src__0001  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0002 XDP  vss:src__0002  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0003 XDP  vss:src__0003  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0004 XDP  vss:src__0004  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0005 XDP  vss:src__0005  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0006 XDP  vss:src__0006  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0007 XDP  vss:src__0007  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0008 XDP  vss:src__0008  Snapmirrored
                                      Idle           -         true    -
...
```

各コンスティチュエントのSnapMirror関係のステータスがになり、再同期が成功したことが示さ`Snapmirrored`れます。

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーリリース"
- "snapmirror resync"
- "snapmirror show"

SnapMirror関係にある**FlexGroup**ボリュームの拡張

SnapMirror関係にある**ONTAP FlexGroup**ボリュームの拡張

ONTAP 9 3以降では、新しいコンスティチュエントをボリュームに追加すること

で、SnapMirror関係にあるソースFlexGroupボリュームとデスティネーションFlexGroupボリュームを拡張できます。デスティネーションボリュームは、手動または自動で拡張できます。

タスクの内容

- 拡張後、SnapMirror関係のソースFlexGroupボリュームとデスティネーションFlexGroupボリュームでコンスティチュエントの数が一致している必要があります。

  ボリュームのコンスティチュエントの数が一致しないと、SnapMirror転送は失敗します。

- 拡張プロセスの実行中はSnapMirror処理を実行しないでください。
- 拡張プロセスが完了する前に災害が発生した場合は、SnapMirror関係を解除し、処理が成功するまで待つ必要があります。

> 拡張プロセスの実行中にSnapMirror関係を解除するのは、災害が発生した場合のみにしてください。災害が発生した場合の解除処理にはしばらく時間がかかることがあります。解除処理が完了してから再同期処理を実行するようにしてください。解除処理が失敗した場合は、解除処理を再試行する必要があります。解除処理に失敗した場合、一部の新しいコンスティチュエントがデスティネーションFlexGroupボリュームに残る可能性があります。処理を進める前に、それらのコンスティチュエントを手動で削除することを推奨します。

SnapMirror関係のソース**ONTAP FlexGroup**ボリュームの拡張

ONTAP 9 3以降では、ソースボリュームに新しいコンスティチュエントを追加することで、SnapMirror関係のソースFlexGroupボリュームを拡張できます。通常のFlexGroupボリューム（読み書き可能ボリューム）と同じ方法でソースボリュームを拡張できます。

手順

1. ソースFlexGroupボリュームを拡張します。 `volume expand -vserver vserver_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src

Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
Partial Snapshot copies cannot be restored.
Do you want to continue? {y|n}: Y
[Job 146] Job succeeded: Successful
```

ボリュームの拡張前に作成されたすべてのSnapshotの状態がpartialに変わります。

デスティネーション FlexGroup ボリュームの拡張と SnapMirror 関係の再確立は、自動または手動で実行できます。デフォルトでは、 SnapMirror 関係は自動拡張用に設定されており、ソースボリュームが拡張されるとデスティネーション FlexGroup ボリュームも自動的に拡張されます。

開始する前に

- ソース FlexGroup ボリュームが拡張されている必要があります。
- SnapMirror関係は状態である必要があり `SnapMirrored`ます。

  SnapMirror 関係が解除または削除されていない必要があります。

タスクの内容

- デスティネーション FlexGroup ボリュームを作成すると、そのボリュームにはデフォルトで自動拡張が設定されます。

  必要に応じて、デスティネーション FlexGroup ボリュームを手動拡張に変更できます。

  デスティネーション FlexGroup ボリュームは自動的に拡張することを推奨します。

- ソースの FlexGroup ボリュームとデスティネーションの FlexGroup ボリュームの拡張が完了し、コンスティチュエントの数が同じになるまでは、すべての SnapMirror 処理が失敗します。
- SnapMirror 関係を解除または削除したあとにデスティネーション FlexGroup ボリュームを拡張した場合、元の関係を再同期することはできません。

  デスティネーションFlexGroupボリュームを再利用する場合は、SnapMirror関係の削除後にボリュームを拡張しないでください。

選択肢

- 更新の転送を実行し、デスティネーション FlexGroup ボリュームを自動的に拡張します。

  a. SnapMirror更新の転送を実行します。 `snapmirror update -destination-path svm:vol_name`

  b. SnapMirror関係のステータスが状態になっていることを確認し `SnapMirrored`ます。 `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                             Snapmirrored
                                     Idle           -         true
-
```

アグリゲートのサイズと可用性に基づいてアグリゲートが自動的に選択され、ソース FlexGroup のコンスティチュエントに一致する新しいコンスティチュエントがデスティネーション FlexGroup ボリュームに追加されます。拡張の完了後、再同期処理が自動的に開始されます。

- デスティネーション FlexGroup ボリュームを手動で拡張します。
  a. SnapMirror関係が自動拡張モードの場合は、SnapMirror関係を手動拡張モードに設定します。 `snapmirror modify -destination-path svm:vol_name -is-auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

  b. SnapMirror関係を休止します。 `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

  c. デスティネーションFlexGroupボリュームを拡張します。 `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2  -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

d. SnapMirror関係を再同期します。 `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

e. SnapMirror関係のステータスがになっていることを確認し `SnapMirrored`ます。 `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

関連情報

- "スナップミラーの静止"
- "snapmirror resync"
- "snapmirror show"

ONTAP FlexGroupボリュームから**SnapMirror**単一ファイルのリストアを実行する

ONTAP 9 .8以降では、FlexGroup SnapMirrorボルトまたはUDPデスティネーションから単一ファイルをリストアできます。

タスクの内容

- 任意のジオメトリのFlexGroupボリュームから任意のジオメトリのFlexGroupボリュームに復元できます。
- 復元操作ごとに 1 つのファイルのみがサポートされます。
- 元のソースFlexGroupボリュームまたは新しいFlexGroupボリュームに復元できます。
- リモートフェンシングされたファイルの検索はサポートされていません。

  ソースファイルがフェンシングされている場合、単一ファイルのリストアは失敗します。

- 中止された単一ファイルの復元を再開またはクリーンアップできます。
- 失敗した単一ファイル復元転送をクリーンアップするには、 `clean-up-failure`オプションの `snapmirror restore`指示。

  の詳細については `snapmirror restore`、を"ONTAPコマンド リファレンス"参照してください。

- FlexGroupボリュームの拡張は、 FlexGroup の単一ファイルのリストアが進行中または中止された状態にあるときにサポートされます。

手順

1. FlexGroupボリュームからファイルをリストアします。 `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

   次に、FlexGroupの単一ファイルのリストア処理の例を示します。

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path
vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-
d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631.
vserverA::> snapmirror show

Source              Destination Mirror   Relationship
Total Last
Path       Type   Path            State    Status           Progress
Healthy Updated
---------- ----      ------------     -------    ---------
----- --------- ------- --------
vs0:v1d RST    vs0:v2          -           Transferring Idle 83.12KB
true 09/19 11:38:42

vserverA::*> snapmirror show vs0:fg2

Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
```

```
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
```

```
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

関連情報

- "snapmirror show"

SnapVaultバックアップからの**ONTAP FlexGroup**ボリュームのリストア

SnapVaultセカンダリボリューム内のSnapshotからFlexGroupボリュームのフルリストア処理を実行できます。FlexGroupボリュームは元のソースボリュームまたは新しいFlexGroupボリュームにリストアできます。

開始する前に

FlexGroupのSnapVaultバックアップからリストアする場合は、一定の考慮事項に注意する必要があります。

- SnapVaultバックアップからの部分Snapshotでサポートされるのはベースラインリストアのみです。デスティネーションボリュームのコンスティチュエントの数は、Snapshotの作成時にソースボリュームのコンスティチュエントの数と一致している必要があります。
- リストア処理に失敗した場合、リストア処理が完了するまでは他の処理を実行できなくなります。リストア処理を再試行するか、パラメータを指定してリストア処理を実行します `cleanup`。
- 1つのFlexGroupボリュームをソースボリュームにできるのは、1つのバックアップ関係またはリストア関係だけです。2つのSnapVault関係、2つのリストア関係、またはSnapVault関係とリストア関係のソースにすることはできませんFlexGroup。
- SnapVaultのバックアップ処理とリストア処理を並行して実行することはできません。ベースラインリストア処理または増分リストア処理の実行中は、バックアップ処理を休止する必要があります。
- 部分的なSnapshotのリストア処理は、デスティネーションFlexGroupボリュームから中止する必要があり

ます。ソースボリュームから部分的なSnapshotのリストア処理を中止することはできません。

- リストア処理を中止する場合は、前回のリストア処理と同じSnapshotを使用してリストア処理を再開する必要があります。

タスクの内容

デスティネーションFlexGroupボリュームのアクティブなクォータルールは、リストアの実行前に非アクティブ化されます。

コマンドを使用すると、リストア処理の完了後にクォータルールを再アクティブ化できます `volume quota modify`。

手順

1. Restore the FlexGroup Volume： `snapmirror restore -source-path` *`src_svm:src_flexgroup`* `-destination-path` *`dest_svm:dest_flexgroup`* `-snapshot` *`snapshot_name`* `snapshot_name`ソースボリュームからデスティネーションボリュームにリストアするSnapshotです。Snapshotを指定しない場合、デスティネーションボリュームは最新のSnapshotからリストアされます。

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

関連情報

- "スナップミラー復元"

ONTAP FlexGroupボリュームでの**SVM**保護の無効化

FlexGroupボリュームでSVM DRフラグがに設定されている場合は `protected`、フラグをunprotectedに設定してFlexGroupボリュームでSVM DRを無効にすることができます `protection`。

開始する前に

- プライマリとセカンダリの間のSVM DR関係が正常な状態である。
- SVM DR保護パラメータがに設定されている `protected`。

手順

1. コマンドを使用してFlexGroupボリュームのパラメータをに `unprotected`変更し `vserver-dr-protection`、保護を無効にし `volume modify`ます。

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. セカンダリサイトでSVMを更新します。 `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. SnapMirror関係が正常であることを確認します。 `snapmirror show`
4. FlexGroup SnapMirror関係が削除されたことを確認します。 `snapmirror show -expand`

関連情報

- "snapmirror show"
- "snapmirror update"

ONTAP FlexGroupボリュームで**SVM**保護を有効にする

FlexGroupボリュームでSVM DR保護フラグがに設定されている場合は `unprotected`、フラグをに設定してSVM DR保護を有効にすることができます `protected`。

開始する前に

- プライマリとセカンダリの間のSVM DR関係が正常な状態である。
- SVM DR保護パラメータがに設定されている `unprotected`。

手順

1. を使用してFlexGroupボリュームのパラメータをに `protected`変更し `vserver-dr-protection`、保護を有効にし `volume modify`ます。

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. セカンダリサイトでSVMを更新します。 `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. SnapMirror関係が正常であることを確認します。 `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                  Idle           -         true    -
```

4. FlexGroup SnapMirror関係が正常であることを確認します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                  Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                              Snapmirrored
                                  Idle           -         true    -
6 entries were displayed.
```

関連情報

- "snapmirror show"

FlexVolボリュームからFlexGroupボリュームへの変換

ONTAP FlexVolボリュームからFlexGroupボリュームへの変換について

FlexVol volumeをスペース制限を超えて拡張する場合は、FlexVol volumeをFlexGroupボリュームに変換できます。ONTAP 9 .7以降では、スタンドアロンのFlexVolボリュームまたはSnapMirror関係にあるFlexVolボリュームをFlexGroupボリュームに変換できます。

FlexVolボリュームをFlexGroupボリュームに変換する場合の考慮事項

知っておくべき"サポートされている機能と操作" FlexVolボリュームをFlexGroupボリュームに変換する前に、次の点を確認してください。

変換中にサポートされない処理

ボリューム変換の実行中は、次の処理は実行できません。

- ボリューム移動
- アグリゲートの再配置
- ハイアベイラビリティ構成での計画的なテイクオーバーとギブバック
- ハイアベイラビリティ構成での手動および自動のギブバック
- クラスタのアップグレードとリバート
- FlexCloneボリュームをスプリット
- ホリユウムノリホスト
- ボリュームの変更とオートサイズ
- ボリュームの名前変更
- アグリゲートへのオブジェクトストアの接続
- MetroCluster構成でのネゴシエートスイッチオーバー
- SnapMirrorの処理
- Snapshotカラノリストア
- クォータの処理
- ストレージ効率化の処理

これらの処理は、変換が成功したあとにFlexGroupボリュームに対して実行できます。

FlexGroupでサポートされない構成

- オフラインまたは制限状態のボリューム
- SVMルートボリューム
- SAN
- SMB 1.0
- NVMeネエムスヘエス
- リモートのボリュームシャドウコピーサービス（VSS）

ONTAP FlexVolボリュームからONTAP FlexGroupボリュームへの変換

ONTAP 9 .7以降では、FlexVol volumeからFlexGroupボリュームへのインプレース変換を実行できます。データコピーや追加のディスクスペースは必要ありません。

開始する前に

- ONTAP 9.8以降では、移行したボリュームをFlexGroupボリュームに変換できます。
- 変換するFlexVol volumeがオンラインになっている必要があります。
- FlexVol volumeの処理と設定は、変換プロセスと互換性がある必要があります。

  変換が正常に行われない可能性がある次の条件を確認します。

  - FlexVolボリュームは、7MTT（ONTAP 9.7）を使用して7-Modeから移行されました。

    ONTAP 9.8以降では、移行したボリュームを変換できます。

  - ボリューム上で、FlexGroup ボリュームでまだサポートされていないものが有効になっています。たとえば、SAN LUN、Windows NFS、SMB1、スナップショット命名/自動削除、vmalign セット、ONTAP 9.11.1 より前のリリースの SnapLock (SnapLock は ONTAP 9.11.1 以降でサポートされています)、スペース SLO、論理スペース強制/レポートなどです。詳細については、を参照してください "FlexGroupボリュームでサポートされる構成とサポートされない構成"。
  - 変換するFlexVolボリュームが配置されているSVMが現在SVM DRを使用しています。
  - NetApp FlexCloneボリュームが存在し、FlexVolボリュームが親ボリュームです。変換対象のボリュームを親またはクローンにすることはできません。
  - ボリュームがNetApp FlexCacheの元のボリュームである。
  - ONTAP 9.7以前では、NetApp Snapshotは255個以下にする必要があります。ONTAP 9.8以降では、1023個のSnapshotがサポートされます。
  - Storage Efficiencyが有効になっている。これらは無効にする必要があり、変換後に再度有効にすることができます。
  - ボリュームがSnapMirror関係のソースであり、デスティネーションはまだ変換されていません。
  - ボリュームがアクティブな（休止されていない）SnapMirror関係の一部である。
  - クォータが有効になります。これらは無効にする必要があり、変換後に再度有効にすることができます。
  - ボリューム名が197文字を超えています。
  - ボリュームがアプリケーションに関連付けられている。

    これはONTAP 9.7にのみ該当します。ONTAP 9.8では、この制限が解除されました。

  - ミラーリング、ジョブ、wafliron、NDMPバックアップなどのONTAPプロセスが実行されている およびinode変換が進行中です。
  - ボリュームがSVMルートボリュームである。
  - ボリュームがいっぱいです。

    これらの非互換性が存在する場合、FlexVolボリュームでボリュームの変換が中止されるとエラーメッセージが生成されます。対処方法を実行してから変換を再試行できます。

- FlexVolボリュームの最大容量が現在80%以上の場合は、インプレース変換ではなく、新しく作成したFlexGroupボリュームにデータをコピーすることを検討してください。FlexGroupメンバーボリュームは時間の経過とともに自然にリバランシングされますが、大容量のFlexVolボリュームをFlexGroupボリュームに変換すると、パフォーマンスやバランスの問題が発生する可能性があり、メンバーボリューム間で迅速にリバランシングされません。

非常に大規模なFlexGroupを変換すると、FlexGroupボリュームのメンバーコンスティチュエントが非常にいっぱいになり、パフォーマンスの問題が発生する可能性があります。詳細については、TRの「FlexGroupボリュームを作成しないタイミング」セクションを参照してください"FlexGroup ボリューム-ベストプラクティスおよび実装ガイド"。

手順

1. FlexVolボリュームがオンラインであることを確認します。 `volume show -fields vol_name volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexvol
```

2. FlexVol volumeを問題なく変換できるかどうかを確認します。

   a. advanced権限モードにログインします。 `set -privilege advanced`

   b. 変換プロセスを確認します。 `volume conversion start -vserver vs1 -volume flexvol -check-only true`

   ボリュームを変換する前に、すべてのエラーを修正する必要があります。

   FlexGroupボリュームをFlexVol volumeに戻すことはできません。

3. 変換を開始します。 `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion Snapshot copies cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. 変換が成功したことを確認します。 `volume show vol_name -fields volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexgroup
```

結果

FlexVol volumeがシングルメンバーFlexGroupボリュームに変換されます。

終了後

必要に応じて、FlexGroupボリュームを拡張できます。

ONTAP FlexVol volume SnapMirror関係をONTAP FlexGroup Volume SnapMirror関係に変換する

ONTAPでFlexVol volume SnapMirror関係をFlexGroup Volume SnapMirror関係に変換するには、まずデスティネーションFlexVol volumeを変換してからソースFlexVol volumeを変換する必要があります。

タスクの内容

- FlexGroup変換は、SnapMirror非同期関係でのみサポートされます。
- FlexGroup変換は、 SnapMirrorクラウド関係ではサポートされていません。
- 変換時間はいくつかの変数に依存する。変数には次のようなものがあります。
  - コントローラのCPU
  - 他のアプリケーションによるCPUの使用率
  - 初期スナップショット内のデータ量
  - ネットワーク帯域幅
  - 他のアプリケーションによって使用される帯域幅

開始する前に

- 変換するFlexVol volumeがオンラインになっている必要があります。
- SnapMirror関係のソースFlexVol volumeを複数のSnapMirror関係のソースボリュームにすることはできません。

  ONTAP 9.9.1以降では、FlexGroupボリュームでファンアウトSnapMirror関係がサポートされます。詳細については、を参照してください "FlexGroupのSnapMirrorカスケード/ファンアウト関係の作成に関する考慮事項"。

- FlexVol volumeの処理と設定は、変換プロセスと互換性がある必要があります。

  FlexVol volumeに互換性の問題があり、ボリュームの変換が中止されると、エラーメッセージが生成されます。対処方法を実行してから変換を再試行できます。

手順

1. SnapMirror関係が正常であることを確認します。

```
snapmirror show
```

変換できるのはXDPタイプのミラー関係のみです。

例：

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:src_dpv DP   vs2:dst_dpv  Snapmirrored
                                     Idle           -         true    -
vs0:src_xdp XDP  vs2:dst_xdp  Snapmirrored
                                     Idle           -         true    -
```

2. ソースボリュームに変換互換性があるかどうかを確認します。

   a. advanced権限モードにログインします。

      ```
      set -privilege advanced
      ```

   b. 変換プロセスを確認します。

      ```
      volume conversion start -vserver <src_svm_name> -volume <src_vol>
      -check-only true
      ```

      例：

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+
ボリュームを変換する前に、すべてのエラーを修正する必要があります。

3. デスティネーションFlexVolをFlexGroupボリュームに変換します。

   a. FlexVol SnapMirror関係を休止します。

```
snapmirror quiesce -destination-path <dest_svm:dest_volume>
```

例：

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

b. 変換を開始します。

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

例：

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp

Warning: After the volume is converted to a FlexGroup, it will not be
possible
to change it back to a flexible volume.
Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has
been successfully converted to a FlexGroup volume.
You must now convert the relationship's source volume, "vs0:src_xdp", to
a FlexGroup.
Then, re-establish the SnapMirror relationship using the "snapmirror
resync" command.
```

4. ソースFlexVolボリュームをFlexGroupボリュームに変換します。'

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

例：

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion snapshots cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. 関係を再同期します。

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

例：

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

終了後

ソースFlexGroupボリュームを拡張してコンスティチュエントを追加した場合は、デスティネーションボリュームも拡張する必要があります。

関連情報

- "スナップミラーの静止"
- "snapmirror resync"
- "snapmirror show"

FlexCacheホリユウムノカンリ

ONTAP FlexCacheボリュームの詳細

NetApp FlexCacheテクノロジは、特にクライアントが同じデータに繰り返しアクセスする必要がある場合に、データアクセスの高速化、WANレイテンシの低減、読み取り処理が大量に発生するワークロードのWAN帯域幅コストの削減を実現します。FlexCacheボリュームを作成する場合は、元のボリュームのアクティブにアクセスされるデータ（ホットデータ）のみを含む既存（元の）ボリュームのリモートキャッシュを作成します。

FlexCacheに含まれるホットデータの読み取り要求を受信した場合、クライアントに到達するまでデータを移動する必要がないため、元のボリュームよりも高速に応答できます。FlexCacheボリュームは、読み取り頻度の低いデータ（コールドデータ）の読み取り要求を受信した場合、元のボリュームから必要なデータを取得し、クライアント要求を処理する前にデータを格納します。以降、そのデータに対する読み取り要求

はFlexCacheボリュームから直接提供されます。最初の要求が完了すると、データをネットワーク経由で転送したり、負荷の高いシステムから提供したりする必要がなくなります。たとえば、単一のアクセスポイントで頻繁に要求されるデータに対して、クラスタ内でボトルネックが発生しているとします。クラスタ内でFlexCacheを使用してホットデータに複数のマウントポイントを提供することで、ボトルネックを軽減し、パフォーマンスを向上させることができます。別の例として、複数のクラスタからアクセスされるボリュームへのネットワークトラフィックを減らす必要があるとします。FlexCacheボリュームを使用して、元のボリュームからネットワーク内のクラスタにホットデータを分散させることができます。これにより、ユーザにより近いアクセスポイントが提供されるため、WANトラフィックが削減されます。

FlexCacheテクノロジを使用して、クラウド環境やハイブリッドクラウド環境のパフォーマンスを向上させることもできます。FlexCacheボリュームを使用すると、オンプレミスのデータセンターからクラウドにデータをキャッシュすることで、ワークロードをハイブリッドクラウドに移行できます。また、FlexCacheボリュームを使用して、あるクラウドプロバイダから別のクラウドプロバイダへ、または同じクラウドプロバイダの2つのリージョン間でデータをキャッシュすることで、クラウドサイロを解消することもできます。

ONTAP 9 .10.1以降では、すべてのFlexCacheボリュームを対象に設定できます"グローバルファイルロックを有効にする"。グローバルファイルロックを使用すると、別のユーザがすでに開いているファイルにユーザがアクセスできなくなります。元のボリュームに対する更新は、すべてのFlexCacheボリュームに同時に分散されます。

ONTAP 9 .9.1以降では、FlexCacheボリュームで見つからないファイルのリストが維持されます。これにより、クライアントが存在しないファイルを検索するときに、オリジンに複数の呼び出しを送信する必要がなくなり、ネットワークトラフィックが削減されます。

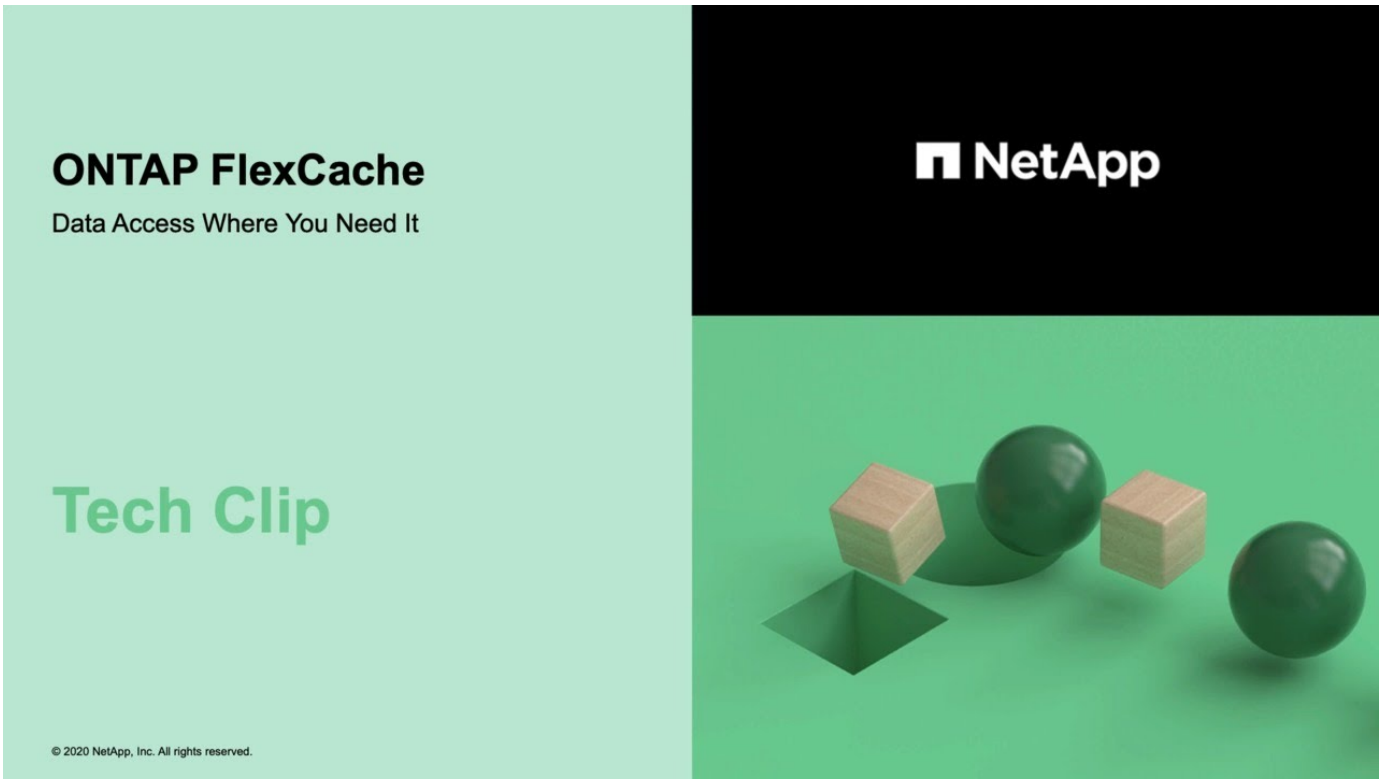
"FlexCacheとその元のボリュームでサポートされる機能"ONTAPのバージョン別にサポートされているプロトコルのリストなど、追加のリストも用意されています。

ONTAP FlexCacheテクノロジのアーキテクチャの詳細については、を参照してください"TR-4743 ：『FlexCache in ONTAP 』"。

ビデオ

FlexCacheでグローバルデータの**WAN**レイテンシと読み取り時間を削減する方法

ONTAP FlexCacheのパフォーマンス上のメリットをご確認ください。



ONTAP FlexCacheでサポートされる機能とサポートされない機能

ONTAP 9.5以降では、FlexCacheボリュームを設定できます。FlexVolボリュームは元のボリュームとして、FlexGroupボリュームはFlexCacheボリュームとしてサポートされま

す。ONTAP 9.7以降では、FlexVolボリュームとFlexGroupボリュームの両方が元のボリュームとしてサポートされます。元のボリュームとFlexCacheボリュームでサポートされる機能とプロトコルは異なります。

> キャッシュボリュームと元のボリュームの両方がサポートされているバージョンのONTAPで実行されていれば、相互運用できます。機能がサポートされるのは、キャッシュとオリジンの両方で少なくともサポートが導入されたONTAPバージョンかそれ以降のONTAPバージョンが実行されている場合のみです。

FlexCacheボリュームと元のボリューム間の**ONTAP**バージョンのサポート

元のボリュームとキャッシュボリュームの間でサポートされるONTAPの推奨バージョンは、4つ前または4つ以降です。たとえば、キャッシュでONTAP 9.14.1が使用されている場合、元のキャッシュで使用できる最も古いバージョンはONTAP 9.10.1です。

サポートされるプロトコル

プロトコル	元のボリュームでのサポート	FlexCacheボリュームでのサポート
NFSv3	○	○
NFSv4	○ NFSv4.xプロトコルを使用してキャッシュボリュームにアクセスするには、元のクラスタとキャッシュクラスタの両方でONTAP 9 10.1以降を使用している必要があります。元のクラスタとFlexCacheクラスタには異なるONTAPバージョンを設定できますが、どちらもONTAP 9 .10.1以降のバージョンである必要があります。たとえば、元のクラスタにはONTAP 9 .10.1、キャッシュにはONTAP 9 .11.1などのように指定できます。	○ ONTAP 9 10.1以降でサポートされています。 NFSv4.xプロトコルを使用してキャッシュボリュームにアクセスするには、元のクラスタとキャッシュクラスタの両方でONTAP 9 10.1以降を使用している必要があります。元のクラスタとFlexCacheクラスタには異なるONTAPバージョンを設定できますが、どちらもONTAP 9 .10.1以降のバージョンである必要があります。たとえば、元のクラスタにはONTAP 9 .10.1、キャッシュにはONTAP 9 .11.1などのように指定できます。
NFSv4.2	○	いいえ
SMB	○	○ ONTAP 9 8以降でサポートされています。

サポートされる機能

機能	元のボリュームでのサポート	FlexCacheボリュームでのサポート
自律型ランサムウェア対策	○ ONTAP 9 .10.1以降のFlexVol元のボリュームでサポートされ、ONTAP 9 .13.1以降のFlexGroup元のボリュームでサポートされます。を参照して "自律型ランサムウェア対策のユースケースと考慮事項"	いいえ
ウィルス対策	○ ONTAP 9 7以降でサポートされています。	該当なし オリジンでアンチウイルススキャンを設定する場合、キャッシュでは必要ありません。オリジンのウィルス対策スキャンは、書き込み元に関係なく、書き込みがコミットされる前にウィルスに感染したファイルを検出します。FlexCacheでアンチウイルススキャンを使用する方法の詳細については、を参照して "FlexCacheとONTAPのテクニカルレポート"ください。
監査	○ ONTAP 9 7以降でサポートされています。標準のONTAP監査を使用して、FlexCache関係におけるNFSファイルアクセスイベントを監査できます。詳細については、を参照してください。 FlexCacheの監査に関する考慮事項	○ ONTAP 9 7以降でサポートされています。標準のONTAP監査を使用して、FlexCache関係におけるNFSファイルアクセスイベントを監査できます。詳細については、を参照してください。 FlexCacheの監査に関する考慮事項
Cloud Volumes ONTAP	○ ONTAP 9.6以降でサポート	○ ONTAP 9.6以降でサポート
コンパクション	○ ONTAP 9.6以降でサポート	○ ONTAP 9.7以降でサポート
圧縮	○ ONTAP 9.6以降でサポート	○ ONTAP 9.6以降でサポート

重複排除	○	○ インライン重複排除は、ONTAP 9以降のFlexCacheボリュームでサポートされます。6.ボリューム間重複排除は、ONTAP 9以降のFlexCacheボリュームでサポートされます。7.
FabricPool	○	○ ONTAP 9.7以降でサポート
FlexCache DR	○	○ ONTAP 9 .9.1以降でNFSv3プロトコルを使用する場合にのみサポートされます。FlexCacheボリュームは、別 々 のSVMまたはクラスタに配置する必要があります。
FlexGroupボリューム	○ ONTAP 9.7以降でサポート	○
FlexVol volume	○	いいえ
FPolicy	○ ONTAP 9.7以降でサポート	○ ONTAP 9以降ではNFSがサポートされています。7.ONTAP 9 14.1以降ではSMBでサポートされます。
MetroCluster構成	○ ONTAP 9.7以降でサポート	○ ONTAP 9.7以降でサポート
Microsoftオフロードデータ転送（ODX）	○	いいえ
NetAppアグリゲート暗号化（NAE）	○ ONTAP 9.6以降でサポート	○ ONTAP 9.6以降でサポート
NetAppボリューム暗号化（NVE）	○ ONTAP 9.6以降でサポート	○ ONTAP 9.6以降でサポート

ONTAP S3 NASバケット	○ ONTAP 9.12.1以降でサポート	いいえ
QoS	○	○ ファイルレベルのQoSはFlexCacheボリュームではサポートされません。
qtree	○ ONTAP 9 .6以降では、qtreeを作成および変更できます。ソース上に作成されたqtreeには、キャッシュ上でアクセスできます。	いいえ
クォータ	○ ONTAP 9.6以降では、FlexCache送信元ボリュームでのクォータの適用がユーザ、グループ、およびqtreeでサポートされます。	いいえ FlexCacheライトアラウンドモード（デフォルトモード）では、キャッシュの書き込みは元のボリュームに転送されます。クォータは元のボリュームで適用されます。 ONTAP 9.6以降では、FlexCacheボリュームでリモート クォータ（rquota）がサポートされます。
SMB変更通知	○	○ ONTAP 9.14.1以降では、SMB変更通知がキャッシュでサポートされます。
SnapLockボリューム	いいえ	いいえ
SnapMirror非同期関係*	○	いいえ

	• FlexCacheの起源： • 元のFlexVolからFlexCacheボリュームを作成できます。 • 元のFlexGroupからFlexCacheボリュームを作成できます。 • SnapMirror関係にある元のプライマリボリュームのFlexCacheボリュームを作成できます。 • ONTAP 9 .8以降では、SnapMirrorセカンダリボリュームをFlexCacheの元のボリュームにすることができます。SnapMirrorセカンダリボリュームはアイドル状態で、SnapMirror更新はアクティブではありません。アイドル状態にしないと、FlexCacheの作成が失敗します。	SnapMirror同期関係
いいえ	いいえ	SnapRestore
○	いいえ	スナップショット
○	いいえ	SVM DR設定
○ ONTAP 9.5以降でサポートされます。SVM DR関係のプライマリSVMに元のボリュームを含めることができますが、SVM DR関係を解除した場合は、新しい元のボリュームを使用してFlexCache関係を再作成する必要があります。	いいえ プライマリSVMにはFlexCacheを作成できますが、セカンダリSVMには作成できません。プライマリSVM内のFlexCacheボリュームは、SVM DR関係の一部としてレプリケートされません。	ストレージレベルのアクセス保護（SLAG）
いいえ	いいえ	シンプロビジョニング
○	○ ONTAP 9.7以降でサポート	ボリュームクローニング
○ ONTAP 9以降では、元のボリュームおよび元のボリューム内のファイルのクローニングがサポートされています。6.	いいえ	ボリューム移動

○	○（ボリュームコンスティチュエントのみ） FlexCacheのボリュームコンスティチュエントの移動は、ONTAP 9 .6以降でサポートされます。	ホリユウムノリホスト
いいえ	いいえ	vStorage API for Array Integration（VAAI）

9.5より前のONTAP 9リリースでは、元のFlexVolボリュームは、Data ONTAP 8 .2.x 7-Modeを実行しているシステムで作成されたFlexCacheボリュームにのみデータを提供できます。ONTAP 9 .5以降では、元のFlexVolボリュームから、ONTAP 9システム上のFlexCacheボリュームにもデータを提供できます。7-Mode FlexCacheからONTAP 9 FlexCacheへの移行の詳細については、を参照してください"NetAppテクニカルレポート4743：『FlexCache in ONTAP』"。

ONTAP FlexCacheボリュームのサイジングに関するガイドライン

ボリュームのプロビジョニングを開始する前に、FlexCacheボリュームの制限を確認しておく必要があります。

FlexVol volumeのサイズ制限は元のボリュームに適用されます。FlexCacheボリュームのサイズは、元のボリューム以下にすることができます。FlexCacheボリュームのサイズは、元のボリュームサイズの10%以上にすることを推奨します。

また、FlexCacheボリュームに関する次の制限も確認しておく必要があります。

制限	ONTAP 9.8以降	ONTAP 9.7	ONTAP 9.6～9.5
元のボリュームから作成できるFlexCacheの最大数	100	10	10
推奨されるノードあたりの元のボリュームの最大数	100	100	10
推奨されるノードあたりのFlexCacheの最大数	100	100	10
ノードあたりのFlexCacheボリュームで推奨されるFlexGroupコンスティチュエントの最大数	800	800	40
ノードあたりのFlexCacheあたりのコンスティチュエントの最大数	32	32	32

関連情報

- "NetAppの相互運用性"

ONTAP FlexCacheボリュームの作成

同じクラスタにFlexCacheボリュームを作成すると、ホットオブジェクトにアクセスする際のパフォーマンスが向上します。データセンターが異なる場所にある場合は、リモートクラスタにFlexCacheボリュームを作成してデータアクセスを高速化できます。

タスクの内容

- ONTAP 9 .5以降では、FlexCacheでFlexVolボリュームが元のボリュームとして、FlexGroupボリュームがFlexCacheボリュームとしてサポートされます。
- ONTAP 9.7以降では、FlexVol volumeボリュームとFlexGroupボリュームの両方が元のボリュームとしてサポートされます。
- ONTAP 9.14.0以降では、暗号化されたソースから暗号化されていないFlexCacheボリュームを作成できます。

開始する前に

- ONTAP 9.5以降が実行されている必要があります。
- ONTAP 9 .6以前を実行している場合は、を実行する必要があります"FlexCacheライセンスを追加する"。

  ONTAP 9 .7以降にはFlexCacheライセンスは必要ありません。ONTAP 9 .7以降では、FlexCache機能がONTAPに含まれているため、ライセンスやアクティブ化は不要になりました。

> HAペアでを使用している場合は"SAS ドライブまたは NVMe ドライブの暗号化（ SED 、 NSE 、 FIPS ）"、システムを初期化する前に、HAペア内のすべてのドライブに対応するトピックの手順に従う必要があります"FIPSドライブまたはSEDを非保護モードに戻す"（ブートオプション4または9）。これを行わないと、ドライブを転用した場合にデータが失われる可能性があります。

例 **12.** 手順

System Manager

1. FlexCacheボリュームが元のボリュームとは別のクラスタにある場合は、クラスタピア関係を作成します。
   a. ローカルクラスタで、*[保護]>[概要]*をクリックします。
   b. を展開し、[ネットワークインターフェイスの追加]*をクリックして、クラスタのクラスタ間ネットワークインターフェイスを追加します。

      リモートクラスタでこの手順を繰り返します。

   c. リモートクラスタで、**[保護]>[概要]***をクリックします。**[Cluster Peers]**セクション内をクリックし ⋮ 、[Generate Passphrase]*をクリックします。
   d. 生成されたパスフレーズをコピーし、ローカルクラスタに貼り付けてください。
   e. ローカルクラスタで、[クラスタピア]の*[クラスタのピアリング]*をクリックし、ローカルクラスタとリモートクラスタをピアリングします。
2. SVMピア関係を作成します。

   [Storage VMピア]でをクリックし、*[Storage VMのピアリング]*をクリックし ⋮ てStorage VMをピアリングします。
3. Storage > Volumes （ストレージ）を選択します。
4. 「 * 追加」を選択します。
5. を選択し、[リモートボリュームのキャッシュとして追加]*を選択します。

   ⓘ ONTAP 9.8以降を実行していて、QoSを無効にするかカスタムQoSポリシーを選択する場合は、**[**その他のオプション**]***をクリックし、[ストレージと最適化]で[パフォーマンスサービスレベル]*を選択します。

CLI

1. FlexCacheボリュームを別のクラスタに作成する場合は、クラスタピア関係を作成します。
   a. デスティネーションクラスタで、データ保護のソースクラスタとのピア関係を作成します。

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

   ONTAP 9 .6以降では、クラスタピア関係の作成時にTLS暗号化がデフォルトで有効になります。TLS暗号化は、元のボリュームとFlexCacheボリュームの間のクラスタ間通信でサポートされます。必要に応じて、クラスタピア関係のTLS暗号化を無効にすることもできます。

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

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

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

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

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

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

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. FlexCacheボリュームが元のボリュームとは別のSVMにある場合は、をアプリケーションとしたSVMピア関係を作成し `flexcache`ます。

a. SVMが別のクラスタにある場合は、ピアリングするSVMのSVM権限を作成します。

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

次の例は、すべてのローカルSVMに適用されるSVMピア権限を作成する方法を示しています。

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. SVMピア関係を作成します。

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. FlexCacheボリュームを作成します。

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

次の例は、FlexCacheボリュームを作成し、プロビジョニングする既存のアグリゲートを自動的に選択します。

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

次の例は、FlexCacheボリュームを作成し、ジャンクション パスを設定します。

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. FlexCacheボリュームと元のボリュームのFlexCache関係を確認します。

a. クラスタ内のFlexCache関係を表示します。

```
volume flexcache show
```

```
cluster1::> volume flexcache show
Vserver Volume      Size       Origin-Vserver Origin-Volume
Origin-Cluster
------- ----------- ---------- -------------- -------------
--------------
vs_1    fc1         160MB      vs_1           vol_1
cluster1
```

b. 元のクラスタのすべてのFlexCache関係を表示します。+
`volume flexcache origin show-caches`

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume   Cache-Vserver    Cache-Volume
Cache-Cluster
-------------- --------------- ---------------  --------------
---------------
vs0            ovol1           vs1              cfg1
clusA
vs0            ovol1           vs2              cfg2
clusB
vs_1           vol_1           vs_1             fc1
cluster1
```

結果

FlexCacheボリュームが作成されました。クライアントは、FlexCacheボリュームのジャンクションパスを使用してボリュームをマウントできます。

関連情報

"クラスタとSVMのピアリング"

FlexCacheライトバック

ONTAP FlexCacheライトバックの詳細

ONTAP 9.15.1で導入されたFlexCacheライトバックは、キャッシュへの書き込み処理の代替モードです。ライトバックを使用すると、書き込みがキャッシュの安定したストレージにコミットされ、データが元のストレージに到達するのを待たずにクライアントに確認応答が返されます。データは非同期的に元のデータにフラッシュされます。その結果、グローバルに分散されたファイルシステムが実現し、特定のワークロードや環境に対してローカルに近い速度で書き込みを実行できるようになり、パフォーマンスが大幅に向上します。

ONTAP 9.12.1では、ライトバック機能がパブリックプレビューとして導入されました。これはライトバックバージョン1（wbv1）と呼ばれ、ライトバックバージョン2（wbv2）と呼ばれるONTAP 9.15.1のライトバックと同じと考えるべきではありません。

ライトバックとライトアラウンド

FlexCacheはONTAP 9.5で導入されて以来、読み取り/書き込み可能なキャッシュですが、ライトアラウンドモードで動作します。キャッシュでの書き込みは、安定したストレージにコミットされるためにオリジンに送られました。送信元は、安定したストレージへの書き込みを正常にコミットしたあと、キャッシュへの書き込みを確認応答しました。その後、キャッシュはクライアントへの書き込みを確認応答します。このため、書き込みが行われるたびに、キャッシュと送信元の間のネットワークをトラバースするというペナルティが発生します。FlexCacheライトバックはこれを変更します。

ONTAP 9.15.1にアップグレードすると、従来のライトアラウンドキャッシュをライトバックキャッシュに変換し、必要に応じてライトアラウンドに戻すことができます。ただし、これにより、問題が発生した場合に診断ログの読み取りが困難になる可能性があります。

	ライトアラウンド	ライトバック
ONTAPバージョン	9.6以上	9.15.1以上
ユースケース	読み取り負荷の高いワークロード	書き込み負荷の高いワークロード
データのコミット日時	由来	キャッシュ
顧客体験	WANライク	LANライク
制限	オリジンごとに100	オリジンあたり10
"キャップ定理"	使用可能で、パーティションに耐性がある	可用性と一貫性

FlexCacheライトバックに関する用語

FlexCacheライトバックを使用する主な概念と用語を理解します。

期間	定義
ダーティデータ	キャッシュの安定したストレージにコミットされたが、送信元にフラッシュされていないデータ。
排他ロック委任**(XLD)**	ファイル単位でキャッシュに付与されるプロトコルレベルのロック権限。この権限を使用すると、キャッシュがオリジンに接続せずにクライアントに排他的な書き込みロックを渡すことができます。
共有ロック委任（**SLD**）	ファイル単位でキャッシュに付与されるプロトコルレベルのロック権限。この権限を使用すると、キャッシュはオリジンに接続せずに共有読み取りロックをクライアントに渡すことができます。
ライトバック	FlexCache処理のモード。キャッシュへの書き込みがそのキャッシュの安定したストレージにコミットされ、クライアントに即座に確認応答が返されます。データは非同期的に元のデータに書き戻されます。
書き替え	FlexCache処理のモード。キャッシュへの書き込みが元のストレージに転送され、安定したストレージにコミットされます。コミットされると、送信元はキャッシュへの書き込みを確認応答し、キャッシュはクライアントへの書き込みを確認応答します。

期間	定義
ダーティー・データ・レコード・システム（**DDR**）	ライトバックが有効なキャッシュ内のダーティデータをファイル単位で追跡する独自のメカニズム。
原点	すべてのFlexCacheキャッシュボリュームのソースデータを含むFlexGroupまたはFlexVol。データは一元化された情報源であり、ロックをオーケストレーションし、データの整合性、通貨性、一貫性を100%保証します。
キャッシュ	FlexCacheオリジンのスパースキャッシュボリュームであるFlexGroup。

一貫性、電流、一貫性

FlexCacheは、場所を問わず適切なデータを保持するためのネットアップのソリューションです。FlexCacheは常に100%の一貫性、電流、一貫性を備えています。

- *一貫性：*データはアクセスされる場所を問わず同じです。
- *現在：*データは常に最新です。
- *一貫性：*データは正しい/破損していません。

ONTAP FlexCacheライトバックのガイドライン

FlexCacheライトバックには、オリジンとキャッシュの間の多くの複雑なやり取りが含まれます。最適なパフォーマンスを実現するには、次のガイドラインに従って環境を構築する必要があります。これらのガイドラインは、コンテンツ作成時に入手可能な最新のONTAPメジャーバージョン（ONTAP 9.15.1）に基づいています。

ベストプラクティスとして、本番環境以外の環境で本番ワークロードをテストします。これらのガイドライン以外でFlexCacheライトバックを実装する場合は、これがさらに重要になります。

次のガイドラインは、NetApp内部で十分にテストされています。それは*強く*それらの内にとどまることをお勧めします。そうしないと、予期しない動作が発生する可能性があります。

- ONTAP 9.15.1P5では、FlexCacheライトバックの大幅な機能拡張が導入されました。9.15.1P5以降に現在推奨されているリリースをオリジンクラスタとキャッシュクラスタの両方で実行することを推奨します。
- 現在の反復計算では、FlexCacheボリューム全体に対して1つのコンスティチュエントを使用してFlexCacheライトバックキャッシュを設定する必要があります。マルチコンスティチュエントFlexCachesを使用すると、データが不要にキャッシュから削除される可能性があります。
- テストは、100GB未満のファイルと、キャッシュとオリジンの間のWANラウンドトリップ時間が100msを超えないように実行されました。この制限外のワークロードがあると、予期しないパフォーマンス特性が発生する可能性があります。
- SMB代替データストリームに書き込むと、メインファイルがキャッシュから削除されます。メインファイルのすべてのダーティデータは、そのファイルで他の操作を実行する前にオリジンにフラッシュする必要があります。代替データストリームもオリジンに転送されます。
- ファイル名を変更すると、そのファイルがキャッシュから削除されます。ファイルのすべてのダーティーデータは、そのファイルで他の操作を実行する前に、オリジンにフラッシュする必要があります。

- 現時点では、ライトバックが有効なFlexCacheボリューム上のファイルに対して変更または設定できる属性は次のとおりです。
  - タイムスタンプ
  - モードビット
  - NT ACL
  - 所有者
  - グループ
  - サイズ

    変更または設定されたその他の属性は送信元に転送され、その結果ファイルがキャッシュから削除される可能性があります。他の属性の変更やキャッシュでの設定が必要な場合は、アカウントチームにPVRを開くよう依頼してください。
- 元のボリュームでSnapshotが作成されると、その元のボリュームに関連付けられたライトバックが有効になっているすべてのキャッシュから、未処理のダーティーデータがすべてリコールされます。大量のライトバック処理が実行中の場合は、これらのダーティファイルの削除に時間がかかることがあるため、処理の再試行が複数回必要になることがあります。
- 原点の使用率が80%未満である必要があります。元のボリュームに20%以上のスペースが残っていないと、キャッシュボリュームに排他的ロック委譲が許可されません。この場合、ライトバックが有効なキャッシュへの呼び出しはオリジンに転送されます。これにより、元のスペースが不足して、ライトバックが有効なキャッシュにダーティデータが孤立したままになるのを防ぐことができます。

ONTAP FlexCacheライトバックアーキテクチャ

FlexCacheは、ライトバックモードとライトアラウンドモードの両方を含め、高い整合性を考慮して設計されています。ONTAP 9.15.1で導入された従来のライトアラウンド処理モードと新しいライトバック処理モードはどちらも、アクセスされるデータの整合性、最新性、一貫性を常に100%保証します。

次の概念では、FlexCacheライトバックの動作について詳しく説明します。

委譲

委譲とデータ委譲をロックすると、FlexCacheはライトバックキャッシュとライトアラウンドキャッシュの両方で、データの整合性、一貫性、最新の状態を維持できます。オリジンが両方の委譲をオーケストレーションします。

ロックイジョウ

ロックの委譲は、必要に応じてクライアントにプロトコルロックを発行するために、送信元がキャッシュにファイル単位で付与するプロトコルレベルのロック権限です。これらにはおよびが含まれます 排他ロック委任(XLD) 共有ロック委譲（SLD）。

XLDおよびライトバック

ONTAPが競合する書き込みを調整する必要がないようにするために、クライアントがファイルへの書き込みを要求するキャッシュにXLDが付与されます。重要なことは、一度に1つのファイルに対して1つのXLDしか存在できないことです。つまり、1つのファイルに対して複数のライタが存在することはありません。

ファイルへの書き込み要求がライトバックが有効なキャッシュに入ると、次の手順が実行されます。

1. キャッシュは、要求されたファイルのXLDがすでに存在しているかどうかをチェックします。その場合、別のクライアントがキャッシュにあるファイルに書き込んでいない限り、書き込みロックがクライアントに付与されます。キャッシュに要求されたファイルのXLDがない場合、キャッシュはオリジンからXLDを要求します。これは、クラスタ間ネットワークを経由する独自のコールです。
2. キャッシュからXLD要求を受信すると、オリジンはファイルの未処理のXLDが別のキャッシュにあるかどうかをチェックします。その場合、そのファイルのXLDが呼び出され、そのキャッシュからオリジンへのフラッシュがトリガーされ ダーティーデータ ます。
3. そのキャッシュのダーティデータがフラッシュバックされ、オリジンの安定したストレージにコミットされると、オリジンはファイルのXLDを要求元のキャッシュに付与します。
4. ファイルのXLDを受信すると、キャッシュによってクライアントにロックが許可され、書き込みが開始されます。

これらの手順の一部を網羅する高レベルのシーケンス図をシーケンス図で説明します [write-back-sequence-diagram] 。

クライアント側では、すべてのロックは標準のFlexVolまたはFlexGroupに書き込みを行っているかのように機能し、書き込みロックが要求されたときにわずかな遅延が発生する可能性があります。

現在のイテレーションでは、ライトバックが有効なキャッシュがファイルのXLDを保持している場合、ONTAPは操作を含む他のキャッシュでそのファイルへの*すべての*アクセスをブロックします `READ` 。

> オリジンコンスティチュエントあたりのXLD数は170に制限されています。

データ委譲

データ委譲は、送信元がそのファイル用にキャッシュされたデータが最新であることをキャッシュに付与するファイル単位の保証です。キャッシュにファイルのデータ委譲があるかぎり、そのファイルのキャッシュデータをクライアントに提供できます。元のファイルにアクセスする必要はありません。キャッシュにファイルのデータ委任がない場合は、クライアントから要求されたデータを受信するためにオリジンに接続する必要があります。

ライトバックモードでは、ファイルのデータ委譲は、そのファイルのXLDが別のキャッシュまたはオリジンで取得された場合に取り消されます。これにより、読み取り時も含め、他のすべてのキャッシュとオリジンでクライアントからファイルが実質的に遮断されます。これはトレードオフであり、古いデータにアクセスしないようにする必要があります。

ライトバックが有効なキャッシュでの読み取りは、一般にライトアラウンドキャッシュでの読み取りと同様に処理されます。ライトアラウンドキャッシュとライトバックが有効なキャッシュの両方で、要求されたファイルが、読み取りが発行された場所以外のライトバックが有効なキャッシュで排他的な書き込みロックを持つと、初期パフォーマンスが低下する可能性があります `READ` 。XLDを取り消す必要があり、他のキャッシュでの読み取りを処理する前に、ダーティデータをオリジンにコミットする必要があります。

ダーティーデータの追跡

キャッシュからオリジンへのライトバックは非同期的に行われます。これは、ダーティデータがすぐにオリジンに書き戻されるわけではないことを意味します。ONTAPでは、ダーティデータレコードシステムを使用して、ファイルごとにダーティデータを追跡しています。各ダーティデータレコード（DDR）は、特定のファイルの約20MBのダーティデータを表します。ファイルがアクティブに書き込まれている場合、ONTAPは2つのDDRがいっぱいになり、3つ目のDDRが書き込まれると、ダーティデータのフラッシュを開始します。その

結果、書き込み中にキャッシュ内に約40MBのダーティデータが残ります。ステートフルプロトコル（NFSv4.x、SMB）の場合、ファイルを閉じると、残りの40MBのデータが元のボリュームにフラッシュされます。ステートレスプロトコル（NFSv3）の場合、ファイルへのアクセスが別のキャッシュで要求されたとき、またはファイルが2分以上アイドル状態になったあと（最大5分）に、40MBのデータがフラッシュバックされます。タイマートリガー型またはスペーストリガー型ダーティデータフラッシュの詳細については、を参照してください [キャッシュスクラビング]。

DDRとスクラバーに加えて、一部のフロントエンドNAS操作では、ファイルのすべてのダーティデータのフラッシュもトリガーされます。

- `SETATTR`
  - mtime、atime、ctimeのみを変更するsetattrはキャッシュで処理できるため、WANのペナルティを回避できます。
- `CLOSE`
- `OPEN` 別のキャッシュ
- `READ` 別のキャッシュ
- `READDIR` 別のキャッシュ
- `READDIRPLUS` 別のキャッシュ
- `WRITE` 別のキャッシュ

切断モード

ファイルのXLDがライトアラウンドキャッシュに保持され、そのキャッシュがオリジンから切断された場合でも、そのファイルの読み取りは他のキャッシュおよびオリジンで引き続き許可されます。この動作は、XLDがライトバックが有効なキャッシュに保持されている場合に異なります。この場合、キャッシュが切断されている場合、ファイルへの読み取りはどこでもハングします。これにより、100%の一貫性、通貨、一貫性が維持されます。クライアントに書き込み確認応答されたすべてのデータが元のボリュームに確実に格納されるため、読み取りはWrite-aroundモードで許可されます。切断中のライトバックモードでは、切断前にライトバックが有効なキャッシュに書き込まれて確認されたすべてのデータがオリジンに送信されたことをオリジンが保証することはできません。

ファイルのXLDを持つキャッシュが長時間切断された場合、システム管理者はオリジンでXLDを手動で取り消すことができます。これにより、ファイルへのIOが、サバイバーキャッシュとオリジンで再開されます。

> XLDを手動で取り消すと、切断されたキャッシュにあるファイルのダーティデータが失われます。XLDの手動取り消しは、キャッシュとオリジンの間で壊滅的な中断が発生した場合にのみ実行してください。

キャッシュスクラビング

ONTAPには、タイマーの期限切れやスペースのしきい値超過など、特定のイベントに応じて実行されるスクラバーがあります。スクラバーは、スクラビングされているファイルに対して排他ロックを取得し、スクラビングが完了するまで、そのファイルへのIOを事実上凍結します。

スクラバーには以下が含まれます。

- *キャッシュ上のmtimeベースのスクラビング：*このスクラビングは5分ごとに開始され、変更されていないファイルを2分間スクラビングします。ファイルのダーティーデータがキャッシュに残っている場合、そのファイルへのIOは休止され、ライトバックがトリガーされます。IOはライトバックの完了後に再開さ

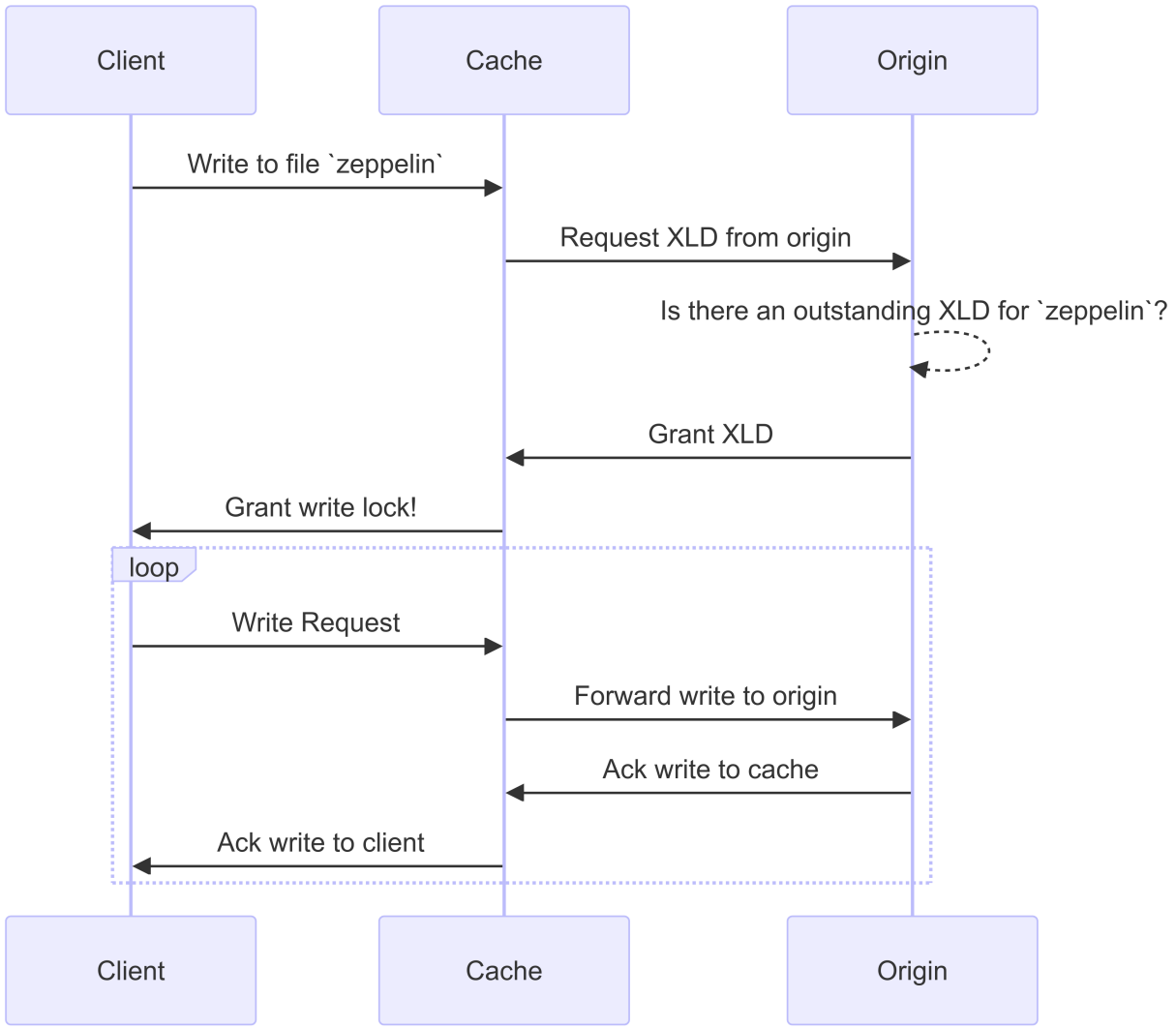
れます。

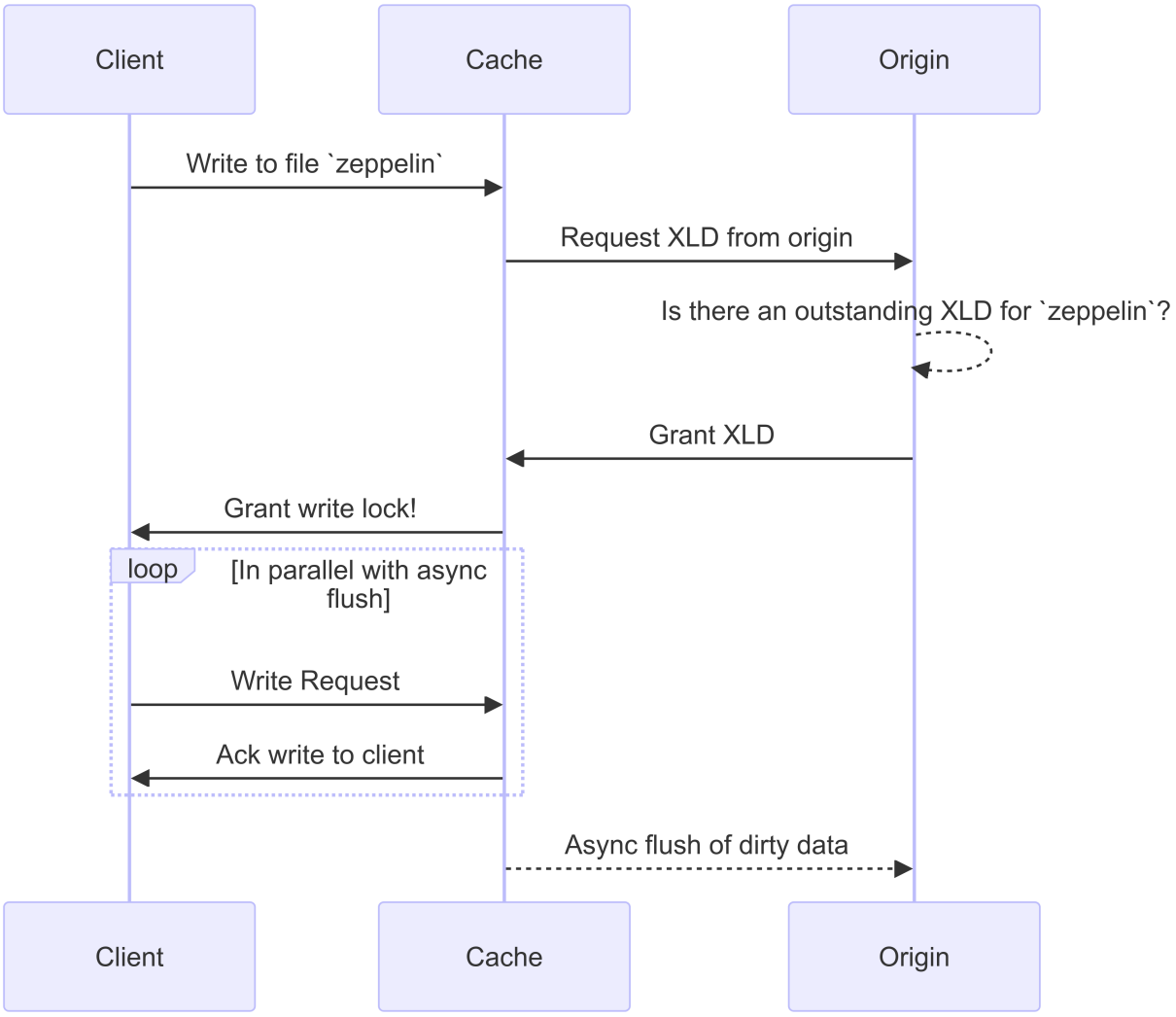
- * mtimeベースのscrubber on origin：*キャッシュにあるmtimeベースのscrubberと同様に、これも5分ごとに実行されます。ただし、変更されていないファイルは15分間スクラビングされ、inodeの委譲が呼び出されます。このスクラバーはライトバックを開始しません。
- * RW制限ベースのオリジンスクラバー：* ONTAPは、オリジンコンスティチュエントごとに配布されるRWロック委譲の数を監視します。この数が170を超えると、ONTAPはLeast-Recently-Used（LRU）ベースで書き込みロック委譲のスクラビングを開始します。
- キャッシュ上のスペースベーススクラビング： FlexCacheボリュームの使用率が90%に達すると、キャッシュはスクラビングされ、LRUベースで削除されます。
- 元のスペースベーススクラビング： FlexCache元のボリュームの使用率が90%に達すると、キャッシュはスクラビングされ、LRUベースで削除されます。

シーケンス図

これらのシーケンス図は、ライトアラウンドモードとライトバックモードの間の書き込み確認応答の違いを示しています。

ライトアラウンド





ONTAP FlexCacheライトバックのユースケース

これらはライトバックが有効なFlexCacheに最適な書き込みプロファイルです。ワークロードをテストして、ライトバックまたはライトアラウンドが最高のパフォーマンスを提供するかどうかを確認する必要があります。

ライトバックはライトアラウンドの代わりにはなりません。ライトバックは書き込み負荷の高いワークロード向けに設計されていますが、多くのワークロードにはライトアラウンドが適しています。

対象となるワークロード

ファイルサイズ

ファイルサイズは、ファイルの呼び出しと呼び出しの間に実行される書き込み数よりも重要ではありません `OPEN CLOSE` 。サイズの小さいファイルは本質的に呼び出し回数が少なく、ライトバックにはあまり `WRITE` 適していません。サイズの大きいファイルは、との呼び出しの間に多くの書き込みが行われる可能性があります `OPEN CLOSE` が、これは保証されません。

最大ファイルサイズに関する最新の推奨事項については、ページを参照して"FlexCacheライトバックのガイドライン"ください。

書き込みサイズ

クライアントからの書き込みでは、書き込みコール以外の変更NASコールが関係します。これらには以下が含まれますが、これらに限定されません。

- CREATE
- OPEN
- CLOSE
- SETATTR
- SET_INFO

SETATTR SET_INFO、 atime、 ctime owner、、 group、またはを size`設定したコールは `mtime、キャッシュで処理されます。これらの呼び出しの残りの部分はオリジンで処理され、ライトバックが有効なキャッシュに蓄積されたダーティデータのライトバックをトリガーする必要があります。ライトバックが完了するまで、ファイルへのIOは休止されます。

これらの呼び出しがWANを経由する必要があることを知っておくと、ライトバックに適したワークロードを特定するのに役立ちます。一般的に、 OPEN `CLOSE`上記のいずれかの呼び出しを発行しなくても、との呼び出しの間に実行できる書き込み数が多いほど、パフォーマンスの向上によるライトバックが向上します。

リードアフターライト

FlexCacheでは、これまでリードアフターライトワークロードのパフォーマンスが低下していました。これは、9.15.1より前のライトアラウンド動作が原因です。 WRITE`ファイルへの呼び出しはオリジンでコミットされる必要があり、後続の呼び出しでは `READ データをキャッシュに戻す必要があります。これにより、両方の動作がWANのペナルティを受けることになります。そのため、ライトアラウンドモードのFlexCacheでは、リードアフターライトワークロードは推奨されません。9.15.1でライトバックが導入されたことで、データはキャッシュにコミットされ、キャッシュから即座に読み取ることができるようになり、WANのペナルティが解消されました。ワークロードにFlexCacheボリュームでのリードアフターライトが含まれている場合は、キャッシュをライトバックモードで動作するように設定する必要があります。

リードアフターライトがワークロードの重要な部分である場合は、ライトバックモードで動作するようにキャッシュを設定する必要があります。

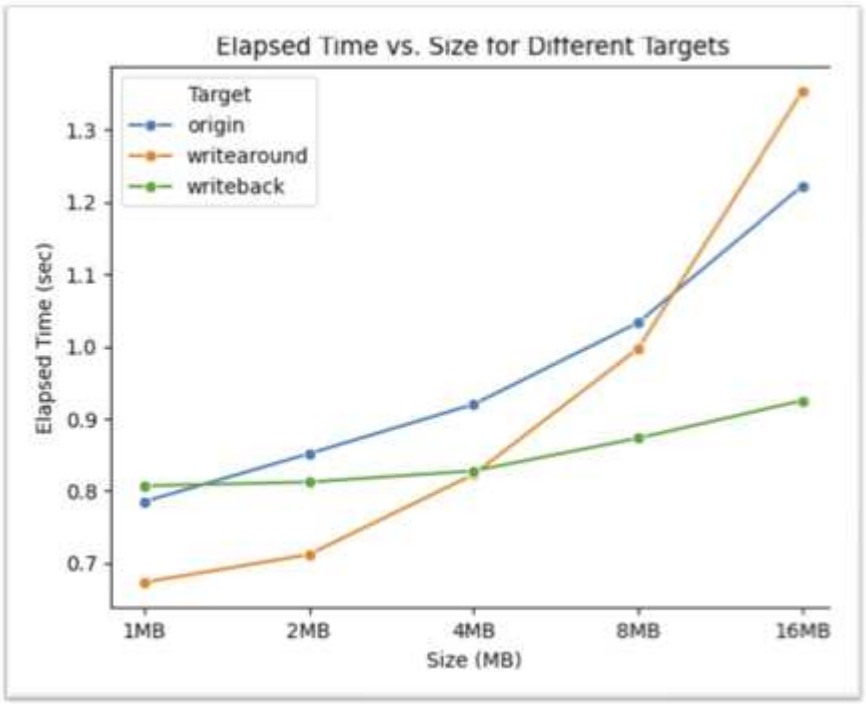
Write-after-write

ファイルがキャッシュにダーティデータを蓄積すると、キャッシュはデータを非同期的に元のデータに書き込みます。これは当然のことながら、クライアントがダーティデータがオリジンへのフラッシュバックを待機している状態でファイルを閉じた場合に発生します。クローズされたばかりのファイルに別のオープンまたは書き込みが入ってきてもダーティデータが残っている場合、すべてのダーティデータがオリジンにフラッシュされるまで書き込みは中断されます。

レイテンシに関する考慮事項

FlexCacheがライトバックモードで動作している場合は、レイテンシが増加するとNASクライアントの方が有利になります。ただし、低レイテンシの環境で得られる利点よりも、ライトバックのオーバーヘッドが大きくなる点があります。一部のNetAppテストでは、ライトバックのメリットは、キャッシュとオリジンの間の最小レイテンシが8ミリ秒前後で始まっていました。このレイテンシはワークロードによって異なります。ワークロードのポイントオブリターンをテストして確認してください。

次のグラフは、NetAppラボテストにおけるライトバックのポイントを示しています。 `x`軸はファイルサイズで、 `y`軸は経過時間です。このテストではNFSv3を使用し、とを256KBにマウントし、 `rsize wsize` 64ミリ秒のWANレイテンシを実現しました。このテストでは、キャッシュとオリジンの両方に小さいONTAP Selectインスタンスを使用し、1回のスレッド書き込み処理を実行しました。結果は異なる場合があります。



ライトバックはクラスタ内キャッシングには使用しないでください。クラスタ内キャッシングは、元のキャッシュとキャッシュが同じクラスタ内にある場合に実行されます。

ONTAP FlexCacheライトバックの前提条件

FlexCacheをライトバックモードで導入する前に、パフォーマンス、ソフトウェア、ライセンス、およびシステム構成の要件を満たしていることを確認してください。

CPUとメモリ

ライトバック対応キャッシュによって開始されたライトバック メッセージを吸収するために、各オリジン クラスタ ノードに少なくとも 128 GB の RAM と 20 個の CPU が搭載されていることが 強く推奨 されます。これはA400以上に相当します。送信元クラスタが複数のライトバックが有効なFlexCachesの送信元として機能する場合、より多くのCPUとRAMが必要になります。

ワークロードにオリジンのサイズが十分でない場合、ライトバックが有効になっているキャッシュまたはオリジンのパフォーマンスに大きな影響を与える可能性があります。

ONTAPのバージョン

- 元の*_ must_*はONTAP 9.15.1以降を実行している必要があります。
- ライトバックモードで動作する必要があるキャッシュクラスタ*_must_*は、ONTAP 9.15.1以降を実行している必要があります。
- ライトバックモードで動作する必要がないキャッシュクラスタでは、一般にサポートされているすべて

のONTAPバージョンを実行できます。

ライセンス

ライトバック動作モードを含むFlexCacheは、ONTAP購入時に付属しています。追加のライセンスは必要ありません。

ピアリング

- 元のクラスタとキャッシュクラスタは "クラスタピア関係が確立"
- 元のクラスタおよびキャッシュクラスタ上のサーバ仮想マシン（SVM）には、FlexCacheオプションが設定されている必要があります "ピアリングされたSVM" 。

キャッシュクラスタを別のキャッシュクラスタにピアリングする必要はありません。また、キャッシュSVMを別のキャッシュSVMとピアリングする必要もありません。

ONTAP FlexCacheライトバックの相互運用性

FlexCacheをライトバックモードで導入する際の相互運用性に関する考慮事項を理解します。

ONTAPのバージョン

ライトバック動作モードを使用するには、キャッシュとオリジン*の両方がONTAP 9.15.1以降を実行している必要があります。

ライトバックが有効になっているキャッシュが不要なクラスタでは、以前のバージョンのONTAPを実行できますが、そのクラスタはライトアラウンドモードでしか動作しません。

環境内にONTAPのバージョンを混在させることができます。

クラスタ	**ONTAP**のバージョン	ライトバックのサポート
原点	ONTAP 9 .15.1	N/A†
*クラスタ1 *	ONTAP 9 .15.1	○
*クラスタ2 *	ONTAP 9 .14.1	いいえ

クラスタ	**ONTAP**のバージョン	ライトバックのサポート
原点	ONTAP 9 .14.1	N/A†
*クラスタ1 *	ONTAP 9 .15.1	いいえ
*クラスタ2 *	ONTAP 9 .15.1	いいえ

†オリジンはキャッシュではないため、ライトバックもライトアラウンドもサポートされません。

では [example2-table]、どちらのクラスタもライトバックモードを有効にできません。これは、厳しい要件である送信元がONTAP 9.15.1以降を実行していないためです。

クライアントの相互運用性

FlexCacheボリュームがライトアラウンドモードで動作しているかライトバックモードで動作しているかに関係なく、ONTAPで一般的にサポートされているクライアントはすべて、そのボリュームにアクセスできます。サポートされているクライアントの最新のリストについては、ネットアップのを参照してください "Interoperability Matrix"。

クライアントのバージョンは特に重要ではありませんが、NFSv3、NFSv4.0、NFSv4.1、SMB2.x、またはSMB3.xをサポートできる新しいクライアントが必要です。SMB1とNFSv2は廃止されたプロトコルであり、サポートされていません。

ライトバックとライトアラウンド

に示すように [example1-table]、ライトバックモードで動作するFlexCacheは、ライトアラウンドモードで動作するキャッシュと共存できます。ライトアラウンドとライトバックを特定のワークロードと比較することを推奨します。

ライトバックとライトアラウンドでワークロードのパフォーマンスが同じ場合は、ライトアラウンドを使用します。

ONTAP機能の相互運用性

FlexCache機能の相互運用性の最新リストについては、を参照してください "FlexCacheボリュームでサポートされる機能とサポートされない機能"。

ONTAP FlexCacheライトバックの有効化と管理

ONTAP 9.15.1以降では、FlexCacheボリュームでFlexCacheライトバックモードを有効にすることで、エッジコンピューティング環境や書き込み負荷の高いワークロードのキャッシュのパフォーマンスを向上させることができます。また、必要に応じて、FlexCacheボリュームでライトバックが有効になっているかどうかを確認したり、ボリュームのライトバックを無効にしたりすることもできます。

キャッシュボリュームでライトバックが有効になっている場合、書き込み要求は元のボリュームではなくローカルキャッシュに送信されます。

開始する前に

advanced権限モードにする必要があります。

ライトバックを有効にして新しいFlexCacheボリュームを作成する

手順

ONTAPシステムマネージャまたはONTAP CLIを使用して、ライトバックを有効にして新しいFlexCacheボリュームを作成できます。

System Manager

1. FlexCacheボリュームが元のボリュームとは別のクラスタにある場合は、クラスタピア関係を作成します。
   a. ローカルクラスタで、*[保護]>[概要]*をクリックします。
   b. を展開し、[ネットワークインターフェイスの追加]*をクリックして、クラスタにクラスタ間インターフェイスを追加します。

      リモートクラスタで同じ手順を繰り返します。

   c. リモートクラスタで、**[保護]>[概要]***をクリックします。**[Cluster Peers]**セクション内をクリックし、[Generate Passphrase]*をクリックします。
   d. 生成されたパスフレーズをコピーし、ローカルクラスタに貼り付けてください。
   e. ローカルクラスタで、[クラスタピア]の*[クラスタのピアリング]*をクリックし、ローカルクラスタとリモートクラスタをピアリングします。
2. FlexCacheボリュームが元のボリュームとは異なるクラスタにある場合は、SVMピア関係を作成します。

   で、[Storage VMのピア関係を設定]をクリックし、[Storage VMのピアリング]*をクリックしてStorage VMをピアリングします。

   FlexCacheボリュームが同じクラスタにある場合、System Managerを使用してSVMピア関係を作成することはできません。
3. Storage > Volumes （ストレージ）を選択します。
4. 「 * 追加」を選択します。
5. を選択し、[リモートボリュームのキャッシュとして追加]*を選択します。
6. [Enable FlexCache write-back]*を選択します。

CLI

1. FlexCacheボリュームを別のクラスタに作成する場合は、クラスタピア関係を作成します。
   a. デスティネーションクラスタで、データ保護のソースクラスタとのピア関係を作成します。

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

   ONTAP 9 .6以降では、クラスタピア関係の作成時にTLS暗号化がデフォルトで有効になります。TLS暗号化は、元のボリュームとFlexCacheボリュームの間のクラスタ間通信でサポートされます。必要に応じて、クラスタピア関係のTLS暗号化を無効にすることもできます。

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

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

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

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

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

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

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. FlexCacheボリュームが元のボリュームとは別のSVMにある場合は、をアプリケーションとしたSVMピア関係を作成し `flexcache`ます。

a. SVMが別のクラスタにある場合は、ピアリングするSVMのSVM権限を作成します。

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

次の例は、すべてのローカルSVMに適用されるSVMピア権限を作成する方法を示しています。

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. SVMピア関係を作成します。

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. ライトバックを有効にしてFlexCacheボリュームを作成します。

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

既存の**FlexCache**ボリュームで**FlexCache**ライトバックを有効にする

ONTAPシステムマネージャまたはONTAP CLIを使用して、既存のFlexCacheボリュームでFlexCacheライトバックを有効にできます。

System Manager

1. [ストレージ]>[ボリューム]*を選択し、既存のFlexCacheボリュームを選択します。
2. ボリュームの[Overview]ページで、右上にある*[Edit]*をクリックします。
3. ウィンドウで、[FlexCacheライトバックを有効にする]*を選択します。

CLI

1. 既存のFlexCacheボリュームでライトバックを有効にします。

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

FlexCacheライトバックが有効かどうかの確認

手順

FlexCacheライトバックが有効になっているかどうかは、System ManagerまたはONTAP CLIを使用して確認できます。

System Manager

1. [ストレージ]>[ボリューム]*を選択し、ボリュームを選択します。
2. ボリューム*で、[FlexCacheの詳細]を探し、**FlexCache**ボリュームで**FlexCache**ライトバックが[有効]*に設定されているかどうかを確認します。

CLI

1. FlexCacheライトバックが有効になっているかどうかを確認します。

```
volume flexcache config show -volume <cache_flexgroup_name> -fields
is-writeback-enabled
```

FlexCacheボリュームのライトバックを無効にする

FlexCacheボリュームを削除する前に、FlexCacheライトバックを無効にする必要があります。

手順

System ManagerまたはONTAP CLIを使用して、FlexCacheライトバックを無効にできます。

System Manager

1. [ストレージ]>[ボリューム]*を選択し、FlexCacheライトバックが有効になっている既存のFlexCacheボリュームを選択します。
2. ボリュームの[Overview]ページで、右上にある*[Edit]*をクリックします。
3. ウィンドウで、[FlexCacheライトバックを有効にする]*の選択を解除します。

CLI

1. ライトバックを無効にします。

```
volume flexcache config modify -volume <cache_vol_name> -is
-writeback-enabled false
```

ONTAP FlexCacheライトバックに関するよくある質問

このFAQは、質問に対する簡単な回答を探している場合に役立ちます。

ライトバックを使用したい。どのバージョンの**ONTAP**を実行する必要がありますか？

キャッシュと送信元の両方でONTAP 9.15.1以降が実行されている必要があります。最新のPリリースを実行することを推奨します。エンジニアリング部門は、ライトバック対応キャッシュのパフォーマンスと機能を絶えず改善しています。

オリジンにアクセスするクライアントは、ライトバックが有効なキャッシュにアクセスするクライアントに影響を与えますか。

はい。オリジンは、どのキャッシュとも同じ権利をデータに持ちます。ファイルをキャッシュから削除する必要があるファイルに対して処理を実行する場合、またはロック/データ委譲を取り消す必要があるファイルに対して処理を実行すると、キャッシュ上のクライアントからファイルへのアクセスに遅延が生じることがあります。

ライトバックが有効な**FlexCaches**に**QoS**を適用できますか。

はい。各キャッシュとオリジンには、それぞれ独立したQoSポリシーを適用できます。これは、ライトバックで開始されるクラスタ間トラフィックには直接影響しません。QoSによってライトバックが有効なキャッシュでフロントエンドトラフィックを制限することで、間接的にクラスタ間ライトバックトラフィックの速度を低下させることができます。

ライトバックが有効な**FlexCaches**ではマルチプロトコル**NAS**はサポートされていますか。

はい。ライトバックが有効なFlexCachesでは、マルチプロトコルが完全にサポートされています。現在、NFSv4.2およびS3は、ライトアラウンドモードまたはライトバックモードで動作するFlexCacheではサポートされていません。

ライトバックが有効な**FlexCaches**では、**SMB**代替データストリームはサポートされていますか。

SMB Alternate Data Stream（ADS；代替データストリーム）はサポートされていますが、ライトバックによって高速化されることはありません。ADSへの書き込みはオリジンに転送され、WAN遅延のペナルティが発生します。書き込みによって、広告が含まれているメインファイルもキャッシュから削除されます。

キャッシュを作成した後で、ライトアラウンドモードとライトバックモードを切り替えることはできますか。

はい。あなたがしなければならないのは、リンク:../ FlexCache - writeback / FlexCache -writeback-enable -task.htmlコマンド]のフラグ[`flexcache modify`を切り替えることだけです `is-writeback-enabled`。

FlexCacheボリュームを管理します。

ONTAP FlexCacheボリュームの監査について

7以降では、**ONTAP**の標準の監査および**ONTAP 9**によるファイルポリシー管理を使用して、**FlexCache**関係における**NFS**ファイルアクセスイベントを監査できます。

ONTAP 9 14.1以降では、NFSまたはSMBを使用するFlexCacheボリュームでFPolicyがサポートされます。以前は、SMBを使用するFlexCacheではFPolicyはサポートされていませんでした。

標準の監査とFPolicyは、FlexVolボリュームと同じCLIコマンドで設定および管理されます。ただし、FlexCacheボリュームではいくつかの動作が異なります。

- * ネイティブ監査 *
  - 監査ログのデスティネーションとしてFlexCacheボリュームを使用することはできません。
  - FlexCacheボリュームの読み取りと書き込みを監査する場合は、キャッシュSVMと元のSVMの両方で監査を設定する必要があります。

これは、ファイルシステム操作が処理される場所で監査されるためです。つまり、読み取りはキャッシュSVMで監査され、書き込みは元のSVMで監査されます。

- 書き込み処理の発生元を追跡するために、書き込み元のFlexCacheボリュームを識別するために、SVMのUUIDとMSIDが監査ログに追加されます。

- * FPolicy *
  - FlexCacheボリュームへの書き込みは元のボリュームでコミットされますが、FPolicy設定ではキャッシュボリュームの書き込みを監視します。これは、書き込みが元のボリュームで監査される標準の監査とは異なります。
  - キャッシュと元のSVMでONTAPのFPolicy設定が同じである必要はありませんが、同様の設定を2つ導入することを推奨します。そのためには、元のSVMと同様に設定し、新しいポリシーの範囲をキャッシュSVMに限定して、キャッシュ用の新しいFPolicyポリシーを作成します。
  - FPolicy設定の拡張子のサイズは、20KB（20480バイト）に制限されています。FlexCacheボリュームのFPolicy設定で使用される拡張子のサイズが20KBを超えると、EMSメッセージ `nblade.fpolicy.extn.failed`がトリガーされます。

元のボリュームから**ONTAP FlexCache**ボリュームのプロパティを同期する

FlexCache ボリュームの一部のボリュームプロパティは、常に元のボリュームと同期されている必要があります。元のボリュームでプロパティが変更されたあとに、FlexCache ボリュームのボリュームプロパティの自動同期が失敗した場合は、プロパティを手動で同期できます。

タスクの内容

FlexCache ボリュームの次のボリュームプロパティは、常に元のボリュームと同期されている必要があります。

- セキュリティケイシキ(`-security-style`
- ボリューム名(`-volume-name`）
- サイタイテイレクトリサイス(`-maxdir-size`
- 最小先読み(`-min-readahead`）

ステップ

1. FlexCacheボリュームから、ボリュームプロパティを同期します。

   ```
   volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
   ```

   ```
   cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
   ```

ONTAP FlexCache関係の設定を更新する

ボリュームの移動、アグリゲートの再配置、ストレージフェイルオーバーなどのイベントが発生すると、元のボリュームと FlexCache ボリュームの構成情報が自動的に更新されます。自動更新が失敗した場合は EMS メッセージが生成され、 FlexCache 関係の設

定を手動で更新する必要があります。

元のボリュームと FlexCache ボリュームが切断モードになっている場合は、 FlexCache 関係を手動で更新するために追加の処理が必要になることがあります。

タスクの内容

FlexCache ボリュームの設定を更新する場合は、元のボリュームからコマンドを実行する必要があります。元のボリュームの設定を更新する場合は、 FlexCache からコマンドを実行する必要があります。

ステップ

1. FlexCache関係の設定を更新します。

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

ONTAP FlexCacheボリュームでファイルアクセス時間の更新を有効にする

ONTAP 9 .11.1以降では、FlexCacheボリュームのフィールドを有効にしてファイルアクセス時間の更新を許可できます `-atime-update`。属性を使用してアクセス時間の更新期間を設定することもできます `-atime-update-period`。属性は `-atime-update-period`、アクセス時間の更新を実行する頻度と、更新がいつ元のボリュームに反映されるかを制御します。

概要

ONTAPにはというボリュームレベルのフィールドが用意されており `-atime-update`、READ、READLINK、READDIRを使用して読み取られたファイルおよびディレクトリのアクセス時間の更新を管理できます。atimeは、アクセス頻度の低いファイルやディレクトリのデータライフサイクルの決定に使用されます。アクセス頻度の低いファイルは、最終的にアーカイブストレージに移行され、その後テープに移動されることがよくあります。

atime-updateフィールドは、既存および新規に作成されたFlexCacheではデフォルトで無効になっています。ONTAP 9.11.1より前のリリースでFlexCacheボリュームを使用している場合は、元のボリュームで読み取り処理が実行されたときにキャッシュが不要に削除されないように、atime-updateフィールドを無効にしておく必要があります。ただし、大規模なFlexCacheキャッシュでは、管理者は特別なツールを使用してデータを管理し、ホットデータをキャッシュに残してコールドデータをパージすることができます。atime-updateが無効になっている場合は実行できません。ただし、ONTAP 9 .11.1以降では、およびを有効にして、 `-atime-update-period`,`キャッシュされたデータの管理に必要なツールを使用できます `-atime-update`。

開始する前に

- すべてのFlexCacheボリュームでONTAP 9 .11.1以降が実行されている必要があります。
- 権限モードを使用する必要があり `advanced`ます。

タスクの内容

86400秒に設定する `-atime-update-period`と、ファイルに対して実行された読み取りに類似した処理の数に関係なく、24時間ごとに1回のアクセス時間更新が許可されます。

を0に設定する `-atime-update-period`と、読み取りアクセスごとにメッセージが送信元に送信されます。送信

元は、atimeが古いことを各FlexCacheボリュームに通知します。これはパフォーマンスに影響します。

手順

1. 特権モードをに設定し `advanced`ます。

   ```
   set -privilege advanced
   ```

2. ファイルアクセス時間の更新を有効にし、更新頻度を設定します。

   ```
   volume modify -volume vol_name -vserver <SVM name> -atime-update true -atime
   -update-period <seconds>
   ```

   次に、86400秒（24時間）をイネーブルにして設定する `-atime-update-period`例を示します `-atime-update`。

   ```
   c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime
   -update-period 86400
   ```

3. が有効であることを確認し `-atime-update`ます。

   ```
   volume show -volume vol_name -fields atime-update,atime-update-period
   ```

   ```
   c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-
   update-period
   vserver volume         atime-update atime-update-period
   ------- -------------- ------------ -------------------
   vs2_c1  cache1_origin1 true         86400
   ```

4. を有効にすると `-atime-update`、FlexCacheボリューム上のファイルを自動的にスクラビングできるかどうか、およびスクラビング間隔を指定できます。

   ```
   volume flexcache config modify -vserver <SVM name> -volume <volume_name> -is
   -atime-scrub-enabled <true|false> -atime-scrub-period <integer>
   ```

パラメータの詳細については `-is-atime-scrub-enabled`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP FlexCacheボリュームでのグローバルファイルロックの有効化

ONTAP 9 .10.1以降では、グローバルファイルロックを適用して、関連するすべてのキャッシュファイルの読み取りを防止できます。

グローバルファイルロックを有効にすると、すべてのFlexCacheボリュームがオンラインになるまで元のボリュームに対する変更が中断されます。グローバルファイルロックは、FlexCacheボリュームがオフラインのときに変更が一時停止され、タイムアウトが発生する可能性があるために、キャッシュと元の間の接続の信頼性を制御できる場合にのみ有効にしてください。

開始する前に

- グローバルファイルロックでは、元のキャッシュと関連するすべてのキャッシュを含むクラスタでONTAP 9 .9.1以降が実行されている必要があります。グローバルファイルロックは、新規または既存のFlexCacheボリュームで有効にできます。このコマンドは1つのボリュームに対して実行でき、関連付けられているすべてのFlexCacheに適用されます。
- グローバルファイルロックを有効にするには、advanced権限レベルが必要です。
- ONTAP 9.9.1より前のバージョンにリバートする場合は、最初に送信元キャッシュと関連するキャッシュでグローバルファイルロックを無効にする必要があります。無効にするには、元のボリュームから次のコマンドを実行します。 `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- グローバルファイルロックを有効にするプロセスは、オリジンに既存のキャッシュがあるかどうかによって異なります。
  - [enable-gfl-new]
  - [enable-gfl-existing]

新しい**FlexCache**ボリュームでグローバルファイルロックを有効にする

手順

1. trueに設定してFlexCacheボリュームを作成し `-is-global-file-locking`ます。

   ```
   volume flexcache create volume volume_name -is-global-file-locking-enabled true
   ```

   のデフォルト値 `-is-global-file-locking`は"`false`"です。以降のコマンドをボリュームに対して実行する場合 `volume flexcache create`は、「true」に設定して渡す必要があります `-is-global-file-locking enabled`。

既存の**FlexCache**ボリュームでグローバルファイルロックを有効にする

手順

1. グローバルファイルロックは元のボリュームから設定する必要があります。
2. 他の既存の関係（SnapMirrorなど）を元のボリュームに含めることはできません。既存の関係はすべて解除する必要があります。コマンドの実行時にすべてのキャッシュとボリュームが接続されている必要があります。接続ステータスを確認するには、次のコマンドを実行します。

   ```
   volume flexcache connection-status show
   ```

   表示されたすべてのボリュームのステータスがと表示されます `connected.`。詳細については、またはを参照してください"FlexCache 関係のステータスを確認します""元のボリュームから FlexCache ボリュームのプロパティを同期する"。

3. キャッシュでグローバルファイルロックを有効にします。

   ```
   volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true
   ```

関連情報

- "ONTAPコマンド リファレンス"

ONTAP FlexCacheボリュームへのデータの事前取り込み

FlexCacheボリュームにデータを事前に取り込むことで、キャッシュされたデータへのアクセスにかかる時間を短縮できます。

開始する前に

- advanced権限レベルのクラスタ管理者である必要があります。
- 事前取り込みに渡すパスが存在している必要があります。存在していないと、事前取り込み処理は失敗します。

タスクの内容

- 事前取り込みはファイルのみを読み取り、ディレクトリをクロールする
- フラグは、事前取り込み用に渡されたディレクトリのリスト全体に適用されます。 `-isRecursion`

手順

1. FlexCacheボリュームにデータを事前に取り込みます。

   ```
   volume flexcache prepopulate -cache-vserver vserver_name -cache-volume -path
   -list path_list -isRecursion true|false
   ```

   - `-path-list`パラメータは、元のルートディレクトリから始まる、事前に取り込む相対ディレクトリパスを指定します。たとえば、元のルートディレクトリの名前が`/origin`で、ディレクトリ`/origin/dir1`と`/origin/dir2`が含まれている場合は、パスリストを次のように指定できます。または `-path-list /dir1, /dir2。 -path-list dir1, dir2`
   - パラメータのデフォルト値 `-isRecursion`はTrueです。

     次の例では、1つのディレクトリパスが事前に入力されています。

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1
       (volume flexcache prepopulate start)
     [JobId 207]: FlexCache prepopulate job queued.
     ```

     次の例では、複数のディレクトリからファイルが事前に取り込まれています。

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
       (volume flexcache prepopulate start)
     [JobId 208]: FlexCache prepopulate job queued.
     ```

     次の例では、1つのファイルが事前に読み込まれています。

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1/file1.txt
  (volume flexcache prepopulate start)
[JobId 209]: FlexCache prepopulate job queued.
```

次の例では、オリジンからすべてのファイルが事前に読み込まれています。

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
  (volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

この例には、事前取り込み用の無効なパスが含まれています。

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
  (volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
       "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. 読み取りファイル数を表示します。

```
job show -id job_ID -ins
```

関連情報

- "ジョブの表示"

ONTAP FlexCache関係を削除する

FlexCacheが不要になった場合は、FlexCache関係とFlexCacheボリュームを削除できます。

手順

1. FlexCacheボリュームがあるクラスタから、FlexCacheボリュームをオフラインにします。

```
volume offline -vserver svm_name -volume volume_name
```

2. FlexCacheボリュームを削除します。

```
volume flexcache delete -vserver svm_name -volume volume_name
```

元のボリュームとFlexCacheボリュームからFlexCache関係の詳細が削除されます。

FlexCacheによるホットスポット修復

ONTAP FlexCacheボリュームを使用したハイパフォーマンスコンピューティングワークロードにおけるホットスポットの修正

アニメーションレンダリングやEDAなど、多くのハイパフォーマンスコンピューティングワークロードで共通する問題はホットスポットです。ホットスポットは、クラスタまたはネットワークの特定の部分の負荷が他の領域と比較して著しく高い場合に発生する状況です。その結果、パフォーマンスのボトルネックが発生し、その場所に集中した過剰なデータトラフィックが原因で全体的な効率が低下します。たとえば、1つまたは複数のファイルが実行中のジョブに対して高い需要があるため、（ボリュームアフィニティ経由で）そのファイルへの要求を処理するために使用されるCPUでボトルネックが発生します。FlexCacheはこのボトルネックの解消に役立ちますが、適切に設定する必要があります。

このドキュメントでは、ホットスポットを修正するためのFlexCacheの設定方法について説明します。

2024年7月以降、これまでPDFとして公開されていたテクニカルレポートの内容がONTAPの製品ドキュメントに統合されました。このONTAPホットスポット修正テクニカルレポートの内容は、発行日時点でまったく新しいものであり、それ以前の形式は作成されていません。

主な概念

ホットスポットの修復を計画する際には、これらの重要な概念を理解することが重要です。

- 高密度**FlexCache**（**HDF**）：キャッシュ容量の要件で許容される数のノードにまたがるように凝縮されたFlexCache
- * HDFアレイ（HDFA）*：同じオリジンのキャッシュで構成され、クラスタ全体に分散されるHDFSのグループ
- * SVM間HDFA *：サーバ仮想マシン（SVM）ごとにHDFAから1つのHDF
- * SVM内HDFA *：1つのSVM内のHDFA内のすべてのHDFS
- * East-Westトラフィック*：間接データアクセスによって生成されるクラスタバックエンドトラフィック

次のステップ

- "高密度FlexCacheを使用してホットスポットの修復を支援する方法を理解する"
- "FlexCacheアレイ密度の決定"
- "HDFSの密度を確認し、SVM間HDFAとSVM内HDFAを使用してNFSを使用してHDFSにアクセスするかどうかを決定します。"
- "ONTAP構成でクラスタ内キャッシングを使用するメリットを実現するために、HDFAとデータLIFを設定する"
- "クライアント設定でONTAP NAS接続を分散するようにクライアントを設定する方法について説明します。"

ONTAP FlexCacheホットスポット修復ソリューションの設計

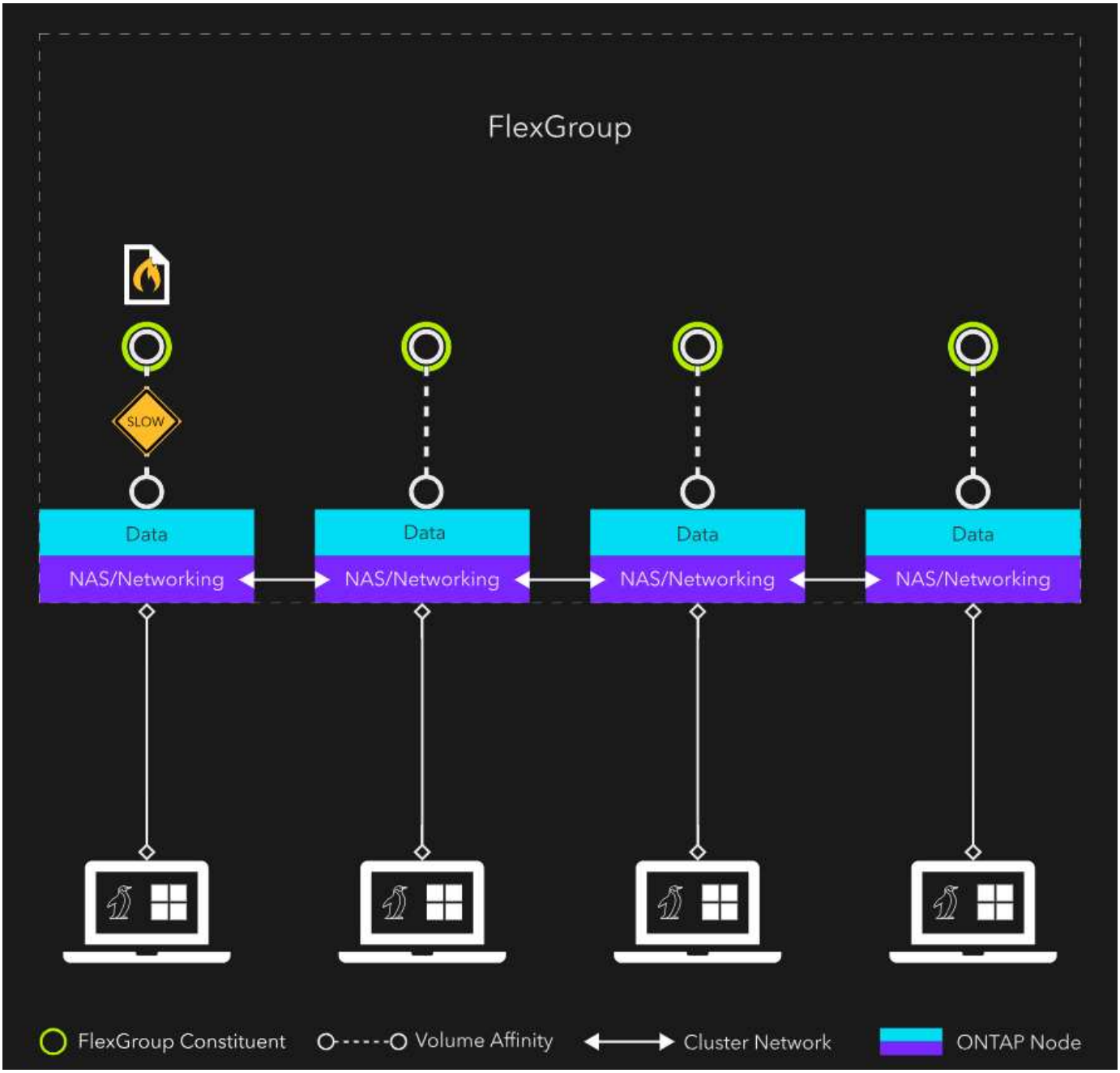
ホットスポットの問題を修正するには、ボトルネックの根本的な原因、自動プロビジョニングされたFlexCacheでは不十分な理由、FlexCacheソリューションを効果的に設計するために必要な技術的な詳細を確認します。高密度FlexCacheアレイ（HDFA）を理解して実装することで、パフォーマンスを最適化し、負荷の高いワークロードのボトルネックを解消できます。

ボトルネックの把握

次に、イメージ（ Image ）一般的なシングルファイルホットスポットのシナリオを示します。このボリュームは、各ノードにコンスティチュエントが1つだけ含まれるFlexGroupであり、ファイルはノード1に格納されます。

すべてのNASクライアントのネットワーク接続をクラスタ内の異なるノードに分散しても、ホットファイルが存在するボリュームアフィニティを提供するCPUのボトルネックは解消されません。また、ファイルが存在する以外のノードに接続されているクライアントからのコールに、クラスタネットワークトラフィック（イースト/ウェストトラフィック）を導入します。イースト/ウェストトラフィックのオーバーヘッドは通常は小さいですが、ハイパフォーマンスコンピューティングワークロードの場合は少しずつ考慮されます。

図**1**：**FlexGroup**の単一ファイルホットスポットのシナリオ

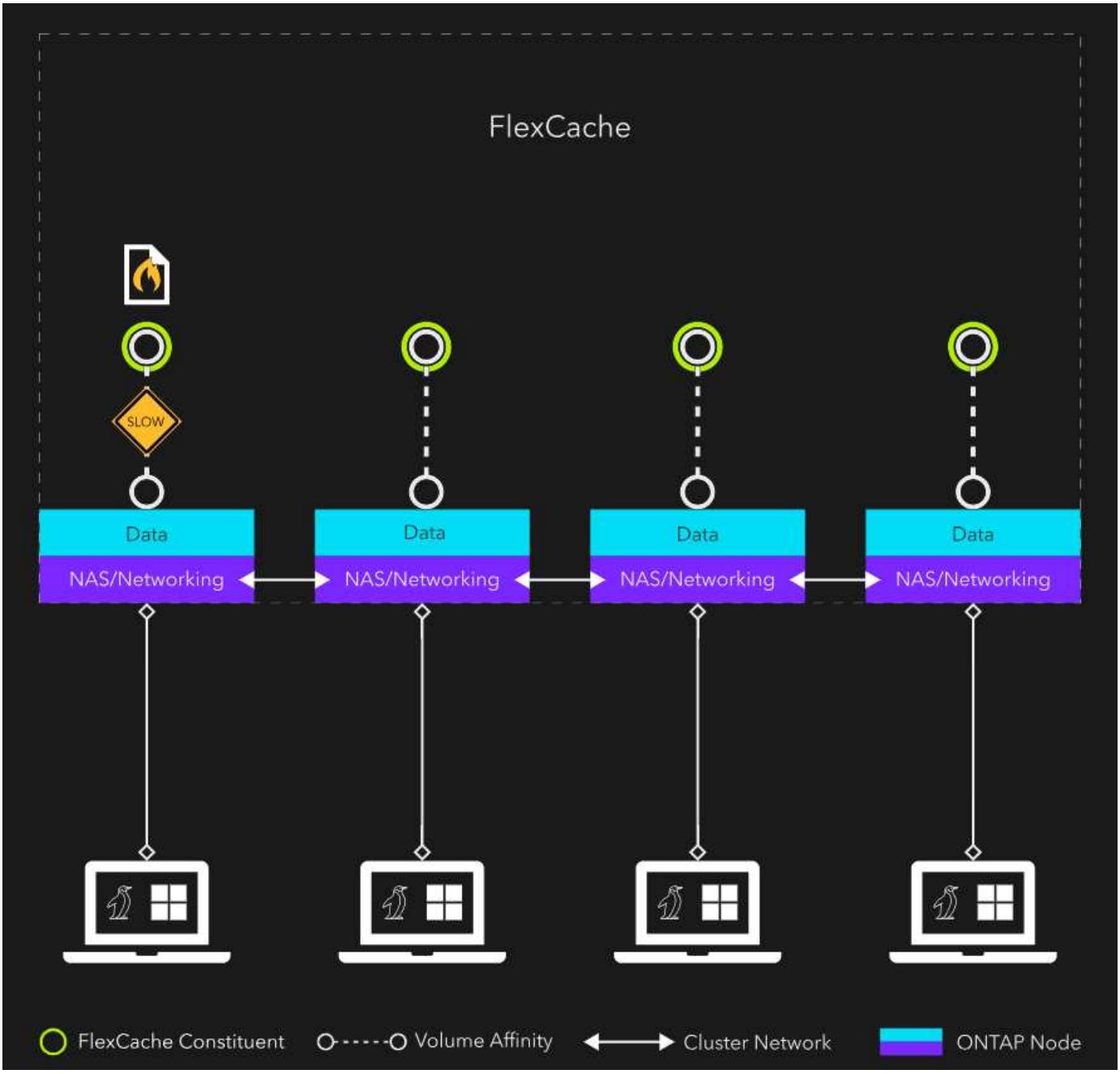


自動プロビジョニングされた**FlexCache**が答えにならない理由

ホットスポットの問題を解決するには、CPUのボトルネックを解消し、できれば東西のトラフィックも解消します。適切に設定されていれば、FlexCacheが役立ちます。

次の例では、 FlexCacheは System Manager、 NetAppコンソール、またはデフォルトの CLI 引数を使用して自動プロビジョニングされます。図1そして図2一見同じように見えます。どちらも 4 つのノードを持つ単一構成要素の NAS コンテナです。唯一の違いは、図 1 の NAS コンテナがFlexGroupであり、図 2 の NAS コンテナがFlexCacheである点です。各図は同じボトルネックを示しています。つまり、ホット ファイルへのアクセスを提供するボリューム アフィニティ用のノード 1 の CPU と、レイテンシに寄与する東西トラフィックです。自動プロビジョニングされたFlexCacheではボトルネックは解消されません。

図**2**：自動プロビジョニング**FlexCache**のシナリオ



FlexCacheの構造

ホットスポットの修復のためにFlexCacheを効果的に設計するには、FlexCacheに関する技術的な詳細を理解する必要があります。

FlexCacheは常にスパースFlexGroupです。FlexGroupは複数のFlexVolで構成されます。このFlexVolのことをFlexGroupコンスティチュエントと呼びます。デフォルトのFlexGroupレイアウトでは、クラスタ内のノードごとに1つ以上のコンスティチュエントがあります。コンスティチュエントは抽象化レイヤの下で「縫い合わせ」され、単一の大規模なNASコンテナとしてクライアントに提供されます。ファイルがFlexGroupに書き込まれると、取り込みのヒューリスティックによって、ファイルを格納するコンスティチュエントが決定されます。クライアントのNAS接続を含むコンスティチュエントでも別のノードでもかまいません。すべてが抽象化レイヤの下で動作し、クライアントからは見えないため、この場所は無関係です。

このFlexGroupの理解をFlexCacheに適用してみましょう。FlexCacheはFlexGroup上に構築されているため、に示すように、デフォルトでは、クラスタ内のすべてのノードにコンスティチュエントを含むFlexCacheが1

つだけ存在し図1ます。ほとんどの場合、これは素晴らしいことです。クラスタ内のすべてのリソースを利用している。

ただし、ホットファイルの修正には、単一ファイルのCPUとイースト/ウェストトラフィックの2つのボトルネックがあるため、これは理想的ではありません。ホットファイルの各ノードのコンスティチュエントで構成されるFlexCacheを作成した場合、そのファイルはそのうちの1つのコンスティチュエントにのみ配置されます。これは、ホットファイルへのすべてのアクセスを処理するCPUが1つあることを意味します。また、ホットファイルに到達するために必要なイースト/ウェストトラフィックの量も制限する必要があります。

このソリューションは、多数の高密度FlexCachesで構成されています。

高密度**FlexCache**の構造

高密度FlexCache（HDF）では、キャッシュされたデータの容量要件が許容される数のノードにコンスティチュエントが配置されます。目的は、キャッシュを単一のノードに配置することです。容量の要件によってそれが不可能になった場合は、コンスティチュエントを少数のノードにしか配置できません。

たとえば、24ノードクラスタでは、次の3つの高密度FlexCachesを使用できます。

- ノード1~8にまたがるノード
- ノード9~16にまたがる秒
- 3分の1はノード17~24にまたがっています。

これら3つのHDFSは、1つの高密度FlexCacheアレイ（HDFA）を構成します。ファイルが各HDF内に均等に分散されている場合、クライアントから要求されたファイルがフロントエンドNAS接続に対してローカルに存在する可能性が8分の1になります。それぞれ2つのノードにまたがる12個のHDFSを使用する場合、ファイルがローカルである可能性は50%です。HDFを1つのノードに縮小して24個のノードを作成できれば、ファイルがローカルであることが保証されます。

この構成により、すべてのEast-Westトラフィックが排除され、最も重要なことは、ホットファイルにアクセスするために24個のCPU/ボリュームアフィニティが提供されることです。

次の手順

"FlexCacheアレイ密度の決定"

関連情報

"FlexGroupおよびTRに関するドキュメント"

ONTAP FlexCache密度の決定

最初のホットスポット修復設計の決定は、FlexCache密度を把握することです。次の例は4ノードクラスタです。ファイル数が各HDFのすべてのコンスティチュエントに均等に分散されているとします。また、すべてのノードにフロントエンドNAS接続が均等に分散されていると仮定します。

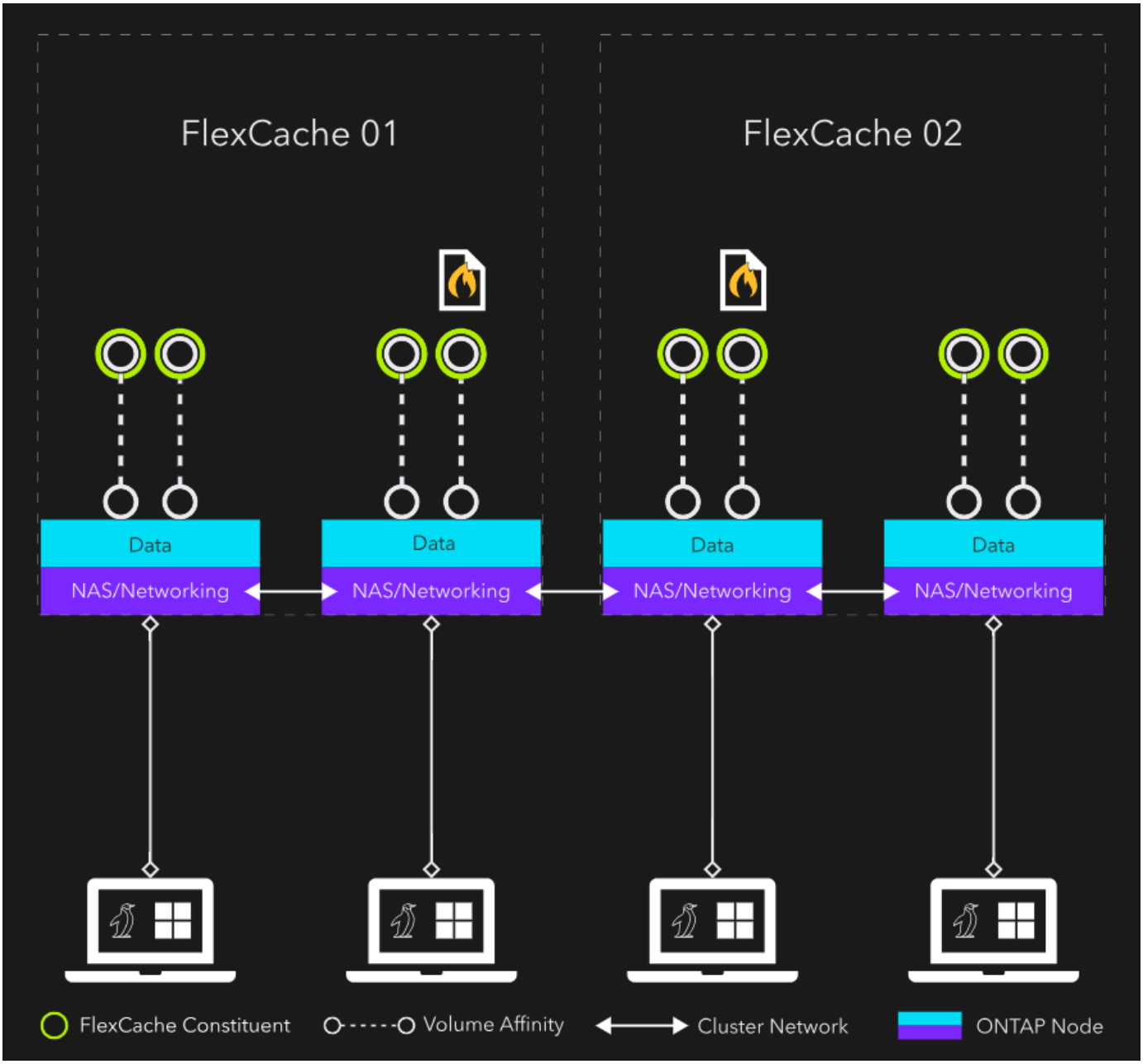
使用できる構成はこれらの例だけではありませんが、スペース要件と使用可能なリソースで許容される数のHDFSを作成するための設計原則を理解しておく必要があります。

HDFAは、次の構文で表されます。 `HDFs per HDFA x nodes per HDF x constituents per node per HDF`

2x2x2 HDFAノセツテイ

図1は、2x2x2のHDFA構成の例です。2つのHDFSがそれぞれ2つのノードにまたがり、各ノードに2つのコンスティチュエントボリュームが含まれています。この例では、各クライアントがホットファイルに直接アクセスできる可能性は50%です。4つのクライアントのうち2つがイーストウェストトラフィックを持っています。重要なことは、HDFSが2つになったことです。つまり、ホットファイルには2つの個別のキャッシュがあります。これで、ホットファイルへのアクセスを提供する2つのCPU /ボリュームアフィニティが確立されました。

図1：2x2x2 HDFA構成

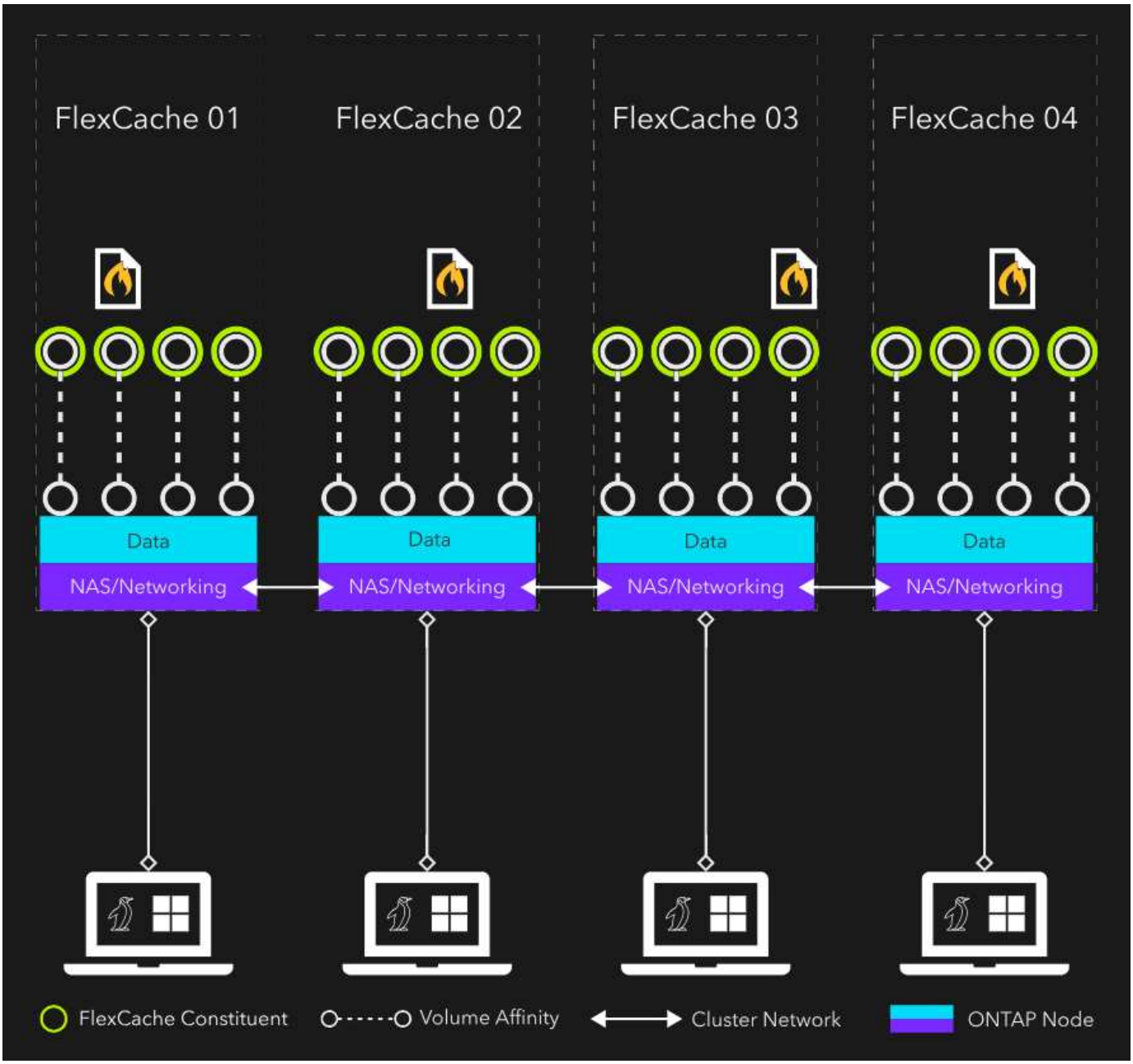


4x1x4 HDFAノセツテイ

図2は、最適な構成を表します。これは、4x1x4のHDFA構成の例です。4つのHDFSがそれぞれ1つのノードに含まれ、各ノードに4つのコンスティチュエントが含まれます。この例では、各クライアントがホットファイルのキャッシュに直接アクセスできることが保証されています。4つの異なるノードに4つのキャッシュファイルがあるため、4つの異なるCPU /ボリュームアフィニティがホットファイルへのサービスアクセスに役立

ちます。また、イースト/ウェストトラフィックは生成されません。

図2：4x1x4 HDFA構成



次のステップ

HDFSの密度を決定したら、NFSを使用してHDFSにアクセスする場合は、設計上の別の決定を行う必要があります"SVM間HDFAとSVM内HDFA"。

ONTAPのSVM間またはSVM内のHDFAオプションを決定する

HDFSの密度を確認したら、NFSを使用してHDFSにアクセスするかどうかを決定し、SVM間HDFAとSVM内HDFAのオプションについて学習します。

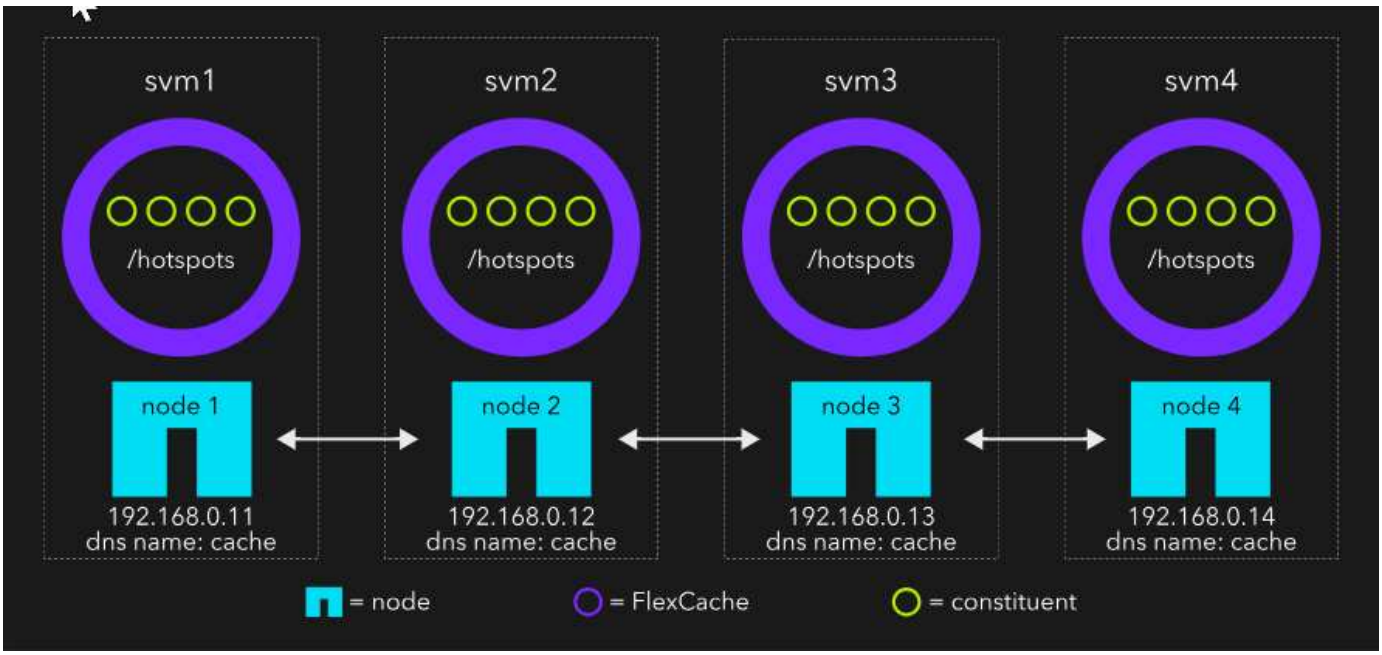
HDFSにアクセスするのがSMBクライアントだけの場合は、すべてのHDFSを1つのSVMに作成する必要があります。DFSターゲットを使用してロードバランシングを行う方法については、Windowsクライアントの設定を参照してください。

SVM間HDFAの導入

SVM間HDFAを使用するには、HDFA内のHDFごとにSVMを作成する必要があります。これにより、HDFA内のすべてのHDFSのジャンクションパスが同じになるため、クライアント側での設定が容易になります。

この例で図1は、各HDFが専用のSVMに配置されています。これはSVM間HDFA環境です。各HDFには/hotspotsのジャンクションパスがあります。また、すべてのIPにはホスト名キャッシュのDNS Aレコードがあります。この構成では、DNSラウンドロビンを使用して、異なるHDFS間でマウントの負荷を分散します。

図1：4x1x4のSVM間HDFA構成

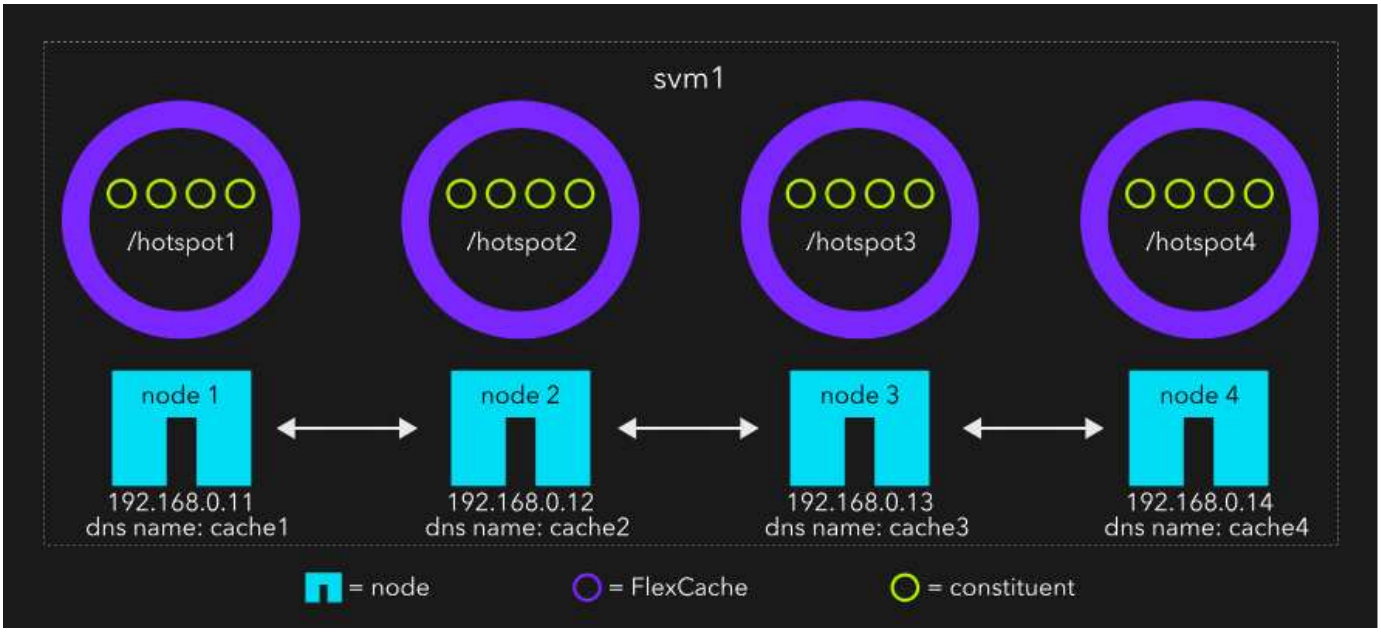


SVM内HDFAの導入

SVM内では、各HDFに一意のジャンクションパスが必要ですが、すべてのHDFSは1つのSVMに含まれます。このセットアップはONTAPでは1つのSVMしか必要ないため簡単ですが、ONTAPでおよびデータLIFを使用してLinux側でさらに高度な設定を行う必要があります `autofs`。

この例で図2は、すべてのHDFが同じSVM内にあります。これはSVM内HDFA環境であり、ジャンクションパスが一意である必要があります。ロードバランシングを適切に機能させるには、IPごとに一意のDNS名を作成し、ホスト名が解決されるデータLIFをHDFが存在するノードにのみ配置する必要があります。また、で説明されているように、複数のエントリを使用してを構成する必要があり `autofs`ます"Linuxクライアントノセツテイ"。

図2：4x1x4のSVM内HDFA構成



次のステップ

これで、HDFAをどのように展開するかがわかりました"HDFAを導入し、分散した方法でアクセスするようにクライアントを設定する"。

HDFAと**ONTAP**データ**LIF**の設定

このホットスポット修復ソリューションのメリットを実現するには、HDFAとデータLIFを適切に設定する必要があります。このソリューションでは、同じクラスタ内でオリジンとHDFAを使用したクラスタ内キャッシングが使用されます。

次に、2つのHDFAサンプル構成を示します。

- SVM間HDFA×2×2
- SVM内HDFA×4

タスクの内容

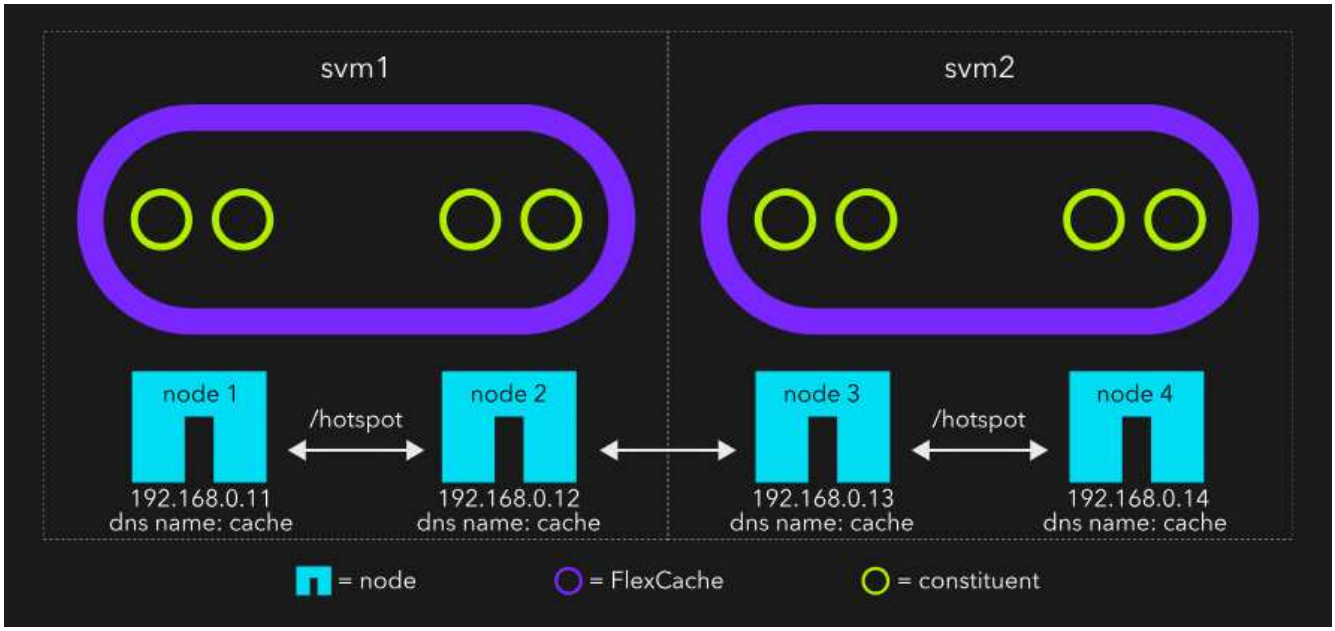
この高度な設定は、ONTAP CLIを使用して実行します。コマンドでは2つの設定を使用する必要があり`flexcache create`ます。また、が設定されていないことを確認する必要があります。

- `-aggr-list`：HDFを制限するノードまたはノードのサブセットにあるアグリゲート（アグリゲートのリスト）を指定します。
- `-aggr-list-multiplier`：オプションに表示されたアグリゲートごとに作成するコンスティチュエントの数を確認します `aggr-list`。アグリゲートが2つ表示されている場合にこの値をに設定すると、`2`コンスティチュエントが4つになります。NetAppでは、アグリゲートあたり最大8個のコンスティチュエントを推奨していますが、16個で十分です。
- `-auto-provision-as`：タブアウトすると、CLIは自動入力を試み、値をに設定します `flexgroup`。これが設定されていないことを確認してください。表示された場合は、削除します。

2x2x2の**SVM**間**HDFA**構成を作成

1. 図1に示すように、2x2x2のSVM間HDFAの構成を支援するために、準備シートを作成します。

図1：2x2x2のSVM間HDFAレイアウト



SVM	HDFあたりのノード数	アグリゲート	ノードあたりのコンスティチュエン	ジャンクションパス	データLIFのIP
svm1	node1、node2	aggr1、aggr2	2	/ホットスポット	192.168.0.11、192.168.0.12
svm2	node3、node4	aggr3、aggr4	2	/ホットスポット	192.168.0.13、192.168.0.14

2. HDFSを作成します。次のコマンドを、準備シートの各行に対して1回ずつ、2回実行します。2回目のイテレーションの値と `aggr-list`値を調整して `vserver`ください。

```
cache::> flexcache create -vserver svm1 -volume hotspot -aggr-list
aggr1,aggr2 -aggr-list-multiplier 2 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot
```

3. データLIFを作成します。このコマンドを4回実行し、準備シートに記載されているノードにSVMごとに2つのデータLIFを作成します。繰り返しごとに値を適切に調整してください。

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

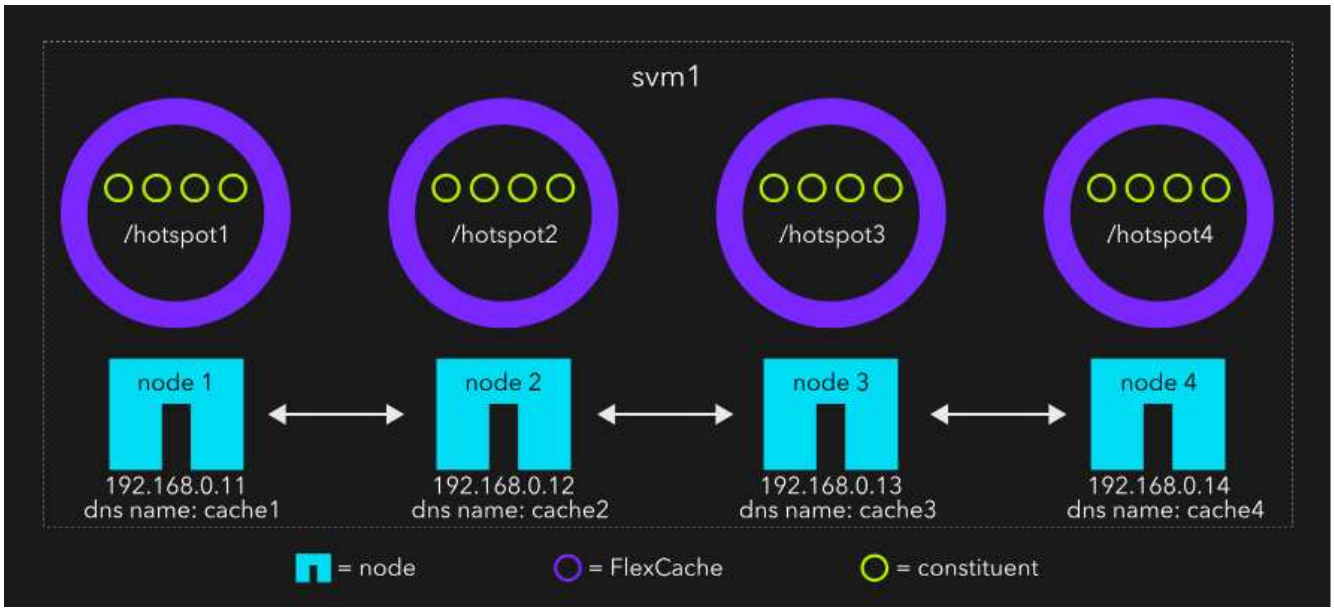
次のステップ

次に、HDFAを適切に利用するようにクライアントを設定する必要があります。を参照して "クライアントセツテイ"

SVM内HDFA（4x1x4）を作成

1. 図2に示すように、4x1x4のSVM間HDFAの構成を支援するために、準備シートに必要事項を記入してください。

   図2：**4x1x4**の**SVM**内**HDFA**レイアウト



SVM	HDFあたりのノード数	アグリゲート	ノードあたりのコンスティチュエン	ジャンクションパス	データLIFのIP
svm1	node1	アグリゲート1	4	/hotspot1	192.168.0.11
svm1	ノード2	aggr2	4	/hotspot2	192.168.0.12
svm1	node3	aggr3	4	/hotspot3	192.168.0.13
svm1	node4	aggr4	4	/hotspot4	192.168.0.14

2. HDFSを作成します。次のコマンドを、準備シートの各行に1回ずつ、4回実行します。各イテレーションの値と `junction-path`値は必ず調整して `aggr-list`ください。

```
cache::> flexcache create -vserver svm1 -volume hotspot1 -aggr-list
aggr1 -aggr-list-multiplier 4 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot1
```

3. データLIFを作成します。このコマンドを4回実行し、SVMに合計4つのデータLIFを作成します。ノードごとに1つのデータLIFが必要です。繰り返しごとに値を適切に調整してください。

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

次のステップ

次に、HDFAを適切に利用するようにクライアントを設定する必要があります。を参照して "クライアントセツテイ"

ONTAP NAS接続を分散するためのクライアントの設定

ホットスポットの問題を解決するには、CPUのボトルネックを回避するためにクライアントを適切に設定します。

Linuxクライアントノセツテイ

SVM内とSVM間のどちらのHDFA環境を選択した場合でも、Linuxでを使用して、異なるHDFS間でクライアントのロードバランシングが行われるようにする必要があります `autofs`。 `autofs`設定はSVM間とSVM内で異なります。

開始する前に

必要であり、適切な依存関係がインストールされている必要があります `autofs`。詳細については、Linuxのマニュアルを参照してください。

タスクの内容

ここで説明する手順では、次のエントリを持つサンプルファイルを使用し `/etc/auto_master`ます。

```
/flexcache auto_hotspot
```

これにより、プロセスがディレクトリにアクセスしようとするときに、ディレクトリ `/flexcache`内で `/etc`呼び出されるファイルを検索するように `auto_hotspot`設定され `autofs`ます。ファイルの内容 `auto_hotspot`によって、ディレクトリ内でマウントするNFSサーバとジャンクションパスが決まり `/flexcache`ます。ここで説明する例は、ファイルのさまざまな構成 `auto_hotspot`です。

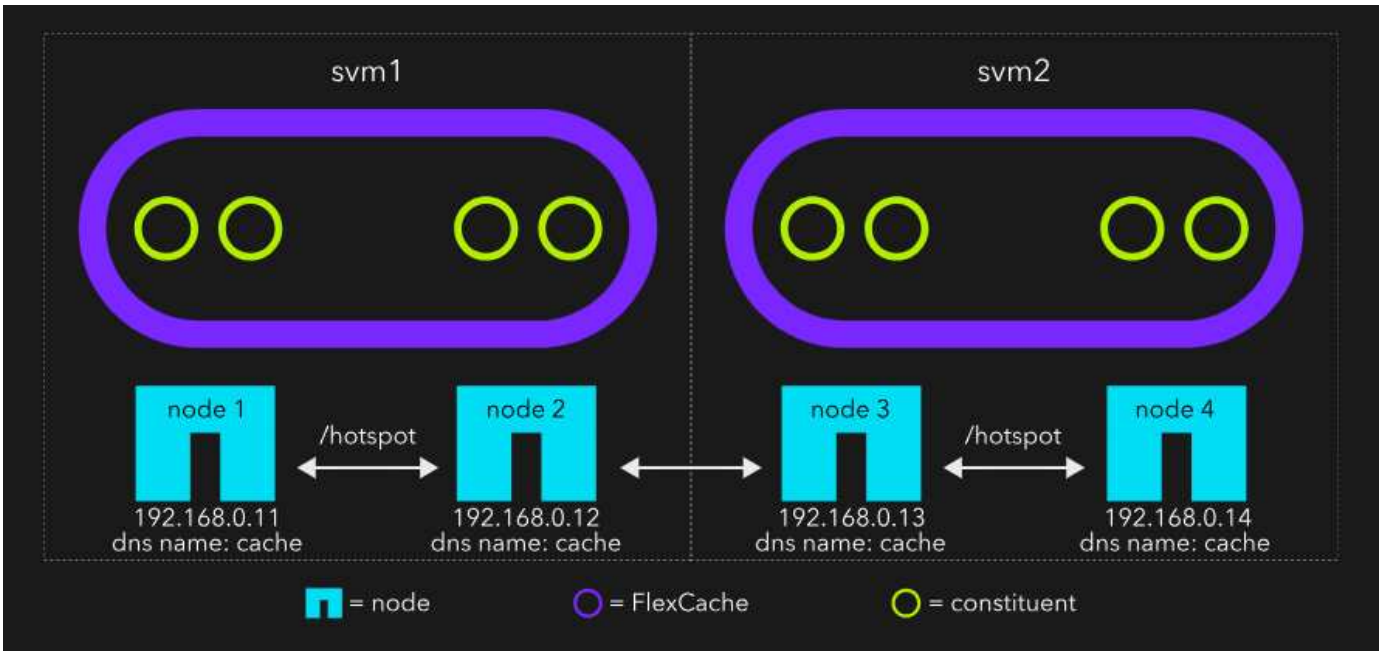
SVM内**HDFA autofs**設定

次の例では、の図のマップを作成し `autofs`図1ます。各キャッシュには同じジャンクションパスがあり、ホスト名には4つのDNS Aレコードがあるため、 `cache`必要なのは1行だけです。

```
hotspot cache:/hotspot
```

この1行だけで、NFSクライアントはホスト名のDNSルックアップを実行し `cache`ます。`DNS`は、`IP`をラウンドロビン方式で返すように設定されています。これにより、フロントエンド`NAS`接続が均等に分散されます。クライアントは`IP`を受信すると、ジャンクションパスをに `/flexcache/hotspot`マウントします `/hotspot`。SVM1、SVM2、SVM3、SVM4に接続することもできますが、特定のSVMは関係ありません。

図**1**：**2x2x2**の**SVM**間**HDFA**



SVM内HDFA autofs設定

次の例では、の図のマップを作成し `autofs`図2ます。HDFジャンクションパス環境に含まれるIPをNFSクライアントがマウントするようにする必要があります。つまり、IP 192.168.0.11以外でマウントしたくないということです `/hotspot1`。これを行うには、マップ内の1つのローカルマウントの場所について、4つのIP/ジャンクションパスのペアをすべてリストし `auto_hotspot`ます。

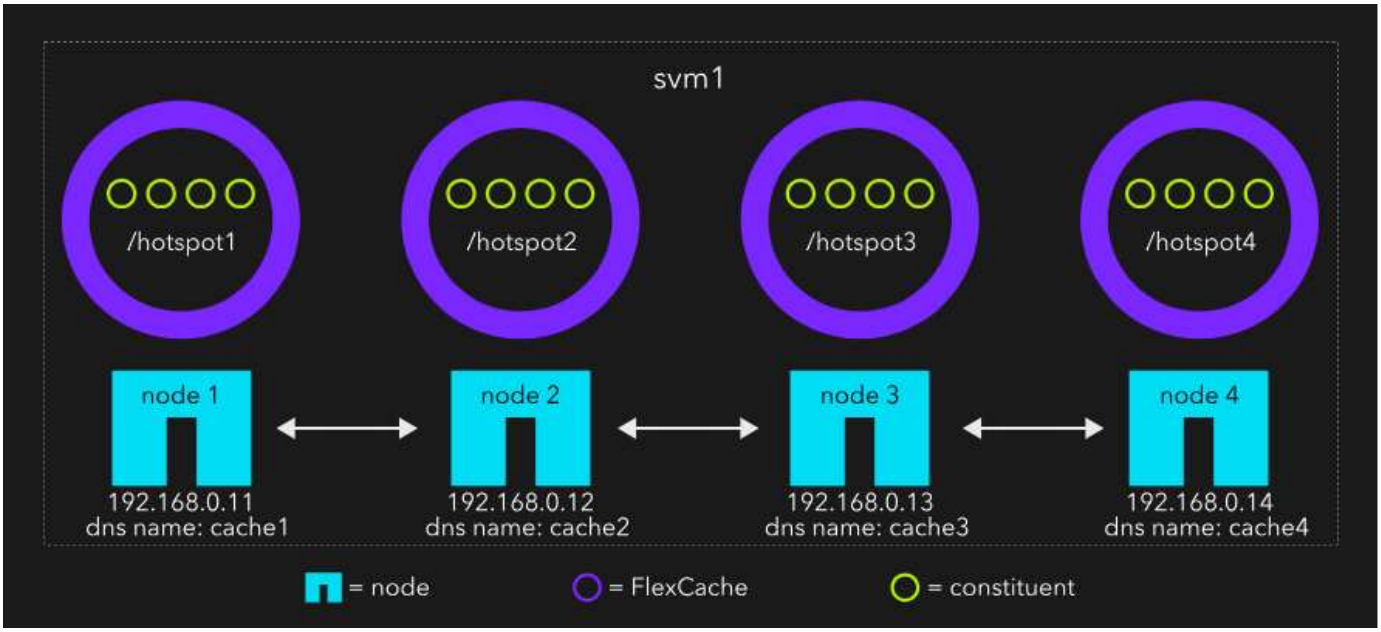
(`\`次の例のバックスラッシュ）は、エントリを次の行に続けて読みやすくします。

```
hotspot     cache1:/hostspot1 \
            cache2:/hostspot2 \
            cache3:/hostspot3 \
            cache4:/hostspot4
```

クライアントがにアクセスしようとすると `/flexcache/hotspot`、 `autofs`は4つのホスト名すべてに対して前方検索を実行します。4つのIPがすべてクライアントと同じサブネットにある場合、または別のサブネットにある場合、は `autofs`各IPにNFS NULL pingを発行します。

このNULL pingは、パケットをONTAPのNFSサービスで処理する必要がありますが、ディスクアクセスは必要ありません。最初に返されるpingはIPで、junction-pathが `autofs`mountを選択します。

図2：SVM内HDFA×4x1x4



Windowsクライアントセツテイ

Windowsクライアントでは、SVM内HDFAを使用する必要があります。SVM内の異なるHDFS間で負荷を分散するには、各HDFに一意の共有名を追加する必要があります。その後、の手順に従って、"Microsoftのドキュメント"同じフォルダに複数のDFSターゲットを実装します。

ネットワーク管理

開始する

System Managerを使用したONTAPネットワークの可視化

ONTAP 9 8以降では、System Managerを使用してネットワークのコンポーネントと構成を示す図を表示し、ホスト、ポート、SVM、ボリュームなどのネットワーク接続パスを確認できます。ONTAP 9 .12.1以降では、LIFとサブネットの関連付けをネットワークインターフェイスグリッドで表示できます。

この図は、**[ネットワーク]>[概要]***を選択するか、ダッシュボードの[ネットワーク]*セクションでを選択すると表示され → ます。

次のカテゴリのコンポーネントを図に示します。

- ホスト
- ストレージ ポート
- ネットワーク インターフェイス
- Storage VM
- データ アクセス コンポーネント

各セクションでは、カーソルを合わせて詳細情報を表示したり、ネットワークの管理タスクや設定タスクを実行したりすることができます。

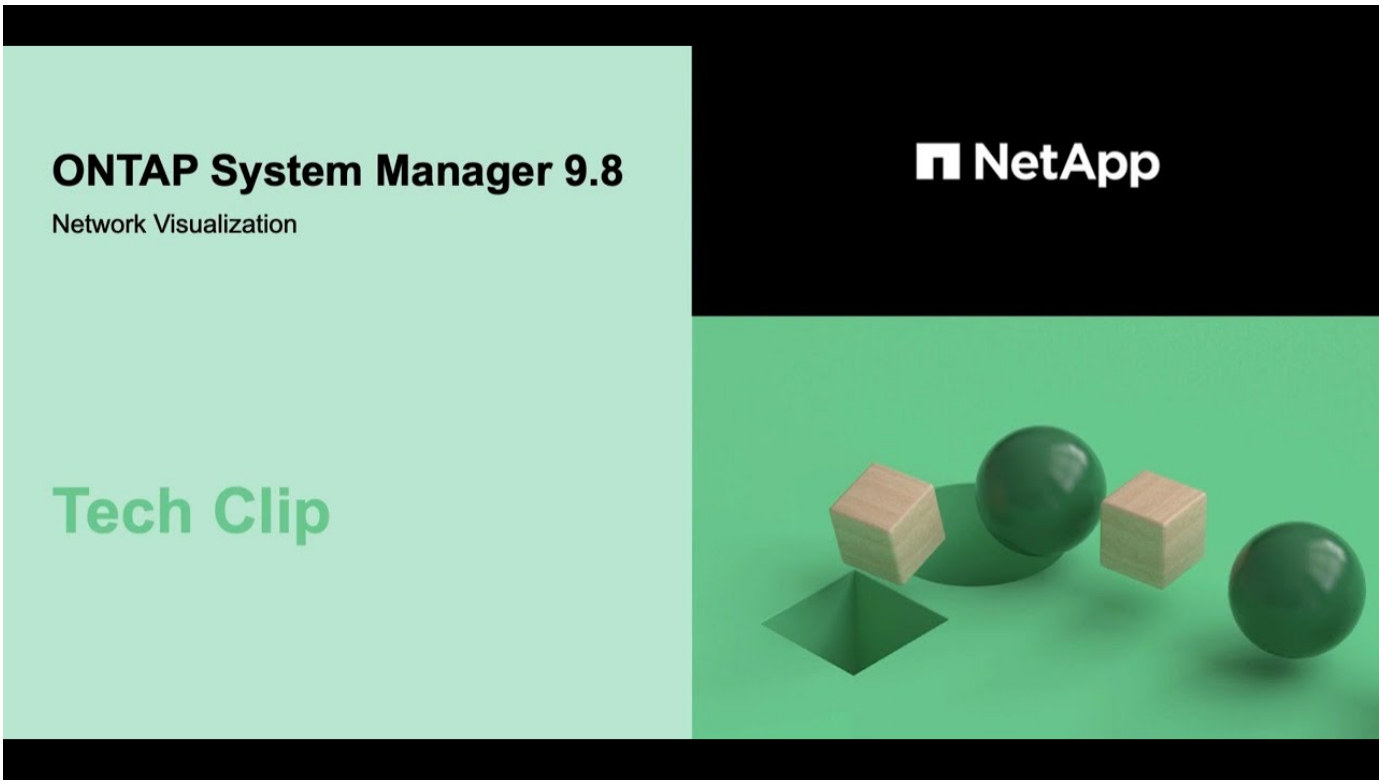
従来のSystem Manager（ONTAP 9 .7以前でのみ使用可能）を使用している場合は、を参照してください"ネットワークの管理"。

例

次に、各コンポーネントの詳細を表示したり、ネットワークを管理するためのアクションを開始したりするために図を操作する方法の例をいくつか示します。

- ホストをクリックすると、その構成（ポート、ネットワークインターフェイス、 Storage VM 、関連するデータアクセスコンポーネント）が表示されます。
- Storage VM内のボリューム数にカーソルを合わせて、ボリュームを選択して詳細を表示します。
- 過去1週間のパフォーマンスを表示するiSCSIインターフェイスを選択してください。
- コンポーネントの横にあるをクリックし ⋮ て、そのコンポーネントを変更するアクションを開始します。
- 正常でないコンポーネントの横に「X」が表示され、ネットワークで問題が発生する可能性がある場所をすばやく特定します。

System Managerネットワークの可視化ビデオ



ONTAPクラスタのネットワークコンポーネントの詳細

クラスタをセットアップする前に、クラスタのネットワークコンポーネントについて理解しておく必要があります。クラスタの物理ネットワークコンポーネントを論理コンポーネントに構成することで、ONTAPの柔軟性とマルチテナンシー機能を活かすことができます。

クラスタのさまざまなネットワークコンポーネントは次のとおりです。

- 物理ポート

  ネットワーク インターフェイス カード（NIC）とホスト バス アダプタ（HBA）は、各ノードから物理ネットワーク（管理ネットワークとデータ ネットワーク）への物理接続（イーサネットおよびFibre Channel）を提供します。

  サイトの要件、スイッチ情報、ポートのケーブル接続情報、およびコントローラのオンボードポートのケーブル接続については、のHardware Universeを参照してください "hwu.netapp.com"。

- 論理ポート

  論理ポートは仮想ローカルエリアネットワーク（VLAN）とインターフェイスグループで構成されます。インターフェイスグループは複数の物理ポートを1つのポートとして扱い、VLANは1つの物理ポートを複数の別 々 のポートに分割します。

- IPspace

  IPspaceを使用すると、クラスタ内のSVMごとに個別のIPアドレススペースを作成できます。これにより、管理上分離されたネットワークドメインに属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

- ブロードキャストドメイン

  ブロードキャストドメインはIPspace内に存在し、同じレイヤ2ネットワークに属する、クラスタ内の多数のノードからのネットワークポートグループを含んでいます。このグループのポートは、SVMでデータトラフィック用に使用されます。

- サブネット

  サブネットはブロードキャスト ドメイン内に作成され、同じレイヤ3サブネットに属するIPアドレスのプールを含んでいます。このIPアドレス プールにより、LIF作成時にIPアドレスが簡単に割り当てられるようになります。

- 論理インターフェイス

  論理インターフェイス（LIF）は、ポートに関連付けられたIPアドレスまたはワールドワイド ポート名（WWPN）です。フェイルオーバー グループ、フェイルオーバー ルール、ファイアウォール ルールなどの属性があります。LIFは、現在バインドされているポート（物理または論理）からネットワーク経由で通信します。

  クラスタ内のLIFのタイプには、データLIF、クラスタ対象管理LIF、ノード対象管理LIF、クラスタ間LIF、クラスタLIFがあります。LIFの所有権は、LIFを実装するSVMによって異なります。データLIFはデータSVMによって、ノード対象管理LIF、クラスタ対象管理LIF、およびクラスタ間LIFは管理SVMによって、クラスタLIFはクラスタSVMによって所有されます。

- DNSゾーン

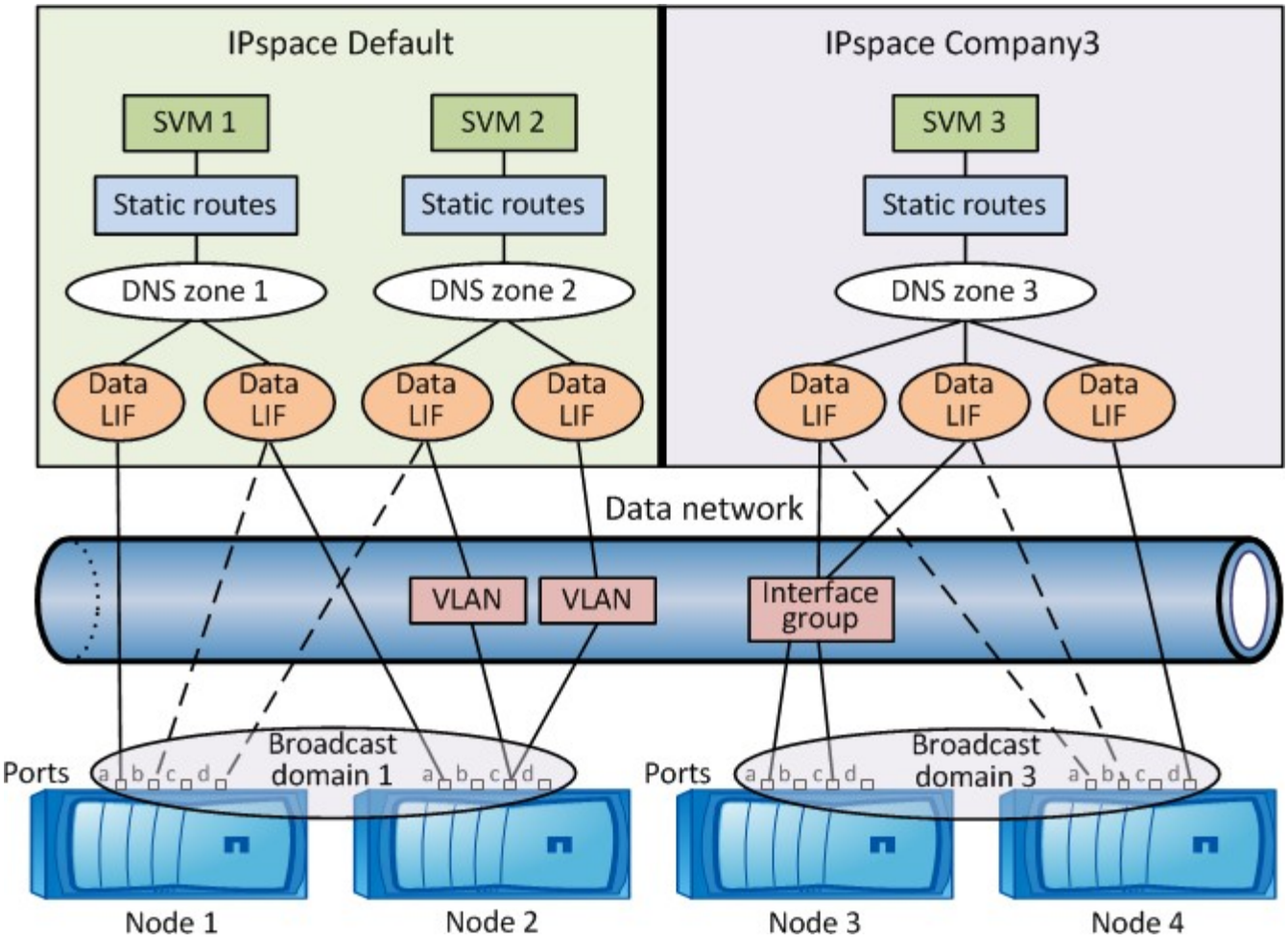
  DNSゾーンはLIFの作成時に指定でき、クラスタのDNSサーバ経由でエクスポートされるLIFの名前を提供します。複数のLIFで同じ名前を共有できるため、DNSロード バランシング機能を使用し、その名前のIPアドレスを負荷に従って分散させることができます。

  SVMには、複数のDNSゾーンを設定できます。

- ルーティング

  それぞれのSVMは、ネットワーク上で完全な機能を持つ独立した存在です。SVMは、LIFおよび設定済みの外部サーバに到達可能なルートを持っています。

  次の図は、4ノード クラスタにおける各種ネットワーク コンポーネントの関係を示しています。

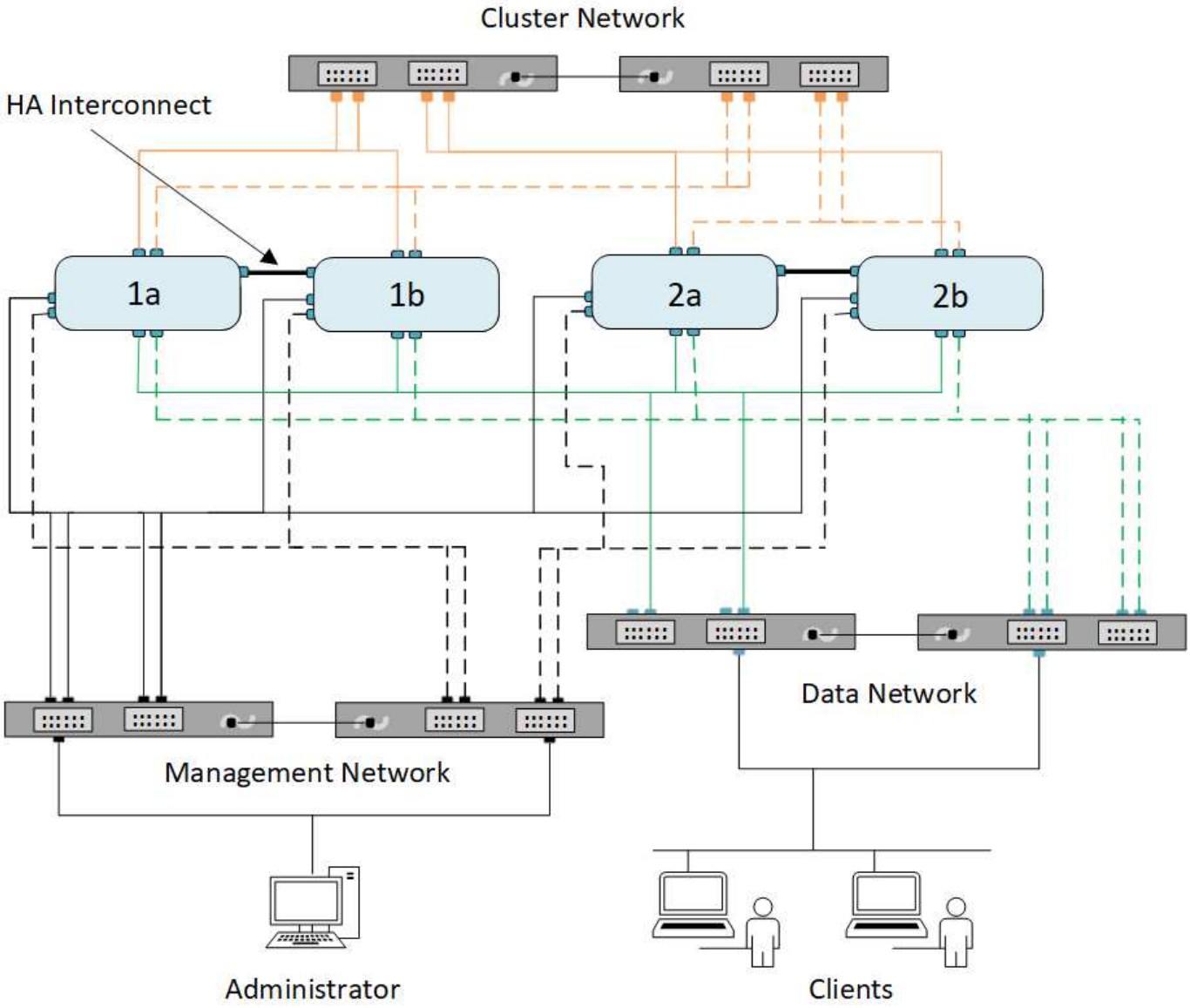


ONTAPネットワークケーブル接続のベストプラクティス

ネットワークケーブル配線のベストプラクティスでは、トラフィックがクラスタ、管理、データのネットワークに分離されます。

クラスタをケーブル配線するときは、クラスタのトラフィックが他のすべてのトラフィックとは別のネットワーク上にあるようにします。必須ではありませんが、ネットワーク管理トラフィックを、データとクラスタ内のトラフィックと分離することを推奨します。このようにネットワークを分離することにより、パフォーマンスとセキュリティが向上して管理しやすくなるだけでなく、ノードへの管理アクセスも簡単になります。

次の図は、3つのネットワークがある4ノードHAクラスタのネットワーク ケーブル配線を示しています。



ネットワーク接続のケーブル配線を行う際は、次のガイドラインに従う必要があります。

- 各ノードを3つの異なるネットワークに接続する必要があります。

  1つは管理用、1つはデータアクセス用、もう1つはクラスタ内通信用です。管理ネットワークとデータネットワークは論理的に分離できます。

- クライアント（データ）のトラフィックフローを改善するために、各ノードに複数のデータネットワーク接続を確立できます。
- クラスタは、データネットワーク接続なしで作成できますが、クラスタインターコネクト接続が含まれている必要があります。
- 各ノードへのクラスタ接続は常に2つ以上にする必要があります。

ネットワークのケーブル接続の詳細については、および "Hardware Universe"を参照して "AFF および FAS システムドキュメントセンター"ください。

ONTAPネットワークで使用するLIFフェイルオーバーポリシーを決定する

ブロードキャストドメイン、フェイルオーバーグループ、およびフェイルオーバーポリシーを組み合わせて、LIFが設定されているノードまたはポートで障害が発生した場合にどのポートがテイクオーバーするかを決定します。

ブロードキャストドメインは、同じレイヤ2イーサネットネットワーク内で到達可能なすべてのポートをリストします。いずれかのポートから送信されたイーサネットブロードキャストパケットは、ブロードキャストドメイン内の他のすべてのポートで認識されます。ブロードキャストドメインのこの共通到達可能性はLIFにとって重要です。LIFがブロードキャストドメイン内の他のポートにフェイルオーバーしても、元のポートから到達できたすべてのローカルホストとリモートホストに引き続き到達できるためです。

フェイルオーバーグループは、相互にLIFフェイルオーバーのカバレッジを提供するブロードキャストドメイン内のポートを定義します。各ブロードキャストドメインには、すべてのポートを含むフェイルオーバーグループが1つあります。ブロードキャストドメイン内のすべてのポートを含むこのフェイルオーバーグループが、LIFに対して推奨されるデフォルトのフェイルオーバーグループです。ブロードキャストドメイン内の同じリンク速度のポートで構成されるフェイルオーバーグループなど、定義するサブセットの数が少ないフェイルオーバーグループを作成できます。

フェイルオーバーポリシーは、ノードまたはポートが停止したときにLIFがフェイルオーバーグループのポートをどのように使用するかを定義します。フェイルオーバーグループに適用されるフィルタの一種として、フェイルオーバーポリシーが考えられます。LIFのフェイルオーバーターゲット（LIFがフェイルオーバーできるポートのセット）は、LIFのフェイルオーバーポリシーをブロードキャストドメイン内のLIFのフェイルオーバーグループに適用することで決まります。

LIFのフェイルオーバーターゲットは、次のCLIコマンドを使用して表示できます。

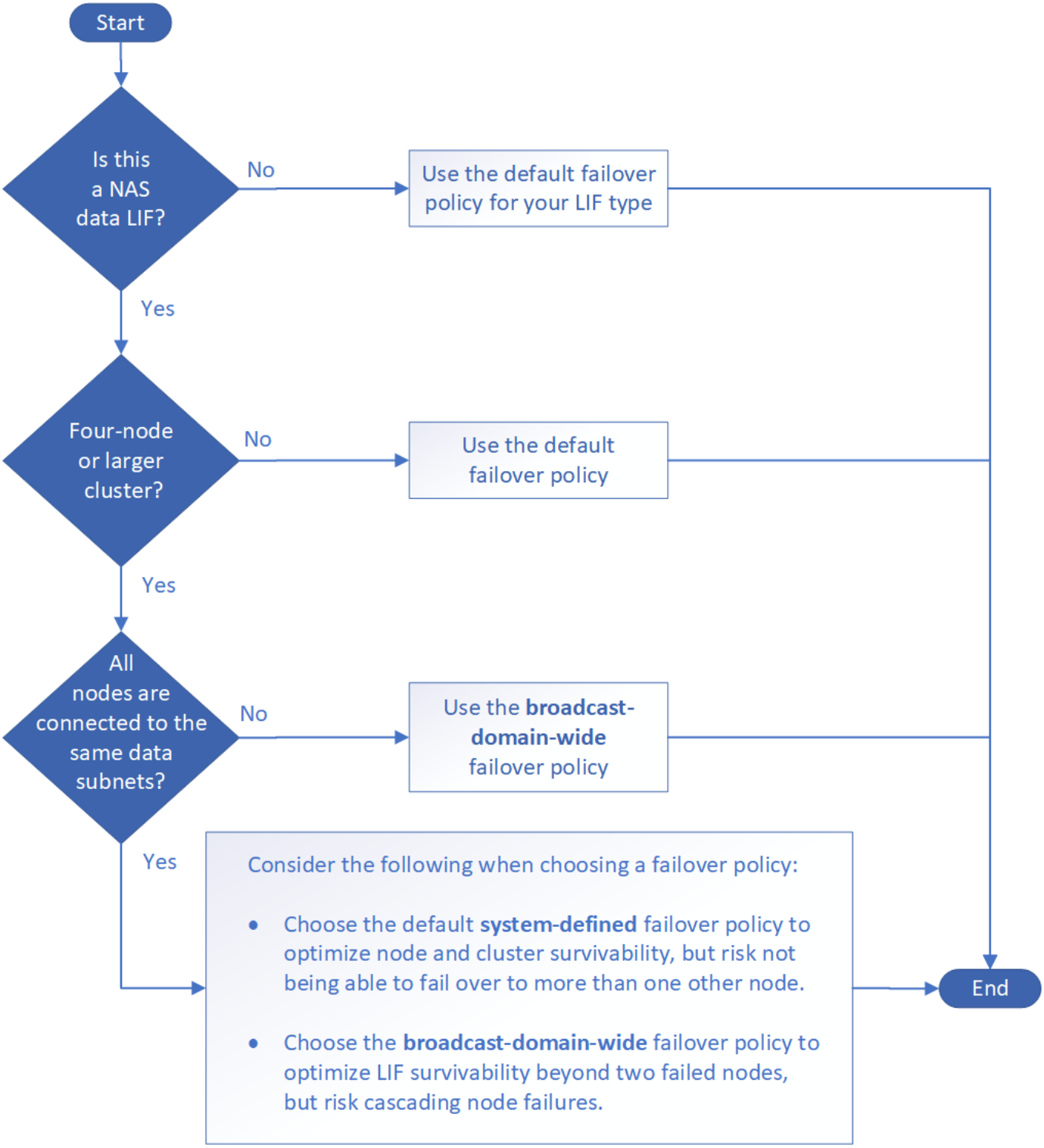
```
network interface show -failover
```

NetAppでは、LIFのタイプに応じたデフォルトのフェイルオーバーポリシーを使用することを強く推奨しています。

使用するLIFフェイルオーバーポリシーを決定する

推奨されるデフォルトのフェイルオーバーポリシーを使用するか、LIFのタイプと環境に基づいて変更するかを決定します。

フェイルオーバーポリシーのデシジョンツリー



LIFタイプ別のデフォルトのフェイルオーバーポリシー

LIFタイプ	デフォルトのフェイルオーバーポリシー	説明
BGPのLIF	無効	別のポートにフェイルオーバーしない。
クラスタLIF	ローカルのみ	LIFは、同じノードのポートにのみフェイルオーバーします。

クラスタ管理LIF	broadcast-domain-wide	クラスタ内のすべてのノードの同じブロードキャストドメイン内のポートにフェイルオーバーします。
クラスタ間LIF	ローカルのみ	LIFは、同じノードのポートにのみフェイルオーバーします。
NASデータLIF	システム定義	HAパートナーではないもう一方のノードにフェイルオーバーします。
ノード管理LIF	ローカルのみ	LIFは、同じノードのポートにのみフェイルオーバーします。
SANデータLIF	無効	別のポートにフェイルオーバーしない。

「sfo-partner-only」フェイルオーバーポリシーはデフォルトではありませんが、LIFをホームノードまたはSFOパートナーのポートにのみフェイルオーバーする場合に使用できます。

関連情報

- "network interface show"

NAS パスのフェイルオーバーワークフロー

ONTAPネットワークでのNASパスのフェイルオーバーの設定

ネットワークの基本概念をすでに理解している場合は、NASパスのフェイルオーバー設定に関するこの「ハンズオン」ワークフローを確認することで、ネットワークの設定にかかる時間を節約できます。

ONTAP 9.7以前のバージョンでは、NASパスのフェイルオーバーを設定するワークフローが異なります。ONTAP 9.7以前を実行するネットワークでNASフェイルオーバーを設定する必要がある場合は、ワークフローを参照して"NASパスのフェイルオーバー ワークフロー（ONTAP 9.7以前）"ください。

NAS LIFは、現在のポートでリンク障害が発生すると、稼働しているネットワーク ポートに自動的に移行します。ONTAPのデフォルトを利用してパスのフェイルオーバーを管理できます。

SAN LIFは移行されません（リンク障害後に手動で移動しないかぎり）。代わりに、ホストのマルチパステクノロジによってトラフィックが別のLIFに転送されます。詳細については、を参照してください "SAN管理"。

1 "ワークシートに記入する"

ワークシートを使用して、NASパスのフェイルオーバーを計画します。

2 **"IPspaceの作成"**

クラスタ内のSVMごとに個別のIPアドレススペースを作成します。

3 "IPspaceへのブロードキャストドメインの移動"

ブロードキャストドメインをIPspaceに移動します。

4 "SVMの作成"

クライアントにデータを提供するSVMを作成します。

5 "LIFの作成"

データへのアクセスに使用するポートにLIFを作成します。

6 "SVM用のDNSサービスの設定"

NFSサーバまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定してください。

ONTAPネットワークでのNASパスのフェイルオーバーに関するワークシート

NASパスのフェイルオーバーを設定する前に、ワークシートのすべてのセクションに情報を入力する必要があります。

ONTAP 9.7以前のバージョンでは、ONTAPネットワークでのNASフェイルオーバーに関する情報が異なります。ONTAP 9.7以前を実行するネットワークでNASフェイルオーバーを設定する必要がある場合は、を参照してください"NASパスのフェイルオーバー設定用ワークシート（ONTAP 9 .7以前）"。

IPspace設定

IPspaceを使用すると、クラスタ内のSVMごとに個別のIPアドレススペースを作成できます。これにより、管理上分離されたネットワークドメインに属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

情報	必須	自分の価値観
IPspace 名 IPspace の一意の識別子。	○	

ブロードキャストドメインの設定

ブロードキャストドメインは、同じレイヤ2ネットワークに属するポートをグループ化し、ブロードキャストドメインポートにMTUを設定します。

ブロードキャストドメインはIPspaceに割り当てられます。IPspaceには1つ以上のブロードキャストドメインを含めることができます。

LIFのフェイルオーバー先のポートは、LIFのフェイルオーバーグループのメンバーである必要があります。ONTAPで作成したブロードキャストドメインごとに、ブロードキャストドメイン内のすべてのポートを含む同じ名前のフェイルオーバーグループも作成されます。

情報	必須	自分の価値観
IPspace 名：ブロードキャストドメインを割り当てる IPspace 。 既存のIPspaceを指定する必要があります。	○	
ブロードキャストドメイン名ブロードキャストドメインの名前を指定します。 この名前はIPspace内で一意である必要があります。	○	
MTUブロードキャストドメインの最大伝送ユニット値。通常は* 1500 または 9000 *に設定されます。 MTU値は、ブロードキャストドメイン内のすべてのポートと、あとでブロードキャストドメインに追加されるすべてのポートに適用されます。 MTU値は、ネットワークに接続されているすべてのデバイスで同じである必要があります。管理トラフィックやサービス プロセッサのトラフィックを処理するe0Mポートについては、MTUを1500バイト以下に設定する必要があります。	○	
ポートは、到達可能性に基づいてブロードキャストドメインに割り当てられます。ポート割り当てが完了したら、コマンドを実行して到達可能性を確認します `network port reachability show`。 これらのポートには、物理ポート、VLAN、インターフェイスグループがあります。 の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。	○	

サブネット構成

サブネットにはIPアドレスのプールとデフォルトゲートウェイが含まれ、IPspace内のSVMで使用されるLIFに割り当てることができます。

- SVMでLIFを作成するときは、IPアドレスとサブネットを指定する代わりにサブネットの名前を指定できます。
- サブネットはデフォルトゲートウェイと一緒に設定できるため、SVMの作成時に別途デフォルトゲートウェイを作成する必要はありません。

- ブロードキャストドメインには1つ以上のサブネットを含めることができます。
- 複数のサブネットをIPspaceのブロードキャストドメインに関連付けることで、異なるサブネット上にあるSVM LIFを設定できます。
- 各サブネットには、同じIPspace内の他のサブネットに割り当てられたIPアドレスと重複しないIPアドレスを含める必要があります。
- サブネットを使用する代わりに、SVMデータLIFに特定のIPアドレスを割り当ててSVM用のデフォルトゲートウェイを作成することができます。

情報	必須	自分の価値観
IPspace 名：サブネットを割り当てる IPspace 。 既存のIPspaceを指定する必要があります。	○	
サブネット名：サブネットの名前。 この名前はIPspace内で一意である必要があります。	○	
ブロードキャストドメイン名サブネットを割り当てるブロードキャストドメインです。 このブロードキャストドメインは指定したIPspaceに存在する必要があります。	○	
サブネット名とマスク IP アドレスが存在するサブネットとマスクを指定します。	○	
Gateway ：サブネットのデフォルトゲートウェイを指定できます。 サブネットの作成時にゲートウェイを割り当てなかった場合は、あとでゲートウェイを割り当てることができます。	いいえ	
IP アドレス範囲： IP アドレスの範囲または特定の IP アドレスを指定できます。 たとえば、次のような範囲を指定できます。 `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` IPアドレスの範囲を指定しない場合、指定したサブネット内のすべての範囲のIPアドレスがLIFに割り当て可能になります。	いいえ	

LIF の関連付けを強制的に更新既存の LIF との関連付けを強制的に更新するかどうかを指定します。 デフォルトでは、サービスプロセッサインターフェイスまたはネットワークインターフェイスが指定した範囲のIPアドレスを使用している場合、サブネットの作成は失敗します。 このパラメータを使用すると、手動でアドレスを指定したインターフェイスがサブネットに関連付けられ、コマンドが成功します。	いいえ	

SVM構成

SVMを使用して、クライアントやホストにデータを提供します。

記録した値は、デフォルトのデータSVMを作成するためのものです。MetroClusterソースSVMを作成する場合は、またはを参照してください"Fabric-attached MetroCluster Installation and Configuration Guide""ストレッチ MetroCluster インストールおよび設定ガイド"。

情報	必須	自分の価値観
SVM 名 SVM の完全修飾ドメイン名（ FQDN ）。この名前は、クラスタリーグ全体で一意である必要があります。	○	
ルートボリューム名 SVM ルートボリュームの名前。	○	
アグリゲート名は、 SVM ルートボリュームを保持するアグリゲートの名前です。既存のアグリゲートを指定する必要があります	○	
SVM ルートボリュームのセキュリティ形式。指定できる値は、 * ntfs * 、 * unix * 、および * mixed * です。	○	
IPspace 名： SVM を割り当てる IPspace 。既存のIPspaceを指定する必要があります。	いいえ	
SVM の言語： SVM とそのボリュームで使用されるデフォルトの言語。ボリュームの言語を指定しなかった場合は、 SVM のデフォルトの言語設定は * C.UTF-8 * になります。SVMの言語の設定によって、SVM内のすべてのNASボリュームのファイル名とデータの表示に使用される文字セットが決まります。言語はSVMの作成後に変更できます。	いいえ	

LIFの構成

SVMは、1つ以上のネットワーク論理インターフェイス（LIF）を介してクライアントとホストにデータを提供します。

情報	必須	自分の価値観
SVM 名 LIF の SVM の名前。	○	
LIF の名前 LIF の名前。ノードに使用可能なデータポートがある場合は、ノードごとに複数のデータLIFを割り当てたり、クラスタ内の任意のノードにLIFを割り当てることができます。冗長性を確保するには、データサブネットごとに少なくとも2つのデータLIFを作成し、特定のサブネットに割り当てられたLIFには、異なるノードのホームポートを割り当てる必要があります。* 重要：ノンストップオペレーションソリューション用に Hyper-V または SQL Server over SMB をホストする SMB サーバを設定する場合、クラスタ内の SVM のすべてのノードに少なくとも 1 つのデータ LIF が存在する必要があります。	○	
LIF のサービスポリシーサービスポリシー。サービスポリシーは、LIFを使用できるネットワークサービスを定義します。データSVMとシステムSVMの両方のデータトラフィックと管理トラフィックの管理に組み込みのサービスとサービスポリシーを使用できます。	○	
許可されたプロトコル IP ベースの LIF では、許可されたプロトコルは必要ありません。代わりにサービスポリシーの行を使用してください。FibreChannelポートでSAN LIFに許可するプロトコルを指定してください。これらは、そのLIFを使用できるプロトコルです。LIFを使用するプロトコルは、LIFの作成後は変更できません。LIFの設定時にすべてのプロトコルを指定する必要があります。	いいえ	
ホームノード LIF がホームポートにリバートされるときに LIF が戻るノード。各データLIFのホームノードを記録する必要があります。	○	
ホームポートまたはブロードキャストドメインから次のいずれかを選択しました。 * Port * ：LIF がホームポートにリバートされるときに論理インターフェイスが戻るポートを指定します。この処理は、IPspaceのサブネット内の最初のLIFに対してのみ実行され、それ以外の場合は必要ありません。* ブロードキャストドメイン * ：ブロードキャストドメインを指定します。LIF がホームポートにリバートされるときに論理インターフェイスが戻る適切なポートがシステムによって選択されます。	○	
SVM に割り当てるサブネットの名前を指定します。アプリケーションサーバへの継続的可用性を備えたSMB接続を確立するために使用されるデータLIFは、すべて同じサブネット上にある必要があります。	○（サブネットを使用する場合）	

DNS構成

NFSまたはSMBサーバを作成する前に、SVMでDNSを設定する必要があります。

情報	必須	自分の価値観
SVM 名： NFS または SMB サーバを作成する SVM の名前。	○	
DNS ドメイン名ホストと IP の名前解決を行う際に、ホスト名に付加するドメイン名のリスト。最初にローカルドメインをリストし、次にDNSクエリが最も頻繁に実行されるドメイン名をリストします。	○	
DNS サーバの IP アドレス NFS サーバまたは SMB サーバの名前解決を提供する DNS サーバの IP アドレスのリスト。これらのDNSサーバには、Active DirectoryのLDAPサーバとSMBサーバが参加するドメインのドメインコントローラを見つけるために必要なサービスロケーションレコード（SRV）が含まれている必要があります。SRVレコードは、サービスの名前を、そのサービスを提供するサーバのDNSコンピュータ名にマッピングするために使用されます。ONTAPがローカルDNSクエリを介してサービスロケーションレコードを取得できない場合、SMBサーバの作成に失敗します。ONTAPがActive Directory SRVレコードを確実に見つけることができるようにする最も簡単な方法は、Active Directory統合DNSサーバをSVM DNSサーバとして設定することです。DNS管理者がActive Directoryドメインコントローラに関する情報を含むDNSゾーンにSRVレコードを手動で追加している場合は、Active Directoryに統合されていないDNSサーバを使用できます。Active Directoryに統合されたSRVレコードの詳細については、のトピックを参照してください"Microsoft TechNet での Active Directory の DNS サポートのしくみ"。	○	

動的DNS設定

動的DNSを使用してActive Directory統合DNSサーバにDNSエントリを自動的に追加する前に、SVMで動的DNS（DDNS）を設定する必要があります。

SVM上のすべてのデータLIFについてDNSレコードが作成されます。SVM上に複数のデータLIFを作成することで、割り当てられたデータIPアドレスへのクライアント接続の負荷を分散できます。DNSは、ホスト名を使用して確立された接続を、割り当てられたIPアドレスにラウンドロビン方式で負荷分散します。

情報	必須	自分の価値観
SVM 名： NFS または SMB サーバを作成する SVM 。	○	

DDNS を使用するかどうかで、 DDNS を使用するかどうかを指定します。SVMで設定されているDNSサーバがDDNSをサポートしている必要があります。デフォルトでは、DDNSは無効になっています。	○	
Secure DDNS を使用するかどうかは、 Active Directory 統合 DNS でのみサポートされます。Active Directory統合DNSでセキュアなDDNS更新のみが許可されている場合は、このパラメータの値をtrueにする必要があります。デフォルトでは、Secure DDNSは無効になっています。Secure DDNSは、SVM用のSMBサーバまたはActive Directoryアカウントが作成されたあとにのみ有効にできます。	いいえ	
DNS ドメインの FQDN DNS ドメインの FQDN です。SVMのDNSネームサービス用に設定されているドメイン名と同じ名前を使用する必要があります。	いいえ	

ネットワークポート

ONTAPネットワークポート設定の詳細

ポートは、物理ポート（NIC）または仮想ポート（インターフェイスグループやVLANなど）です。

仮想ポートは、仮想ローカルエリアネットワーク（VLAN）とインターフェイスグループで構成されます。インターフェイスグループは複数の物理ポートを1つのポートとして扱い、VLANは1つの物理ポートを複数の別々 の論理ポートに分割します。

- 物理ポート： LIF は物理ポートに直接設定できます。
- インターフェイスグループ：複数の物理ポートを含むポートアグリゲートで、 1 つのトランクポートとして機能します。インターフェイスグループには、シングルモード、マルチモード、またはダイナミックマルチモードがあります。
- VLAN ： VLAN タグ付き（ IEEE 802.1Q 規格）トラフィックを送受信する論理ポートです。VLANポートの特性には、ポートのVLAN IDが含まれます。基盤となる物理ポートまたはインターフェイスグループポートはVLANトランクポートとみなされ、接続するスイッチポートはVLAN IDをトランクするように設定する必要があります。

  VLANポートの基盤となる物理ポートまたはインターフェイスグループポートは、タグなしトラフィックを送受信するLIFを引き続きホストできます。

- 仮想 IP （ VIP ）ポート： VIP LIF のホームポートとして使用される論理ポート。VIPポートはシステムによって自動的に作成され、サポートされる処理は限られています。VIPポートはONTAP 9以降でサポートされています。5.

ポートの命名規則は *enumberletter* ：

- 最初の文字はポートタイプを表します。「e」はイーサネットを表します。

- 2文字目は、ポートアダプタのスロット番号を示します。
- 3文字目は、マルチポートアダプタでのポートの位置を示します。「a」は最初のポートを示し、「b」は2番目のポートを示します。以下同様に続きます。

たとえば、 `e0b`は、イーサネットポートであり、ノードのマザーボード上にある2番目のポートです。

VLANの名前には、という構文を使用する必要があり `port_name-vlan-id`ます。

`port_name`物理ポートまたはインターフェイスグループを示します。

`vlan-id`ネットワーク上のVLAN IDを指定します。たとえば、 `e1c-80`は有効なVLAN名です。

ネットワークポートの設定

物理ポートを組み合わせて**ONTAP**インターフェイスグループを作成する

インターフェイスグループはLink Aggregation Group（LAG；リンクアグリゲーショングループ）とも呼ばれ、同じノード上の複数の物理ポートを1つの論理ポートにまとめることで作成されます。論理ポートを使用すると、耐障害性と可用性が向上し、負荷も共有できます。

インターフェイス グループの種類

ストレージ システムでは、シングルモード、スタティック マルチモード、およびダイナミック マルチモードという3種類のインターフェイス グループがサポートされています。各インターフェイス グループは、フォールト トレランスのレベルが異なります。マルチモード インターフェイス グループは、ネットワーク トラフィックのロード バランシング方法を提供します。

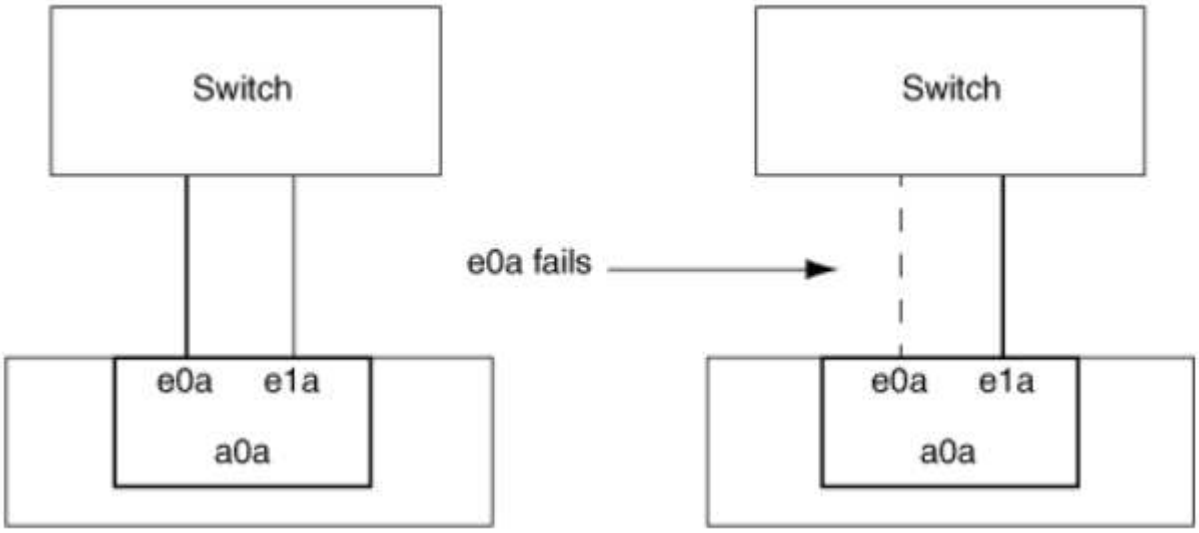
シングルモード インターフェイス グループの特性

シングルモード インターフェイス グループでは、インターフェイス グループの1つのインターフェイスだけがアクティブになります。他のインターフェイスはスタンバイで、アクティブなインターフェイスに障害が発生した場合に動作を引き継ぎます。

シングルモード インターフェイス グループの特性は、次のとおりです。

- フェイルオーバーでは、クラスタがアクティブ リンクを監視して、フェイルオーバーを制御します。クラスタがアクティブ リンクを監視するので、スイッチを設定する必要はありません。
- シングルモード インターフェイス グループには、複数のスタンバイ インターフェイスを設定できます。
- シングルモード インターフェイス グループが複数のスイッチをカバーする場合は、スイッチどうしをInter-Switch Link（ISL;スイッチ間リンク）で接続する必要があります。
- シングルモード インターフェイス グループでは、スイッチ ポートが同じブロードキャスト ドメインに属している必要があります。
- ポートが同じブロードキャスト ドメイン内にあるかどうかを確認するために、リンク監視用ARPパケット（送信元アドレスは0.0.0.0）がポートを介して送信されます。

次の図はシングルモード インターフェイス グループの例です。この例では、e0aとe1aがa0aというシングルモード インターフェイス グループを構成しています。アクティブ インターフェイスのe0aに障害が発生すると、スタンバイ インターフェイスのe1aが処理を引き継ぎ、スイッチとの接続を維持します。



シングルモード機能を実現するためには、フェイルオーバーグループを使用することを推奨します。フェイルオーバーグループを使用すると、2番目のポートを引き続き他のLIFに使用でき、未使用のままにする必要はありません。さらに、フェイルオーバーグループは3つ以上のポートにまたがることも、複数のノードのポートにまたがることもできます。

スタティックマルチモードインターフェイスグループの特性

ONTAPに実装されているスタティックマルチモードインターフェイスグループは、IEEE 802.3ad（static）に準拠しています。スタティックマルチモードインターフェイスグループでは、アグリゲートをサポートしているが、アグリゲートを設定するための制御パケット交換が行われていないスイッチを使用できます。

スタティックマルチモードインターフェイスグループは、Link Aggregation Control Protocol（LACP）とも呼ばれるIEEE 802.3ad（dynamic）に準拠していません。LACPは、Cisco独自のリンクアグリゲーションプロトコルであるポートアグリゲーションプロトコル（PAgP）に相当します。

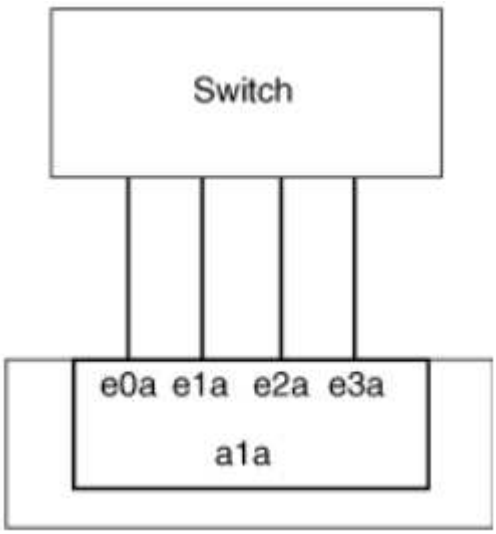
スタティックマルチモードインターフェイスグループの特性は次のとおりです。

- インターフェイスグループ内のすべてのインターフェイスがアクティブで、1つのMACアドレスを共有します。
  - 複数の接続が、インターフェイスグループ内のインターフェイスに分散されます。
  - 各接続またはセッションは、インターフェイスグループ内の1つのインターフェイスを使用します。シーケンシャルロードバランシング方式を使用すると、すべてのセッションがパケット単位で使用可能なリンクに分散され、インターフェイスグループの特定のインターフェイスにバインドされません。
- スタティックマルチモードインターフェイスグループは、最大で「n-1」個のインターフェイスの障害から回復できます。nは、インターフェイスグループを構成するインターフェイスの総数です。
- ポートに障害が発生した場合、またはポートが接続されていない場合、障害が発生したリンクを通過していたトラフィックは、残りのインターフェイスの1つに自動的に再配布されます。
- スタティックマルチモードインターフェイスグループではリンクの喪失は検出できますが、クライアントへの接続の喪失や、接続とパフォーマンスに影響する可能性のあるスイッチの設定ミスは検出できません。
- スタティックマルチモードインターフェイスグループには、複数のスイッチポートでのリンクアグリゲーションをサポートするスイッチが必要です。スイッチは、インターフェイスグループのリンクの接続先ポートがすべて1つの論理ポートを構成するように設定されています。一部のスイッチでは、ジャンボフレ

ーム用に構成されたポートのリンクアグリゲーションがサポートされない場合があります詳細については、スイッチベンダーのマニュアルを参照してください。

- スタティックマルチモードインターフェイスグループのインターフェイス間でトラフィックを分散するために、いくつかのロードバランシングオプションを使用できます。

次の図は、スタティックマルチモードインターフェイスグループの例です。インターフェイスe0a、e1a、e2a、およびe3aは、a1aマルチモードインターフェイスグループの一部です。a1aマルチモードインターフェイスグループの4つのインターフェイスはすべてアクティブです。



単一の集約リンク内のトラフィックを複数の物理スイッチに分散できるようにするテクノロジーがいくつか存在します。この機能を有効にするために使用されるテクノロジは、ネットワーク製品によって異なります。ONTAPのスタティックマルチモードインターフェイスグループは、IEEE 802.3規格に準拠しています。特定のマルチスイッチリンクアグリゲーションテクノロジがIEEE 802.3規格と相互運用または準拠していると言われている場合は、ONTAPと連携して動作する必要があります。

IEEE 802.3規格では、集約リンク内の送信デバイスが送信用の物理インターフェイスを決定すると規定されています。したがって、ONTAPは発信トラフィックの配信のみを担当し、着信フレームの着信方法を制御することはできません。集約リンク上の着信トラフィックの送信を管理または制御する場合は、直接接続されたネットワークデバイスでその送信を変更する必要があります。

ダイナミックマルチモードインターフェイスグループ

ダイナミックマルチモードインターフェイスグループは、Link Aggregation Control Protocol（LACP）を実装して、直接接続されたスイッチにグループメンバーシップを通信します。LACPを使用すると、リンクステータスの喪失および直接接続されたスイッチポートと通信できないノードを検出できます。

ONTAPに実装されているダイナミックマルチモードインターフェイスグループは、IEEE 802.3 AD（802.1AX）に準拠しています。ONTAPは、Cisco独自のリンクアグリゲーションプロトコルであるポートアグリゲーションプロトコル（PAgP）をサポートしていません。

ダイナミックマルチモードインターフェイスグループには、LACPをサポートするスイッチが必要です。

ONTAPは設定不可のアクティブモードでLACPを実装します。これは、アクティブモードまたはパッシブモードに設定されたスイッチと連動します。ONTAPは、IEEE 802.3 AD（802.1AX）で規定されているように、longおよびshortのLACPタイマーを実装します（3秒および90秒の設定不可の値で使用します）。

ONTAPロードバランシングアルゴリズムは、発信トラフィックの送信に使用されるメンバーポートを決定し

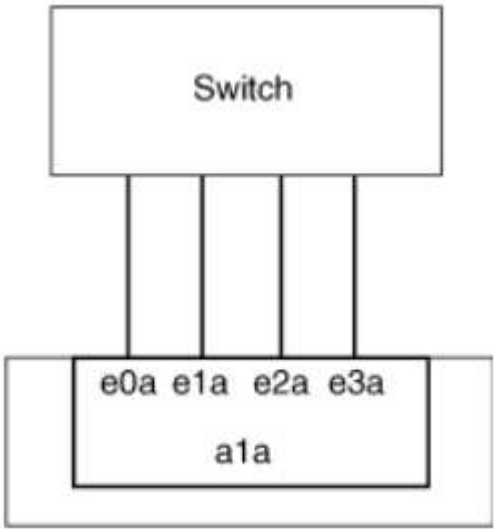
ますが、着信フレームの受信方法は制御しません。スイッチは、スイッチのポートチャネルグループに設定されたロードバランシングアルゴリズムに基づいて、送信に使用されるポートチャネルグループのメンバー（個々 の物理ポート）を決定します。したがって、スイッチの設定によって、トラフィックを受信するストレージシステムのメンバーポート（個 々 の物理ポート）が決まります。スイッチの設定の詳細については、スイッチベンダーのマニュアルを参照してください。

あるインターフェイスが連続するLACPプロトコルパケットの受信に失敗すると、そのインターフェイスは「ifgrp status」コマンドの出力で「lag_inactive」と表示されます。既存のトラフィックは、残りのアクティブインターフェイスに自動的に再ルーティングされます。

ダイナミックマルチモードインターフェイスグループを使用する場合は、次のルールが適用されます。

- ダイナミックマルチモードインターフェイスグループは、ポートベース、IPベース、MACベース、またはラウンドロビンによるロードバランシング方式を使用するように設定する必要があります。
- ダイナミックマルチモードインターフェイスグループでは、すべてのインターフェイスをアクティブにし、1つのMACアドレスを共有する必要があります。

次の図は、ダイナミックマルチモードインターフェイスグループの例です。インターフェイスe0a、e1a、e2a、およびe3aは、a1aマルチモードインターフェイスグループの一部です。a1aダイナミックマルチモードインターフェイスグループの4つのインターフェイスはすべてアクティブです。



マルチモードインターフェイスグループでのロードバランシング

IPアドレスベース、MACアドレスベース、シーケンシャルベース、またはポートベースのロードバランシング方式を使用してマルチモードインターフェイスグループのネットワークポート上でネットワークトラフィックを均等に分散することにより、マルチモードインターフェイスグループのすべてのインターフェイスが送信トラフィックに均等に使用されるようにすることができます。

マルチモードインターフェイスグループのロードバランシング方式は、インターフェイスグループの作成時にのみ指定できます。

- ベストプラクティス * ：可能なかぎりポートベースのロードバランシングを推奨します。ポートベースのロードバランシングは、ネットワークに特定の理由または制限がないかぎり使用してください。

ポートベースのロードバランシング

ポートベースのロードバランシングが推奨されます。

ポートベースのロードバランシング方式を使用すると、マルチモードインターフェイスグループのトラフィックをトランスポートレイヤ（TCP / UDP）ポートに基づいて均等に分散できます。

ポートベースのロードバランシング方式では、トランスポートレイヤのポート番号に加えて、ソースとデスティネーションのIPアドレスに対して高速ハッシュアルゴリズムを使用します。

IPアドレスおよび**MAC**アドレスによるロードバランシング

IPアドレスおよびMACアドレスによるロードバランシングは、マルチモードインターフェイスグループのトラフィックを均等に分散する方法です。

これらのロードバランシング方式では、送信元アドレスと宛先アドレス（IPアドレスとMACアドレス）に対して高速ハッシュアルゴリズムが使用されます。ハッシュアルゴリズムの結果がupリンクステートにないインターフェイスにマッピングされる場合、次のアクティブインターフェイスが使用されます。

ルータに直接接続するシステムでインターフェイスグループを作成する場合は、MACアドレスによるロードバランシング方式を選択しないでください。このような設定では、すべての発信IPフレームの宛先MACアドレスがルータのMACアドレスになります。そのため、インターフェイスグループの1つのインターフェイスだけが使用されます。

IPアドレスによるロードバランシングは、IPv4アドレスとIPv6アドレスの両方で同じように機能します。

シーケンシャルロードバランシング

シーケンシャルロードバランシングを使用すると、ラウンドロビンアルゴリズムを使用して、複数のリンク間でパケットを均等に分散できます。シーケンシャルオプションを使用すると、単一の接続のトラフィックを複数のリンクに分散して、単一の接続のスループットを向上させることができます。

ただし、シーケンシャルロードバランシングはパケット配信の順序が乱れてしまう可能性があるため、パフォーマンスが極端に低下する可能性があります。したがって、シーケンシャルロードバランシングは一般に推奨されません。

インターフェイスグループまたは**LAG**の作成

インターフェイスグループまたはLAG（シングルモード、スタティックマルチモード、またはダイナミックマルチモード（LACP））を作成すると、集約されたネットワークポートの機能を組み合わせて単一のインターフェイスとしてクライアントに提供できます。

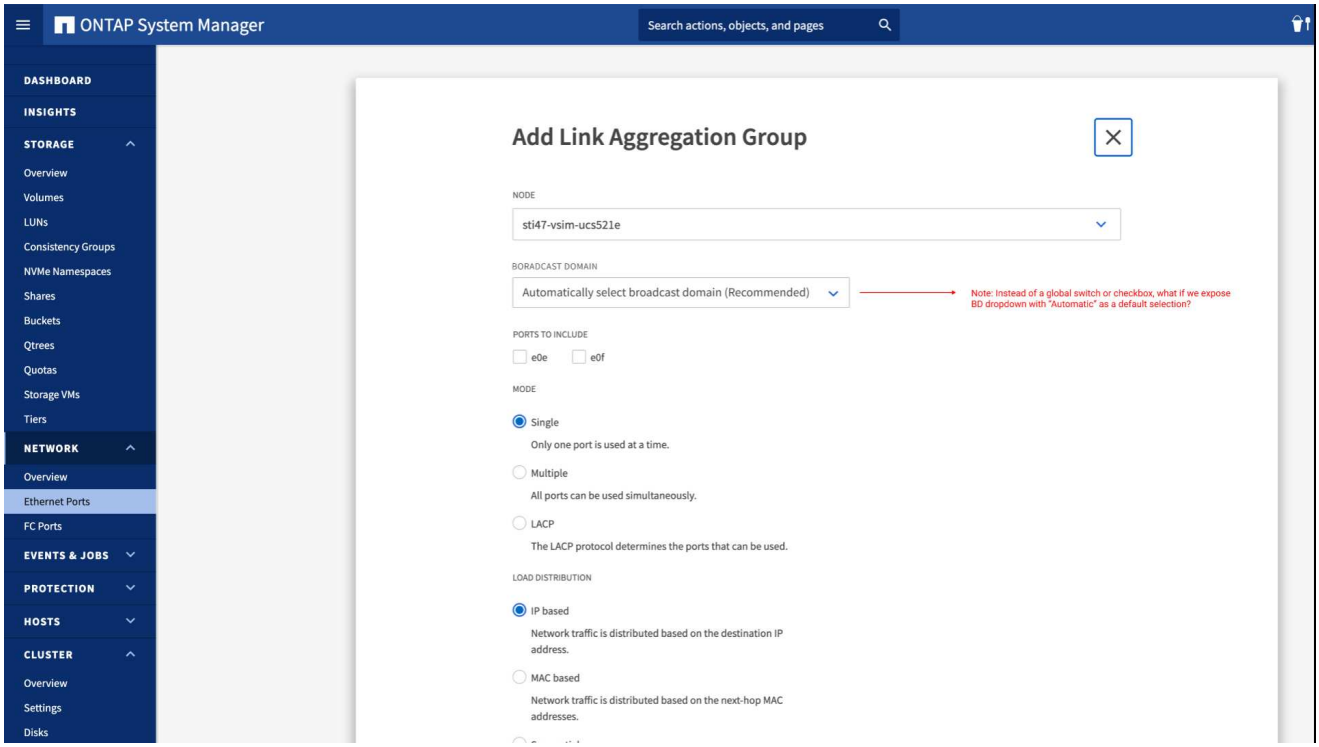
実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- System Managerを使用してLAGを作成します。*

手順

1. [*Network]>[Ethernet port]>[+ Link Aggregation Group]を選択して、LAGを作成します。
2. ドロップダウンリストからノードを選択します。
3. 次のいずれかを選択します。
   a. ONTAP to * automatically select broadcast domain（推奨）*。
   b. ブロードキャストドメインを手動で選択するには、をクリックします。
4. LAGを構成するポートを選択します。
5. モードを選択します。
   a. Single：一度に1つのポートのみが使用されます。
   b. 複数：すべてのポートを同時に使用できます。
   c. LACP：LACPプロトコルによって、使用できるポートが決まります。
6. ロードバランシングを選択します。
   a. IPベース
   b. MACベース
   c. ポート
   d. シーケンシャル
7. 変更を保存します。



CLI

- CLIを使用してインターフェイスグループを作成*

マルチモードインターフェイスグループを作成するときは、次のいずれかのロードバランシング方式を指定できます。

- `port`：ネットワークトラフィックは、トランスポートレイヤ（TCP / UDP）ポートに基づいて分散されます。これが推奨されるロードバランシング方式です。
- `mac`：ネットワークトラフィックはMACアドレスに基づいて分散されます。
- `ip`：ネットワークトラフィックはIPアドレスに基づいて分散されます。
- `sequential`：ネットワークトラフィックは受信したとおりに分散されます。

> インターフェイスグループのMACアドレスは、基盤となるポートの順序、およびこれらのポートがブート時にどのように初期化されるかによって決まります。そのため、ifgrpのMACアドレスがリブート後やONTAPのアップグレード後に変更されることはありません。

ステップ

コマンドを使用し `network port ifgrp create`て、インターフェイスグループを作成します。

インターフェイスグループの名前には、という構文を使用する必要があります `a<number><letter>`。たとえば、a0a、a0b、a1c、a2aは有効なインターフェイスグループ名です。

の詳細については `network port ifgrp create`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、分散機能をportに、モードをmultimodeに設定して、a0aという名前のインターフェイスグループを作成する方法を示しています。

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

インターフェイスグループまたは**LAG**へのポートの追加

すべてのポート速度のインターフェイスグループまたはLAGに最大16個の物理ポートを追加できます。

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

System Manager

- System Managerを使用して、LAGにポートを追加します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGに追加する同じノードの追加ポートを選択します。
3. 変更を保存します。

CLI

- CLIを使用して、インターフェイス・グループにポートを追加します。*

ステップ

インターフェイスグループにネットワークポートを追加します。

```
network port ifgrp add-port
```

次の例は、a0aという名前のインターフェイスグループにポートe0cを追加する方法を示しています。

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

ONTAP 9 8以降では、最初の物理ポートがインターフェイスグループに追加されてから約1分後に、適切なブロードキャストドメインにインターフェイスグループが自動的に配置されます。ONTAPでこの処理を行わず、ifgrpを手動でブロードキャストドメインに配置する場合は、パラメータをコマンドの一部として `ifgrp add-port`指定します `-skip-broadcast-domain-placement`。

のポートインターフェイスグループに関する詳細および設定の制限事項については、を参照して `network port ifgrp add-port`"ONTAPコマンド リファレンス"ください。

インターフェイスグループまたは**LAG**からポートを削除する

LIFをホストするインターフェイスグループからは、そのポートがインターフェイスグループ内の最後のポートでないかぎり、ポートを削除できます。最後のポートがインターフェイスグループから削除されないことを考慮して、インターフェイスグループがLIFをホストしていない、またはインターフェイスグループがLIFのホームポートでないという要件はありません。ただし、最後のポートを削除する場合は、先にインターフェイスグループからLIFを移行または移動する必要があります。

タスクの内容

インターフェイスグループまたはLAGから最大16個のポート（物理インターフェイス）を削除できます。

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

System Manager

- System Managerを使用して、LAGからポートを削除します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGから削除するポートを選択します。
3. 変更を保存します。

CLI

- CLIを使用して、インターフェイスグループからポートを削除します。*

ステップ

インターフェイスグループからネットワークポートを削除します。

```
network port ifgrp remove-port
```

の詳細については `network port ifgrp remove-port`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、a0aという名前のインターフェイスグループからポートe0cを削除する方法を示しています。

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

インターフェイスグループまたは**LAG**を削除する

基盤となる物理ポートに直接LIFを設定する場合や、インターフェイスグループやLAGのモードや分散機能を変更する場合は、インターフェイスグループやLAGを削除できます。

開始する前に

- LIFをホストしているインターフェイスグループまたはLAGは使用できません。
- インターフェイスグループまたはLAGをLIFのホームポートまたはフェイルオーバーターゲットにすることはできません。

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

System Manager

- LAGを削除するには、System Managerを使用します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを削除します。
2. 削除するLAGを選択します。
3. LAGを削除します。

CLI

- CLIを使用してインターフェイスグループ*を削除してください

ステップ

インターフェイスグループを削除するには、コマンドを使用し `network port ifgrp delete`ます。

の詳細については `network port ifgrp delete`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、a0bという名前のインターフェイスグループを削除する方法を示しています。

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

物理ポート経由の**ONTAP VLAN**の設定

ONTAPでVLANを使用すると、分離されたブロードキャストドメインを作成してネットワークを論理的にセグメント化できます。ブロードキャストドメインは、物理的な境界に定義された従来のブロードキャストドメインとは異なり、スイッチポート単位で定義されます。

VLANは複数の物理ネットワークセグメントにまたがることができます。VLANに属するエンドステーションは、機能またはアプリケーションによって関連付けられます。

たとえば、VLAN内のエンドステーションは、エンジニアリングや経理などの部門ごと、またはリリース1やリリース2などのプロジェクトごとにグループ化できます。VLANではエンドステーションが物理的に近接していることは重要ではないため、エンドステーションを地理的に分散させても、スイッチドネットワークにブロードキャストドメインを含めることができます。

ONTAP 9.14.1 および 9.13.1 では、論理インターフェイス (LIF) によって使用されず、接続されたスイッチ上でネイティブ VLAN 接続がないタグなしポートは、劣化としてマークされます。これは、使用されていないポートを特定しやすくするためのもので、停止を示すものではありません。ネイティブVLANでは、ONTAP CFMブロードキャストなどのタグなしトラフィックをifgrpベース ポートで許可します。タグなしトラフィックをブロックしないように、スイッチのネイティブVLANを設定します。

VLANの管理では、VLANに関する情報を作成、削除、または表示できます。

> スイッチのネイティブVLANと同じ識別子のVLANをネットワークインターフェイス上に作成しないでください。たとえば、ネットワークインターフェイスe0bがネイティブVLAN 10上にある場合、そのインターフェイスにVLAN e0b-10を作成しないでください。

VLANを作成します。

同じネットワークドメイン内の分離されたブロードキャストドメインを管理するためのVLANを作成するには、System Managerまたはコマンドを使用し `network port vlan create`ます。

開始する前に

次の要件を満たしていることを確認します。

- ネットワーク上に配置されたスイッチが、IEEE 802.1Q規格に準拠しているか、ベンダー固有のVLANを実装している。
- 複数のVLANをサポートする場合、エンド ステーションが1つ以上のVLANに属するように静的に設定されている。
- VLANは、クラスタLIFをホストしているポートに接続されていない。
- VLANは、「Cluster」IPspaceに割り当てられているポートに接続されていない。
- VLANは、メンバー ポートのないインターフェイス グループ ポートに作成されていない。

タスクの内容

VLANを作成すると、そのVLANがクラスタ内の指定したノードのネットワークポートに接続されます。

ポート上でVLANを初めて設定すると、ポートがダウンし、ネットワークが一時的に切断されることがあります。その後同じポートにVLANを追加しても、ポートの状態には影響しません。

> スイッチのネイティブVLANと同じ識別子のVLANをネットワークインターフェイス上に作成しないでください。たとえば、ネットワークインターフェイスe0bがネイティブVLAN 10上にある場合、そのインターフェイスにVLAN e0b-10を作成しないでください。

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

System Manager

- System Managerを使用してVLANを作成します。*

ONTAP 9 .12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で[オン]を選択することもできます。これまでは、ブロードキャストドメインはレイヤ2の接続に基づいて常に自動的に選択されていました。ブロードキャストドメインを手動で選択すると、ブロードキャストドメインを手動で選択すると接続が失われる可能性があることを示す警告が表示されます。

手順

1. Network > Ethernet port >+VLAN *を選択します。
2. ドロップダウンリストからノードを選択します。
3. 次のいずれかを選択します。
   a. ONTAP to * automatically select broadcast domain（推奨）*。
   b. をクリックして、リストからブロードキャストドメインを手動で選択します。
4. VLANを形成するポートを選択します。
5. VLAN IDを指定します。
6. 変更を保存します。

CLI

- CLIを使用してVLANを作成してください*

特定の状況において、ハードウェアの問題やソフトウェアの設定ミスを修正せずにデグレード状態のポートにVLANポートを作成する場合は、コマンドのパラメータ `network port modify`をに `true` 設定できます `-ignore-health-status`。

の詳細については `network port modify`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用し `network port vlan create`てVLANを作成します。
2. VLANを作成するときは、または `port`オプションと `vlan-id`オプションのいずれかを指定する必要があります `vlan-name`。VLAN名は、ポート（またはインターフェイスグループ）の名前とネットワークスイッチのVLAN IDをハイフンでつないだものです。たとえば `e0c-24`、と `e1c-80`は有効なVLAN名です。

次の例は、ノードの `cluster-1-01`ネットワークポートに接続された `e1c`VLANを作成する方法を示しています `e1c-80`。

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

vlan.8以降では、ONTAP 9が作成されてから約1分後に適切なブロードキャストドメインに自動的に配置されます。この処理をONTAPで行わず、VLANをブロードキャストドメインに手動で配置する場合は、コマンドでパラメータを `vlan create`指定します `-skip-broadcast-domain-placement`。

の詳細については `network port vlan create`、を"ONTAPコマンド リファレンス"参照してください。

VLANの編集

ブロードキャストドメインを変更したり、VLANを無効にしたりできます。

System Managerを使用してVLANを編集する

ONTAP 9 .12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で[オン]を選択することもできます。これまでのブロードキャストドメインは、レイヤ2の接続に基づいて常に自動的に選択されていました。ブロードキャストドメインを手動で選択すると、ブロードキャストドメインを手動で選択すると接続が失われる可能性があることを示す警告が表示されます。

手順

1. Network > Ethernet port > VLAN *を選択します。
2. 編集アイコンを選択します。
3. 次のいずれかを実行します。
   - 別のブロードキャスト ドメインをリストから選択して変更する。
   - [有効*]チェックボックスをオフにします。
4. 変更を保存します。

VLANの削除

NICをスロットから取り外す前に、VLANの削除が必要になることがあります。VLANを削除すると、そのVLANを使用しているすべてのフェイルオーバー ルールとフェイルオーバー グループから自動的に削除されます。

開始する前に

VLANに関連付けられているLIFがないことを確認します。

タスクの内容

ポートから最後のVLANを削除すると、そのポートからネットワークが一時的に切断される可能性があります。

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

System Manager

- VLANを削除するには、System Managerを使用します。*

手順

1. Network > Ethernet port > VLAN *を選択します。
2. 削除するVLANを選択します。
3. [削除（ Delete ）] をクリックします。

CLI

- CLIを使用してVLAN *を削除します

ステップ

コマンドを使用し `network port vlan delete`てVLANを削除します。

次の例は、ノードの `cluster-1-01`ネットワークポート `e1c`からVLANを削除する方法を示してい `e1c-80`ます。

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

の詳細については `network port vlan delete`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPのネットワークポート属性を変更します。

物理ネットワークポートの自動ネゴシエーション、二重モード、フロー制御、速度、および健全性の設定を変更することができます。

開始する前に

LIFをホストしているポートは変更できません。

タスクの内容

- 100GbE、40GbE、10GbE、または1GbEのネットワークインターフェイスの管理設定を変更することは推奨されません。

  二重モードおよびポート速度の設定値のことを管理設定と呼びます。ネットワークの制限によっては、管理設定が運用設定（ポートで実際に使用される二重モードと速度）と異なる場合があります。

- インターフェイスグループの基盤となる物理ポートの管理設定を変更することは推奨されません。

  パラメータ（advanced権限レベルで使用可能）は、 `-up-admin`ポートの管理設定を変更します。

- ノードのすべてのポート、またはノードで動作している最後のクラスタLIFをホストしているポートの管理設定をfalseに設定することは推奨されませ `-up-admin`ん。
- 管理ポートのMTUサイズを変更することは推奨されません `e0M`。
- ブロードキャストドメイン内のポートのMTUサイズは、ブロードキャストドメインに設定されているMTU

値から変更することはできません。

- VLANのMTUサイズは、ベースポートのMTUサイズの値を超えることはできません。

手順

1. ネットワークポートの属性を変更します。

   ```
   network port modify
   ```

2. フィールドをtrueに設定する `-ignore-health-status`と、指定したポートのネットワークポートのヘルスステータスを無視できるようになります。

   ネットワークポートのヘルスステータスは「デグレード」から「正常」に自動的に変更され、このポートを使用してLIFをホストできるようになります。クラスタポートのフロー制御はに設定する必要があります `none`。デフォルトでは、フロー制御はに設定されて `full`います。

次のコマンドは、フロー制御をnoneに設定して、ポートe0bのフロー制御を無効にします。

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

の詳細については `network port modify`、を"ONTAPコマンド リファレンス"参照してください。

40GbE NICポートを変換して、**ONTAP**ネットワーク用の**10GbE**ポートを作成する

X1144A-R6およびX91440A-R6の40GbEネットワークインターフェイスカード（NIC）を変換して、4つの10GbEポートをサポートすることができます。

どちらかの NIC をサポートするハードウェアプラットフォームを、 10GbE のクラスタインターコネクトと顧客データ接続をサポートするクラスタに接続する場合は、 NIC を変換して必要な 10GbE 接続を提供する必要があります。

開始する前に

サポートされているブレークアウトケーブルを使用する必要があります。

タスクの内容

NICをサポートするプラットフォームの一覧については、を参照してください "Hardware Universe"。

X1144A-R6 NIC では、 4 つの 10GbE 接続をサポートするために変換できるのはポート A だけです。ポート A が変換されると、ポート e は使用できなくなります。

手順

1. メンテナンスモードに切り替えます。
2. NIC を 40GbE のサポートから 10GbE のサポートに変換します。

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. convertコマンドの使用が完了したら、ノードを停止します。
4. ケーブルを取り付けるか、交換します。
5. ハードウェアモデルに応じて、SP（サービスプロセッサ）またはBMC（ベースボード管理コントローラ）を使用してノードの電源を再投入し、変換を有効にします。

ONTAPネットワーク用の**UTA X1143A-R6**ポートの設定

X1143A-R6ユニファイドターゲットアダプタのポートは、デフォルトではFCターゲットモードで構成されますが、10Gbイーサネットポートおよびfcoeポート（CNAポート）または16Gb FCイニシエータポートまたはターゲットポートとして構成することができます。これには、 SFP+ アダプタが必要です。

イーサネットおよびFCoE用に設定した場合、X1143A-R6アダプタは、同じ10-GBEポート上でNICおよびFCoEターゲットトラフィックを同時にサポートします。FC用に設定した場合、同じASICを共有する2ポートの各ペアをFCターゲットモードまたはFCイニシエータモード用に個別に設定できます。つまり、1つのX1143A-R6アダプタで、1つの2ポートペアでFCターゲットモードをサポートし、もう1つの2ポートペアでFCイニシエータモードをサポートできます。同じASICに接続されたポートペアは、同じモードで設定する必要があります。

X1143A-R6アダプタは、FCモードでは既存のFCデバイスと同様に動作し、最大速度は16Gbpsです。X1143A-R6アダプタをCNAモードで使用すると、同じ10GbEポートを共有するNICおよびFCoEのトラフィックを同時に処理できます。CNAモードでは、FCoE機能でFCターゲットモードのみがサポートされます。

ユニファイドターゲットアダプタ（ X1143A-R6 ）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

手順

1. ポート設定を表示します。

```
system hardware unified-connect show
```

2. 必要に応じて、Fibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定します。

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. FC または 10Gb イーサネットに適したケーブルを接続します。
4. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、接続先の FC ファブリックに応じて 8Gb SFP または 16Gb SFP を使用します。

UTA2ポートをONTAPネットワークで使用できるように変換する

UTA2ポートは、Converged Network Adapter（CNA；統合ネットワークアダプタ）モードからFibre Channel（FC；ファイバチャネル）モードに、またはその逆に変換できます。

ポートをネットワークに接続する物理メディアを変更する必要がある場合、またはFCイニシエータとターゲットをサポートする場合は、UTA2パーソナリティをCNAモードからFCモードに変更する必要があります。

CNAモトカラ**FC**モトへ

手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. ポートのモードを変更します。

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. ノードをリブートし、アダプタをオンラインにします。

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。
   - ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ ifgrp ）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。
     - LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。
     - コマンドを実行して、ポートを手動で削除し `network port delete`ます。コマンドが失敗した場合は `network port delete`、エラーに対処してからもう一度コマンドを実行する必要があります。
   - ポートが LIF のホームポートとして使用されていない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。VIFマネージャでポートが削除されない場合は、管理者がリブート後にコマンドを使用して手動で削除する必要があります `network port delete`。

     の詳細については `network port delete`、を"ONTAPコマンド リファレンス"参照してください。

5. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、ノードで構成を変更する前に、 8Gb SFP または 16Gb SFP を使用します。

FCモオトカラ**CNA**モオトへ

手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. ポートのモードを変更します。

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. ノードをリブートする
4. 正しいSFP+が取り付けられていることを確認します。

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。

ONTAPネットワーク用の**CNA / UTA2**光モジュールの変換

ユニファイドターゲットアダプタ（CNA / UTA2）用に選択したパーソナリティモードをサポートするように、ユニファイドターゲットアダプタ（CNA / UTA2）の光モジュールを変更する必要があります。

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
2. X1143A-R6アダプタから現在の光モジュールを取り外します。
3. 使用するパーソナリティモード（FCまたはCNA）光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

サポートされるSFP+モジュールおよびCiscoブランドの銅線（Twinax）ケーブルについては、を参照し"NetApp Hardware Universe"てください。

ONTAPクラスタノードからの**NIC**の削除

障害のあるNICをスロットから取り外したり、メンテナンスのためにNICを別のスロットに移動したりしなければならない場合があります。

ONTAP 9.7以前のバージョンでは、NICの取り外し手順が異なります。ONTAP 9.7以前を実行しているONTAPクラスタノードからNICを取り外す必要がある場合は、の手順を参照して"ノードからのNICの取り外し（ONTAP 9.7以前）"ください。

手順

1. ノードの電源をオフにします。
2. NICをスロットから物理的に取り外します。
3. ノードの電源を投入します。
4. ポートが削除されたことを確認します。

```
network port show
```

ONTAPはすべてのインターフェイスグループからポートを自動的に削除します。ポートがインターフェイスグループの唯一のメンバーであった場合、そのインターフェイスグループは削除されます。の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

5. ポートにVLANが設定されていた場合は、VLANが孤立状態になります。孤立状態のVLANは、次のコマンドを使用して確認できます。

```
cluster controller-replacement network displaced-vlans show
```

`displaced-interface show`、 `displaced-vlans show`、および `displaced-vlans restore`の各コマンドは一意であり、で始まる完全修飾コマンド名は必要ありません `cluster controller-replacement network`。

6. これらのVLANは削除されますが、次のコマンドを使用してリストアできます。

```
displaced-vlans restore
```

7. ポートにLIFが設定されている場合は、同じブロードキャストドメイン内の別のポートの新しいホームポートがONTAPによって自動的に選択されます。同じFilerに適切なホーム・ポートが見つからない場合、それらのLIFは削除されたとみなされます。削除されたLIFは、次のコマンドを使用して確認できます。

```
displaced-interface show
```

8. 同じノードのブロードキャストドメインに新しいポートを追加すると、LIFのホームポートは自動的にリストアされます。または、コマンドを使用してホームポートを設定することもできます `network interface modify -home-port -home-node or use the displaced- interface restore`。

関連情報

- "クラスタコントローラ-交換用ネットワークが取り外されました-インターフェイスが削除されました"
- "network interface modify"

ONTAPネットワークポートの健全性を監視する

ネットワークポートの ONTAP 管理では、健常性の自動監視機能と一連のヘルスモニタを使用して、 LIF のホストに適さない可能性のあるネットワークポートを特定できます。

タスクの内容

ヘルスモニタで健全でないと判断されたネットワークポートは、 EMS メッセージで管理者に警告が送信されるか、またはデグレードとマークされます。ONTAPは、デグレード状態のネットワークポートで別の正常なフェイルオーバーターゲットがある場合、そのLIFでのLIFのホストを回避します。ポートは、リンクフラッピング（リンクがアップとダウンを高速で繰り返す状態）やネットワークパーティショニングなどの軽度な障害イベントが原因でデグレード状態になります。

- クラスタIPspace内のネットワークポートは、リンクフラッピングが発生した場合、またはブロードキャストドメイン内の他のネットワークポートへのレイヤ2（L2）の到達可能性が失われた場合にデグレードとマークされます。
- クラスタ以外の IPspace 内のネットワークポートは、リンクフラッピングが発生した場合にデグレードとマークされます。

デグレード状態のポートの以下の動作に注意してください。

- デグレード状態のポートを VLAN またはインターフェイスグループに含めることはできません。

  インターフェイスグループのメンバーポートがデグレードとマークされていて、インターフェイスグループが正常とマークされている場合は、そのインターフェイスグループで LIF をホストできます。

- LIFは、デグレード状態のポートから正常な状態のポートに自動的に移行されます。
- フェイルオーバー時には、デグレード状態のポートはフェイルオーバーターゲットとみなされません。正常なポートがない場合は、通常のフェイルオーバーポリシーに従ってデグレード状態のポートがLIFをホストします。
- デグレード状態のポートに LIF を作成、移行、リバートすることはできません。

  ネットワークポートの設定はに `true`変更できます `ignore-health-status`。その後、正常なポートでLIFをホストできます。

手順

1. advanced権限モードにログインします。

```
set -privilege advanced
```

2. ネットワークポートの健全性の監視で有効になっているヘルスモニタを確認します。

```
network options port-health-monitor show
```

ポートのヘルスステータスは、ヘルスモニタの値によって決まります。

ONTAP でデフォルトで有効になっていて使用可能なヘルスモニタは次のとおりです。

- リンクフラッピングヘルスモニタ：リンクフラッピングを監視します

  5 分以内に複数回のリンクフラッピングが発生しているポートは、デグレードとマークされます。

- L2 到達可能性ヘルスモニタ：同じブロードキャストドメインに設定されたすべてのポートで相互のポートに対するレイヤ 2 到達可能性が確保されているかどうかを監視します

  このヘルスモニタは、すべての IPspace におけるレイヤ 2 到達可能性の問題を報告しますが、デグレードとマークされるのはクラスタ IPspace 内のポートのみです。

- CRC モニタ：ポートの CRC 統計を監視します

  このヘルスモニタはポートをデグレードとマークしませんが、CRCエラー率が非常に高い場合にEMSメッセージを生成します。

の詳細については `network options port-health-monitor show`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドを使用して、IPspaceのヘルスモニタを必要に応じて有効または無効にします `network options port-health-monitor modify`。

   の詳細については `network options port-health-monitor modify`、を"ONTAPコマンド リファレンス"参照してください。

4. ポートの詳細な健全性を表示します。

```
network port show -health
```

コマンド出力には、ポートのヘルスステータス、設定、およびポートがデグレードとマークされた理由のリストが表示され `ignore health status`ます。

ポートのヘルスステータスは `healthy`、または `degraded`です。

設定がの `true`場合 `ignore health status`は、ポートのヘルスステータスが管理者によってからに `healthy`変更されたことを示します `degraded`。

設定がの `false`場合、 `ignore health status`ポートのヘルスステータスはシステムによって自動的に判断されます。

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークポートの到達可能性の監視

到達可能性の監視は、ONTAP 9 .8以降に組み込まれています。この監視機能を使用して、物理ネットワークトポロジがONTAPの設定と一致しない場合を特定します。場合によっては、ONTAPによってポートの到達可能性が修復されることがあります。それ以外の場合は、追加の手順が必要です。

タスクの内容

これらのコマンドを使用して、ONTAPの設定が物理的なケーブル配線またはネットワークスイッチの設定と一致しないことに起因するネットワークの設定ミスを検証、診断、および修復します。

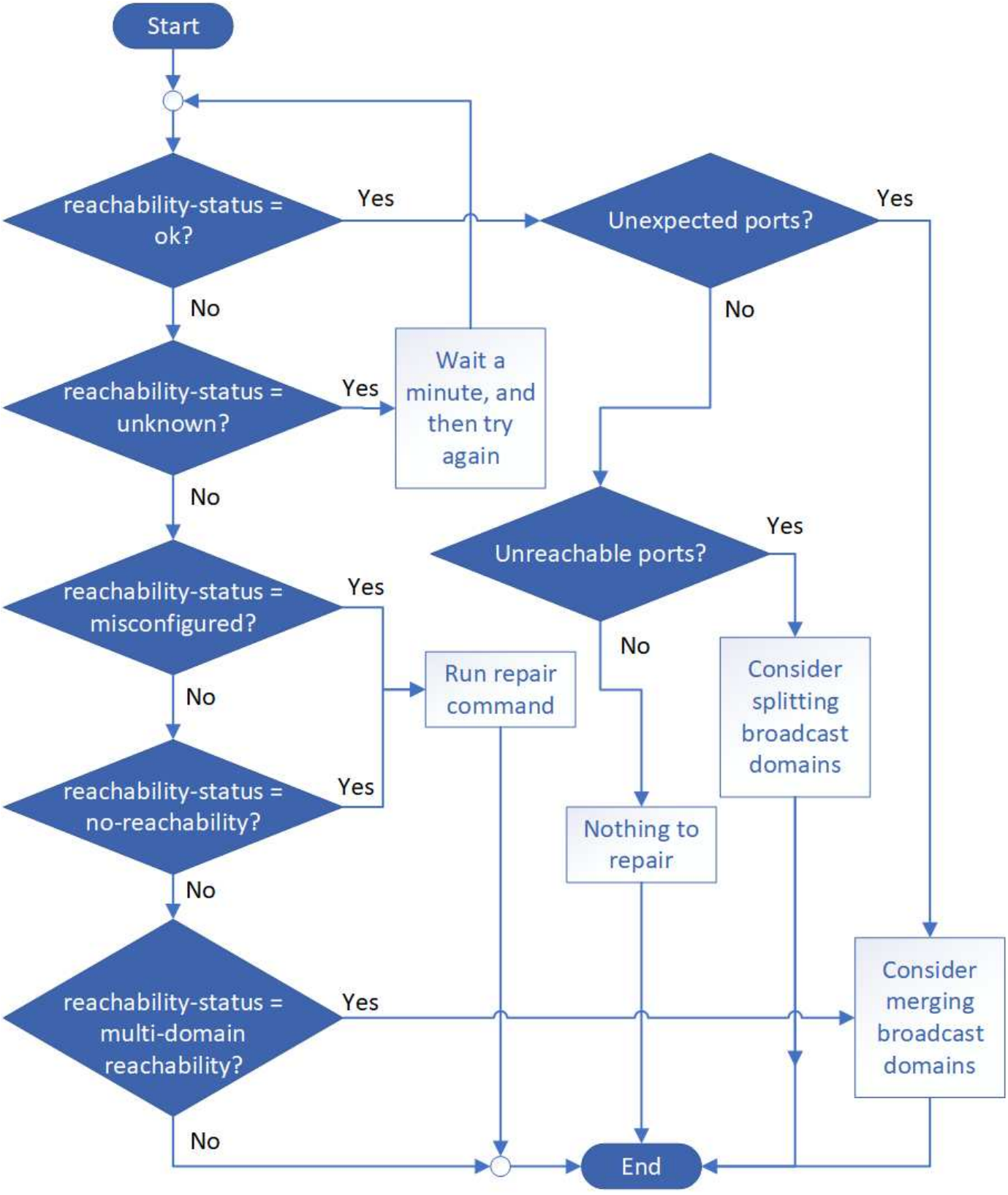
ステップ

1. ポートの到達可能性を表示します。

   ```
   network port reachability show
   ```

   の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。

2. 次のDecision Treeと表を使用して、次の手順を決定します（該当する場合）。



プレゼンスステータス	説明

OK	ポートに割り当てられているブロードキャストドメインにレイヤ 2 の到達可能性があります。到達可能性ステータスが「ok」で、「予期しないポート」がある場合は、1つ以上のブロードキャストドメインをマージすることを検討してください。詳細については、次の _unexpected ports_row を参照してください。 到達可能性ステータスが「ok」で、到達不能なポートがある場合は、1つ以上のブロードキャストドメインをスプリットすることを検討してください。詳細については、次の _Unreachable Ports_row を参照してください。 到達可能性ステータスが「ok」で、予期しないポートや到達不能なポートがない場合、設定は正しいです。
予期しないポートです	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、ポートに割り当てられているブロードキャストドメインを1つ以上のブロードキャストドメインにマージする必要がないかどうかを確認します。 詳細については、を参照してください "ブロードキャストドメインのマージ"。
到達不能ポート	1 つのブロードキャストドメインが 2 つの異なる到達可能性セットにパーティショニングされている場合は、ブロードキャストドメインをスプリットして ONTAP 構成を物理ネットワークトポロジと同期できます。 通常、到達不能なポートのリストには、物理的な設定とスイッチの設定に間違いがないことを確認したあとに、これらのポートを別のブロードキャストドメインに分割する必要があります。 詳細については、を参照してください "ブロードキャストドメインのスプリット"。
誤設定 - 到達可能性	ポートに割り当てられているブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、到達可能なブロードキャストドメインにポートが割り当てられます。 `network port reachability repair -node -port`詳細については、を参照してください"ポートの到達可能性を修復"。

到達不能	既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、自動的にデフォルトIPspace内に作成された新しいブロードキャストドメインにポートが割り当てられます。 `network port reachability repair -node -port`詳細については、を参照してください"ポートの到達可能性を修復"。の詳細については `network port reachability repair`、を"ONTAPコマンド リファレンス"参照してください。
multi-domain-reachable	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、ポートに割り当てられているブロードキャストドメインを1つ以上のブロードキャストドメインにマージする必要がないかどうかを確認します。 詳細については、またはを参照してください"ブロードキャストドメインのマージ""ポートの到達可能性を修復"。
不明	reachable-status が「 unknown 」の場合は、数分待ってからもう一度コマンドを実行してください。

ポートを修理したら、削除されたLIFとVLANを確認して解決する必要があります。ポートがインターフェイスグループに属していた場合は、そのインターフェイスグループの状況についても理解しておく必要があります。詳細については、を参照してください "ポートの到達可能性を修復"。

ONTAPネットワークでのポートの使用状況を確認する

いくつかのwell-knownポートは、特定のサービスとのONTAP通信用に予約されています。ストレージネットワーク環境のポートの値がONTAPポートの値と同じ場合、ポートの競合が発生します。

インバウンドトラフィック

ONTAPストレージのインバウンドトラフィックは、次のプロトコルとポートを使用します。

プロトコル	ポート	目的
すべての ICMP	すべて	インスタンスの ping を実行します
TCP	22	クラスタ管理LIFまたはノード管理LIFのIPアドレスへのSecure Shellアクセス
TCP	80	クラスタ管理LIFのIPアドレスへのWebページアクセス
TCP / UDP	111	rpcbind、NFSのリモートプロシージャコールrpcbind NFSノリモートプロシージャコール
UDP	123	NTP、ネットワークタイムプロトコル

TCP	135	MSRPC、Microsoftリモートプロシージャコール
TCP	139	NetBIOS-SSN、CIFSテノNetBIOSサアヒスセツシヨン
TCP / UDP	161-162	SNMP、簡易ネットワーク管理プロトコル
TCP	443	クラスタ管理LIFのIPアドレスへのセキュアなWebページアクセス
TCP	445	MS Active Domain Services、NetBIOSフレーミングを使用したMicrosoft SMB/CIFS over TCP
TCP / UDP	635	リモート・ファイル・システムとローカルであるかのように通信するためのNFSマウント
TCP	749	Kerberos
UDP	953	名前デーモン
TCP / UDP	2049	NFSサーバデーモン
TCP	2050	NRV、NetAppリモートボリュームプロトコル
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP / UDP	4045	NFSロックデーモン
TCP / UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS RPC rquotad
UDP	4444	KRB524、Kerberos 524
UDP	5353	マルチキャストDNS
TCP	10000	Network Data Management Protocol（NDMP；ネットワークデータ管理プロトコル）を使用したバックアップ
TCP	11104	クラスタピアリング、SnapMirrorのクラスタ間通信セッションの双方向管理
TCP	11105	クラスタピアリング、クラスタ間LIFを使用した双方向のSnapMirrorデータ転送
SSL/TLS	30000	セキュア ソケット (SSL/TLS) を介して DMA と NDMP サーバー間の NDMP セキュア制御接続を受け入れます。セキュリティ スキャナーはポート 30000 の脆弱性を報告する場合があります。

アウトバウンドトラフィック

ONTAPストレージのアウトバウンドトラフィックは、ビジネスニーズに応じて基本ルールまたは高度なルールを使用して設定できます。

基本的なアウトバウンドルール

すべてのポートは、ICMP、TCP、およびUDPプロトコルを介したすべての発信トラフィックに使用できます。

プロトコル	ポート	目的
すべての ICMP	すべて	すべての発信トラフィック
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、ONTAPによる発信通信に必要なポートのみを開くことができます。

Active Directory

プロトコル	ポート	ソース	デスティネーション	目的
TCP	88	ノード管理LIF、データLIF（NFS、CIFS、iSCSI）	Active Directory フォレスト	Kerberos V 認証
UDP	137	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	NetBIOSネームサービス
UDP	138	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	NetBIOS データグラムサービス
TCP	139	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	NetBIOSサービスセッション
TCP	389	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	LDAP
UDP	389	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	LDAP
TCP	445	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
TCP	464	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	Kerberos vパスワードの変更と設定（set_change）
UDP	464	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	Kerberos キー管理
TCP	749	ノード管理LIF、データLIF（NFS、CIFS）	Active Directory フォレスト	Kerberos Vパスワードの変更と設定（RPCSEC_GSS）

AutoSupport

プロトコル	ポート	ソース	デスティネーション	目的

TCP	80	ノード管理LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）

SNMP

プロトコル	ポート	ソース	デスティネーション	目的
TCP / UDP	162	ノード管理LIF	サーバを監視します	SNMP トラップによる監視

SnapMirror

プロトコル	ポート	ソース	デスティネーション	目的
TCP	11104	クラスタ間LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理

その他のサービス

プロトコル	ポート	ソース	デスティネーション	目的
TCP	25	ノード管理LIF	メールサーバ	SMTP アラート。AutoSupport に使用できます
UDP	53	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
UDP	67	ノード管理LIF	DHCP	DHCPサーバ
UDP	68	ノード管理LIF	DHCP	初回セットアップ用の DHCP クライアント
UDP	514	ノード管理LIF	syslogサアハ	syslog 転送メッセージ
TCP	5010	クラスタ間LIF	バックアップエンドポイントまたはリストアエンドポイント	S3 へのバックアップ処理とリストア処理 フィーチャー（ Feature ）
TCP	18600 ～18699	ノード管理LIF	宛先サーバ	NDMP コピー

ONTAP内部ポートの詳細

次の表は、ONTAPが内部で使用するポートとその機能を示しています。ONTAPはこれらのポートを、クラスタ内LIF通信の確立など、さまざまな機能に使用します。

このリストは網羅的なものではなく、環境によって異なる場合があります。

ポート / プロトコル	コンポーネント/機能

514	syslog
900	NetAppクラスタRPC
902	NetAppクラスタRPC
904	NetAppクラスタRPC
905	NetAppクラスタRPC
910	NetAppクラスタRPC
911	NetAppクラスタRPC
913	NetAppクラスタRPC
914	NetAppクラスタRPC
915	NetAppクラスタRPC
918	NetAppクラスタRPC
920	NetAppクラスタRPC
921	NetAppクラスタRPC
924	NetAppクラスタRPC
925	NetAppクラスタRPC
927	NetAppクラスタRPC
928	NetAppクラスタRPC
929	NetAppクラスタRPC
930	カーネル サービスおよび管理機能 (KSMF)
931	NetAppクラスタRPC
932	NetAppクラスタRPC
933	NetAppクラスタRPC
934	NetAppクラスタRPC
935	NetAppクラスタRPC
936	NetAppクラスタRPC
937	NetAppクラスタRPC
939	NetAppクラスタRPC
940	NetAppクラスタRPC
951	NetAppクラスタRPC
954	NetAppクラスタRPC
955	NetAppクラスタRPC
956	NetAppクラスタRPC
958	NetAppクラスタRPC
961	NetAppクラスタRPC

963	NetAppクラスタRPC
964	NetAppクラスタRPC
966	NetAppクラスタRPC
967	NetAppクラスタRPC
975	Key Management Interoperability Protocol（KMIP）
982	NetAppクラスタRPC
983	NetAppクラスタRPC
5125	ディスクの代替制御ポート
5133	ディスクの代替制御ポート
5144	ディスクの代替制御ポート
65502	ノードスコープSSH
65503	LIF共有
7700	クラスターセッションマネージャー (CSM)
7810	NetAppクラスタRPC
7811	NetAppクラスタRPC
7812	NetAppクラスタRPC
7813	NetAppクラスタRPC
7814	NetAppクラスタRPC
7815	NetAppクラスタRPC
7816	NetAppクラスタRPC
7817	NetAppクラスタRPC
7818	NetAppクラスタRPC
7819	NetAppクラスタRPC
7820	NetAppクラスタRPC
7821	NetAppクラスタRPC
7822	NetAppクラスタRPC
7823	NetAppクラスタRPC
7824	NetAppクラスタRPC
7835-7839と7845-7849	クラスタ内通信用のTCPポート
8023	ノードスコープTelnet
8443	Amazon FSx 用の ONTAP S3 NAS ポート
8514	ノードスコープRSH
9877	KMIPクライアントポート（内部ローカルホストのみ）
10006	HA相互接続通信用のTCPポート

IPspace

ONTAP IPspace設定の詳細

IPspaceを使用すると、単一のONTAPクラスタを設定し、複数の管理上分離されたネットワーク ドメインのクライアントが、たとえ同じIPアドレス範囲を使用している場合でもアクセスできるようにすることができます。これにより、クライアント トラフィックを分離してプライバシーとセキュリティを確保することができます。

IPspaceは、Storage Virtual Machine（SVM）が実装される、個別のIPアドレス スペースを定義します。あるIPspaceに対して定義されたポートとIPアドレスは、そのIPspace内でのみ有効です。IPspace内のSVMごとに個別のルーティング テーブルが保持されるため、SVMやIPspaceをまたがってトラフィックがルーティングされることはありません。

IPspaceのルーティング ドメインでは、IPv4およびIPv6のアドレスがサポートされます。

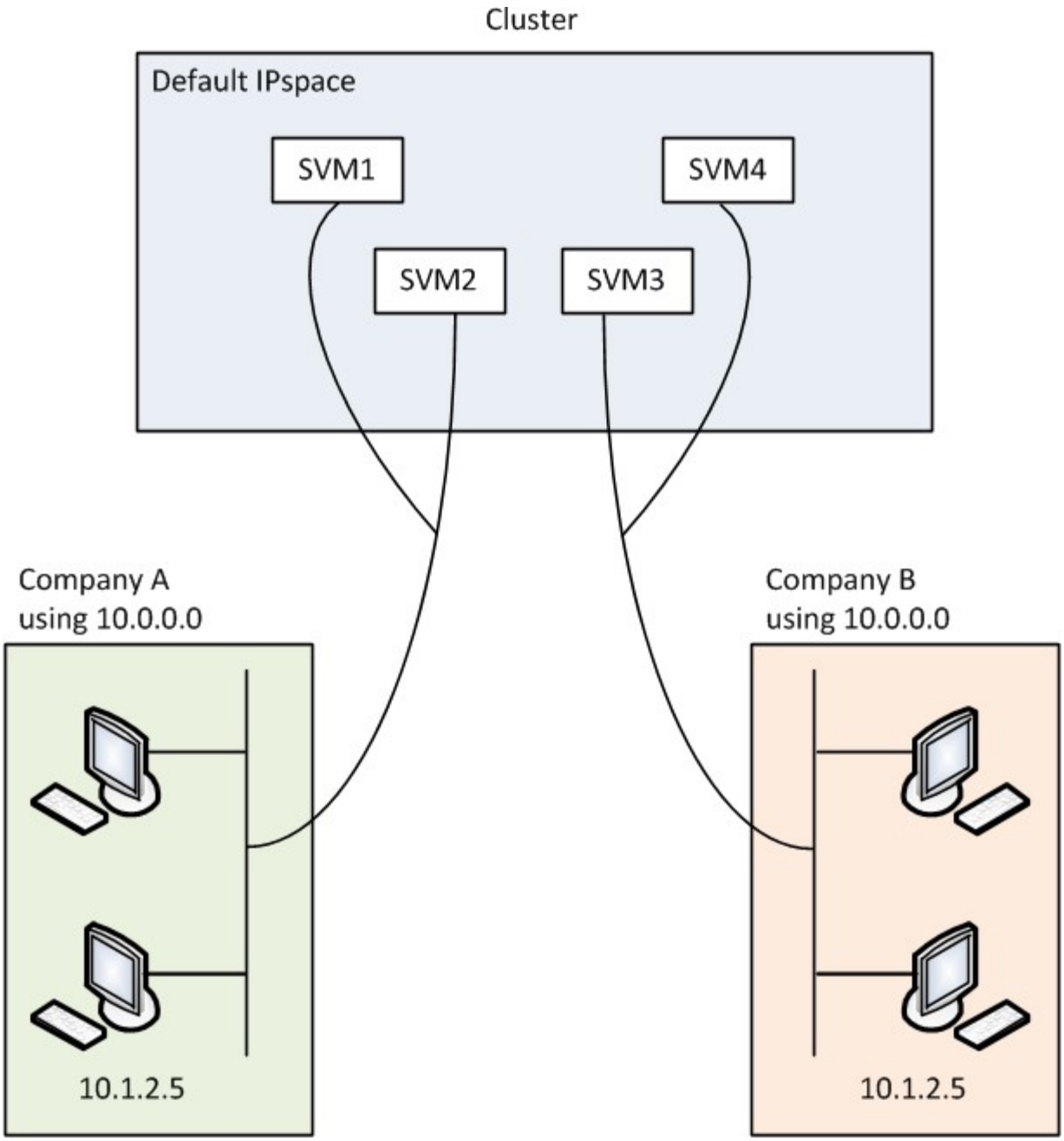
単一の組織のストレージを管理する場合は、IPspaceを設定する必要はありません。単一のONTAPクラスタで複数企業のストレージを管理していて、ユーザ間のネットワーク設定がないことが確実な場合も、IPspaceを使用する必要はありません。多くの場合、Storage Virtual Machine （SVM）を専用のIPルーティング テーブルと一緒に使用することで、IPspaceを使用しなくても固有のネットワーク設定を分離できます。

IPspaceの使用例

ここでは、IPspaceの一般的な用途として、ストレージ サービス プロバイダ（SSP）が、その顧客のA社とB社をSSPのONTAPクラスタに接続する必要があり、両方の会社が同じプライベートIPアドレスの範囲を使用する場合を取り上げます。

SSPは、クラスタに顧客用のSVMを作成し、2つのSVMからA社のネットワークへの専用ネットワーク パス、別の2つのSVMからB社のネットワークへの専用ネットワーク パスを提供します。

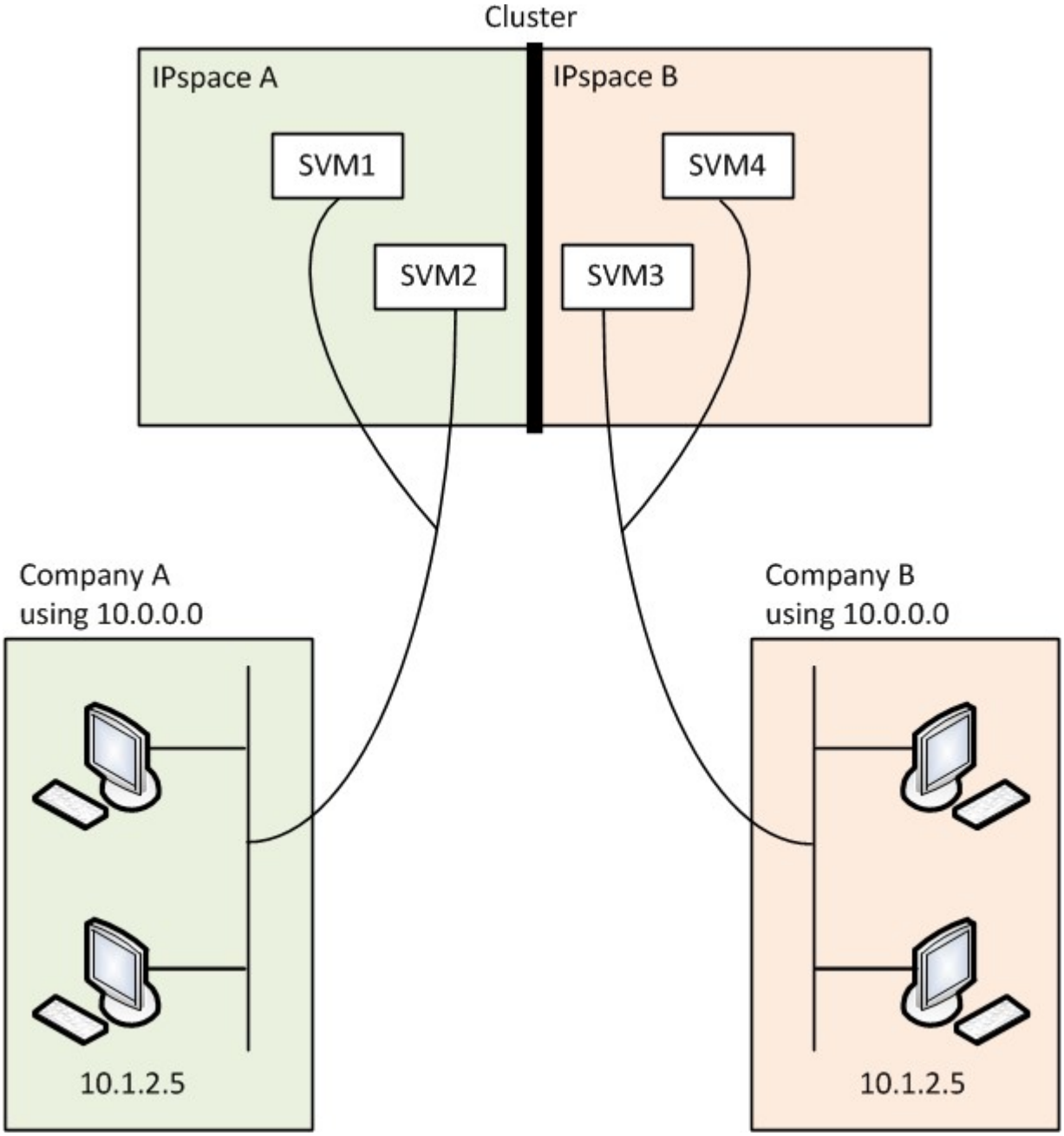
次の図に、この導入形態を示します。これは、両社で非プライベートIPアドレスの範囲を使用する場合に機能します。しかし、図に示すように両社が同じプライベートIPアドレスの範囲を使用すると問題が発生します。



両社がプライベートIPアドレスサブネット10.0.0.0を使用しているため、次の問題が発生します。

- 両社がそれぞれのSVMに同じIPアドレスを使用する場合、SSPにあるクラスタ内のSVMでIPアドレスの競合が発生します。
- 両社がそれぞれのSVMに異なるIPアドレスを使用することに合意した場合でも、問題が生じる可能性があります。
- たとえば、Aのネットワーク内のいずれかのクライアントがBのネットワーク内のクライアントと同じIPアドレスを持っている場合、Aのアドレス空間内のクライアント宛てのパケットはBのアドレス空間内のクライアントにルーティングされ、その逆も同様です。
- 両社が相互に排他的なアドレススペースを使用する場合（たとえば、Aが10.0.0.0、ネットワークマスクが255.128.0.0、Bが10.128.0.0、ネットワークマスクが255.128.0.0など）、SSPはクラスタに静的ルートを設定して、トラフィックをAとBのネットワークに適切にルーティングする必要があります。
- このソリューションは、拡張性（静的ルートが原因）もセキュア（ブロードキャストトラフィックがクラ

スタのすべてのインターフェイスに送信される）もありません。これらの問題を解決するために、SSPはクラスタに2つのIPspace（会社ごとに1つずつ）を定義します。トラフィックがIPspaceをまたがってルーティングされることはないため、すべてのSVMが10.0.0.0というアドレススペースに設定されていても、次の図に示すように、それぞれの会社のデータがそれぞれのネットワークにセキュアにルーティングされます。



また、さまざまな構成ファイル（ファイル、ファイル、 `/etc/hosts.equiv` `the /etc/rc`ファイルなど）で参照されるIPアドレス `/etc/ hosts`は、そのIPspaceに対して相対的です。そのため、IPspaceを使用すると、SSPが複数のSVMの設定と認証データに同じIPアドレスを設定しても競合することはありません。

IPspaceの標準プロパティ

クラスタの最初の作成時に特別なIPspaceがデフォルトで作成されます。さらに、IPspaceごとに特別なStorage Virtual Machine（SVM）が作成されます。

クラスタの初期化時に2つのIPspaceが自動的に作成されます。

- 「デフォルト」のIPspace

  このIPspaceは、ポート、サブネット、およびデータ提供用SVMのコンテナです。クライアントごとに個別のIPspaceを作成する必要がない設定の場合は、すべてのSVMをこのIPspaceに作成できます。このIPspaceには、クラスタ管理ポートとノード管理ポートも含まれています。

- 「クラスタ」IPspace

  このIPspaceには、クラスタ内のすべてのノードのすべてのクラスタポートが含まれます。クラスタの作成時に自動的に作成されます。このIPspaceは、内部のプライベート クラスタ ネットワークへの接続を提供します。ノードをクラスタに追加すると、追加したノードのクラスタ ポートが「Cluster」IPspaceに追加されます。

IPspaceごとに「システム」SVMが1つ存在します。IPspaceを作成すると、デフォルトのシステムSVMがIPspaceと同じ名前で作成されます。

- 「Cluster」IPspaceのシステムSVMは、内部プライベート クラスタ ネットワークのノード間でクラスタ トラフィックを伝送します。

  このSVMの管理はクラスタ管理者が担当し、「Cluster」という名前が割り当てられます。

- 「Default」IPspaceのシステムSVMは、クラスタ間トラフィックを含めた、クラスタとノードの管理トラフィックを伝送します。

  このSVMの管理はクラスタ管理者が担当し、クラスタと同じ名前が使用されます。

- ユーザが作成するカスタムIPspaceのシステムSVMは、そのSVMの管理トラフィックを伝送します。

  このSVMの管理はクラスタ管理者が担当し、IPspaceと同じ名前が使用されます。

1つのIPspaceにクライアント用のSVMを1つ以上配置できます。各クライアントSVMは専用のデータ ボリュームと設定を持ち、他のSVMからは独立して管理されます。

ONTAPネットワーク用のIPspaceの作成

IPspaceは、Storage Virtual Machine（SVM）が配置される個別のIPアドレススペースです。SVMにセキュアなストレージ、管理、およびルーティングが必要な場合は、IPspaceを作成できます。IPspaceを使用すると、クラスタ内のSVMごとに個別のIPアドレススペースを作成できます。これにより、管理上分離されたネットワークドメインに属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

タスクの内容

IPspaceの数はクラスタ全体で512個に制限されています。6GBのRAMを搭載したノードを含むクラスタのIPspaceは、クラスタ全体で256個までに制限されます。ご使用のプラットフォームに適用されるその他の制限については、Hardware Universeを参照してください。

"NetApp Hardware Universe"

「all」はシステムで予約されている名前であるため、IPspace名を「all」にすることはできません。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. IPspaceを作成します。

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

`ipspace_name`は、作成するIPspaceの名前です。次のコマンドは、クラスタにipspace1というIPspaceを作成します。

```
network ipspace create -ipspace ipspace1
```

の詳細については `network ipspace create`、を"ONTAPコマンド リファレンス"参照してください。

2. IPspaceを表示します。

```
network ipspace show
```

```
IPspace              Vserver List          Broadcast Domains
-------------------- --------------------- ------------------------------
Cluster              Cluster               Cluster
Default              Cluster1              Default
ipspace1             ipspace1              -
```

IPspaceが、そのIPspaceのシステムSVMとともに作成されます。システムSVMは管理トラフィックを伝送します。

終了後

MetroCluster構成のクラスタにIPspaceを作成する場合は、IPspaceオブジェクトをパートナークラスタに手動でレプリケートする必要があります。IPspaceをレプリケートする前に作成されてIPspaceに割り当てられたSVMは、パートナークラスタにレプリケートされません。

ブロードキャストドメインは「デフォルト」のIPspaceに自動的に作成され、次のコマンドを使用してIPspace間で移動できます。

```
network port broadcast-domain move
```

たとえば、ブロードキャストドメインを「default」から「ips1」に移動する場合は、次のコマンドを使用します。

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

ONTAPネットワーク上のIPspaceの表示

クラスタに存在するIPspaceのリストを表示して、各IPspaceに割り当てられているStorage Virtual Machine（SVM）、ブロードキャストドメイン、およびポートを確認することができます。

ステップ

クラスタ内の IPspace と SVM を表示します。

```
network ipspace show [-ipspace ipspace_name]
```

次のコマンドは、クラスタ内の IPspace 、 SVM 、およびブロードキャストドメインをすべて表示します。

```
network ipspace show
IPspace         Vserver List              Broadcast Domains
-------------   ------------------------  -------------------
Cluster
                Cluster                   Cluster
Default
                vs1, cluster-1             Default
ipspace1
                vs3, vs4, ipspace1        bcast1
```

次のコマンドは、 ipspace1 という IPspace に属するノードとポートを表示します。

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

の詳細については `network ipspace show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークからのIPspaceの削除

不要になった IPspace は削除できます。

開始する前に

削除する IPspace に関連付けられているブロードキャストドメイン、ネットワークインターフェイス、または SVM がないようにします。

システム定義の「デフォルト」IPspaceと「クラスタ」IPspaceは削除できません。

ステップ

IPspaceを削除します。

```
network ipspace delete -ipspace ipspace_name
```

次のコマンドは、クラスタから ipspace1 という IPspace を削除します。

```
network ipspace delete -ipspace ipspace1
```

の詳細については `network ipspace delete`、を"ONTAPコマンド リファレンス"参照してください。

ブロードキャストドメイン

ONTAPブロードキャストドメインの詳細

ブロードキャストドメインは、同じレイヤ2ネットワークに属するネットワークポートをグループ化するためのものです。グループ化したポートは、データトラフィックまたは管理トラフィック用のStorage Virtual Machine（SVM）で使用できます。

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインの管理が異なります。ONTAP 9.7以前を実行しているネットワークでブロードキャストドメインを管理する必要がある場合は、を参照してください"ブロードキャストドメインの概要（ONTAP 9 .7以前）"。

ブロードキャストドメインはIPspace内にあります。クラスタの初期化では、デフォルトのブロードキャストドメインが2つ作成されます。

- 「Default」ブロードキャストドメインには、「Default」IPspace内のポートが含まれています。

  これらのポートは、主にデータの提供に使用されます。クラスタ管理ポートとノード管理ポートも、このブロードキャスト ドメインに含まれています。

- 「Cluster」ブロードキャスト ドメインには、「Cluster」IPspace内にあるポートが含まれています。

  これらのポートはクラスタ通信に使われ、クラスタの全ノードのすべてのクラスタ ポートが含まれています。

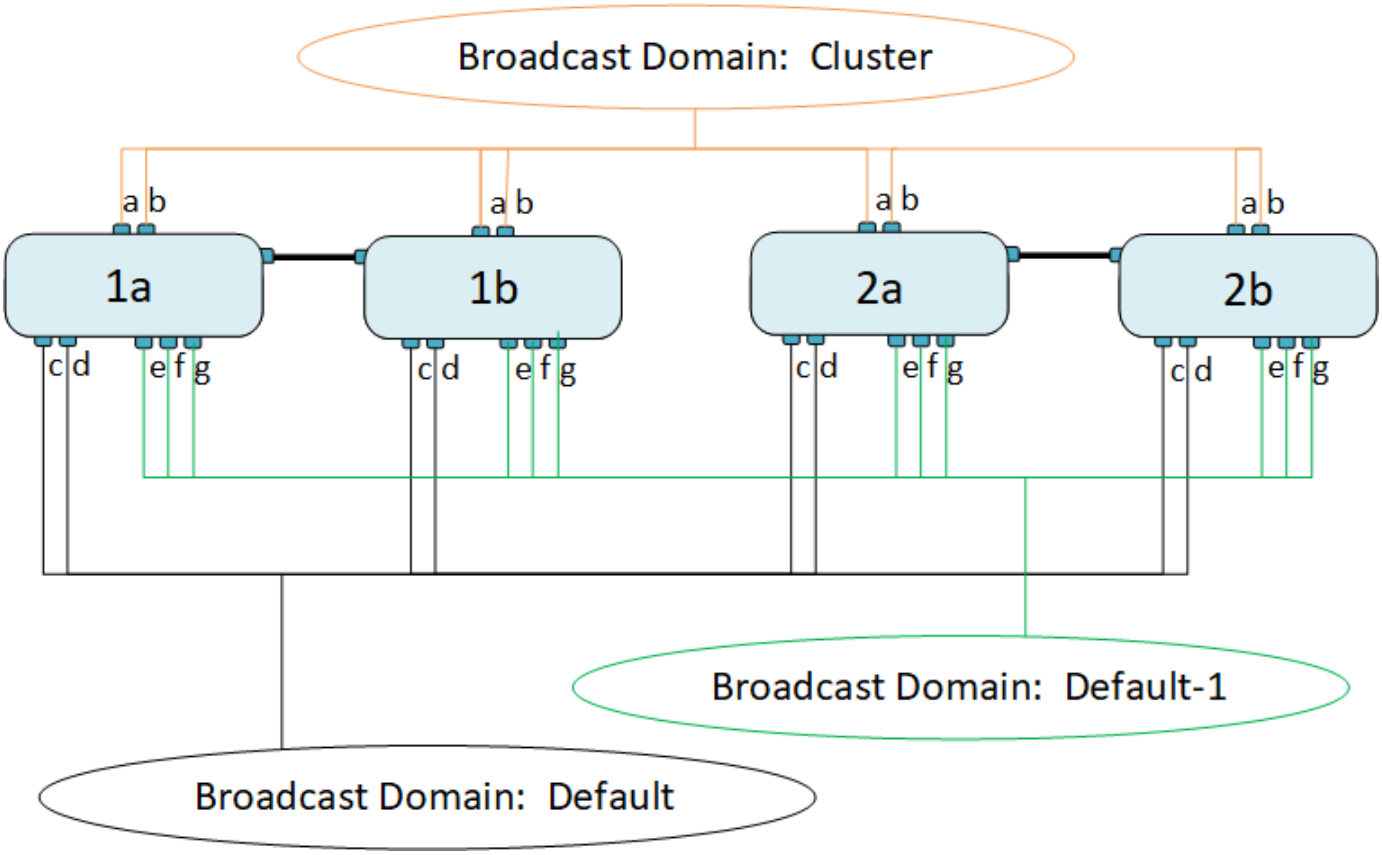
  必要に応じて、ブロードキャスト ドメインがDefault IPspaceに追加で作成されます。「Default」ブロードキャスト ドメインには、管理LIFのホーム ポートと、そのポートへのレイヤ2の到達可能性があるポートがすべて含まれています。追加のブロードキャスト ドメインの名前は、「Default-1」、「Default-2」などとなります。

ブロードキャスト ドメインの使用例

ブロードキャスト ドメインは、同じIPspace内にあり、相互にレイヤ2の到達可能性があるネットワーク ポートの集まりです。一般にクラスタ内の複数のノードのポートが含まれます。

次の図は、4ノード クラスタの3つのブロードキャスト ドメインにポートを割り当てている例を示します。

- 「Cluster」ブロードキャストドメインは、クラスタの初期化時に自動的に作成され、クラスタ内の各ノードのポートaとbが含まれます。
- 「default」ブロードキャストドメインもクラスタの初期化時に自動的に作成され、クラスタ内の各ノードのポートcとdが含まれます。
- クラスタの初期化時に、レイヤ2ネットワークの到達可能性に基づいて追加のブロードキャストドメインが自動的に作成されます。これらの追加のブロードキャストドメインの名前は、Default-1、Default-2のようになります。



各ブロードキャストドメインと同じ名前で、同じネットワークポートを持つフェイルオーバーグループが自動的に作成されます。このフェイルオーバーグループはシステムによって自動的に管理されます。つまり、ブロードキャストドメインのポートが追加または削除されると、そのフェイルオーバーグループのポートも自動的に追加または削除されます。

ONTAPブロードキャストドメインの作成

ブロードキャストドメインは、同じレイヤ2ネットワークに属するクラスタ内のネットワークポートをグループ化します。作成したポートはSVMで使用できます。

ブロードキャストドメインは、クラスタの作成時または追加時に自動的に作成されます。ONTAP 9.12.0以降

では、自動的に作成されたブロードキャストドメインに加えて、System Managerで手動でブロードキャストドメインを追加できます。

> ブロードキャストドメインの作成手順は、ONTAP 9.7以前のバージョンで異なります。ONTAP 9.7以前を実行するネットワークでブロードキャストドメインを作成する必要がある場合は、を参照してください"ブロードキャストドメインの作成（ONTAP 9 .7以前）"。

開始する前に

ブロードキャストドメインに追加するポートは、別のブロードキャストドメインに属していないポートである必要があります。使用するポートが別のブロードキャストドメインに属しているが、使用されていない場合は、元のブロードキャストドメインからそれらのポートを削除します。

タスクの内容

- ブロードキャストドメイン名はすべてIPspace内で一意である必要があります。
- ブロードキャストドメインに追加できるポートは、物理ネットワークポート、VLAN、リンクアグリゲーショングループ/インターフェイスグループ（LAG / ifgrp）です。
- 使用するポートが別のブロードキャストドメインに属しているが、使用されていない場合は、新しいブロードキャストドメインに追加する前に既存のブロードキャストドメインから削除してください。
- ブロードキャストドメインに追加されたポートのMaximum Transmission Unit（MTU；最大伝送ユニット）は、ブロードキャストドメインに設定されているMTU値に更新されます。
- MTU値は、管理トラフィックを処理するe0Mポートを除き、そのレイヤ2ネットワークに接続されているすべてのデバイスで同じである必要があります。
- IPspace名を指定しない場合、ブロードキャストドメインは「Default」IPspaceに作成されます。

システムの設定を簡単にするために、同じポートを含む同じ名前のフェイルオーバーグループが自動的に作成されます。

System Manager

手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン*]を選択します。
2. をクリックし ＋ Add
3. ブロードキャストドメインの名前を指定します。
4. MTUを設定します。
5. IPspaceを選択します。
6. ブロードキャスト ドメインを保存します。

ブロードキャスト ドメインは追加後に編集または削除できます。

CLI

ONTAP 9 .8以降を使用している場合は、レイヤ2の到達可能性に基づいてブロードキャストドメインが自動的に作成されます。詳細については、を参照してください "ポートの到達可能性を修復"。

ブロードキャストドメインを手動で作成することもできます。

手順

1. 現在ブロードキャストドメインに割り当てられていないポートを表示します。

   ```
   network port show
   ```

   大量のポートが表示される場合は、コマンドを使用し `network port show -broadcast-domain`て未割り当てのポートだけを表示します。

2. ブロードキャストドメインを作成します。

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name`は、作成するブロードキャストドメインの名前です。
   b. `mtu_value`はIPパケットのMTUサイズです。通常は1500と9000です。

      この値は、このブロードキャストドメインに追加するすべてのポートに適用されます。

   c. `ipspace_name`は、このブロードキャストドメインを追加するIPspaceの名前です。

      このパラメータの値を指定しないかぎり、「Default」IPspaceが使用されます。

   d. `ports_list`は、ブロードキャストドメインに追加するポートのリストです。

      ポートは、などの形式で追加され `node_name:port_number` `node1:e0c`ます。

3. 必要に応じてブロードキャストドメインが作成されたことを確認します。

   ```
   network port show -instance -broadcast-domain new_domain
   ```

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドは、Default IPspaceにブロードキャストドメインbcast1を作成し、MTUを1500に設定してポートを4つ追加します。

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

の詳細については `network port broadcast-domain create`、を"ONTAPコマンド リファレンス"参照してください。

終了後

この時点で、サブネットを作成してブロードキャストドメインで使用可能になるIPアドレスのプールを定義するか、SVMとインターフェイスをIPspaceに割り当てることができます。詳細については、を参照してください "クラスタとSVMのピアリング"。

既存のブロードキャストドメインの名前を変更する必要がある場合は、コマンドを使用し `network port broadcast-domain rename`ます。

の詳細については `network port broadcast-domain rename`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPブロードキャストドメインのポートを追加または削除する

ブロードキャストドメインは、クラスタの作成時または追加時に自動的に作成されます。ブロードキャストドメインからポートを手動で削除する必要はありません。

物理的なネットワーク接続またはスイッチ設定によってネットワークポートの到達可能性が変わり、ネットワークポートが別のブロードキャストドメインに属している場合は、次のトピックを参照してください。

"ポートの到達可能性を修復"

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインのポートを追加または削除する手順が異なります。ONTAP 9.7以前を実行しているネットワークのブロードキャストドメインに対してポートを追加または削除する必要がある場合は、を参照してください"ブロードキャストドメイン（ONTAP 9 .7以前）のポートを追加または削除します。"。

System Manager

ONTAP 9 14.1以降では、System Managerを使用してブロードキャストドメイン間でイーサネットポートを再割り当てできます。すべてのイーサネットポートをブロードキャストドメインに割り当てることを推奨します。そのため、ブロードキャストドメインからイーサネットポートの割り当てを解除した場合は、別のブロードキャストドメインに再割り当てする必要があります。

手順

イーサネットポートを再割り当てするには、次の手順を実行します。

1. [ネットワーク]>[概要]*を選択します。
2. [ブロードキャストドメイン]*セクションで、ドメイン名の横にあるを選択します ⋮ 。
3. ドロップダウンメニューで、 * Edit * を選択します。
4. [ブロードキャストドメインの編集]*ページで、別のドメインに再割り当てするイーサネットポートの選択を解除します。
5. 選択解除された各ポートについて、* Reassign Ethernet Port ウィンドウが表示されます。ポートを再割り当てするブロードキャストドメインを選択し、[再割り当て]*を選択します。
6. 現在のブロードキャストドメインに割り当てるすべてのポートを選択し、変更を保存します。

CLI

物理的なネットワーク接続またはスイッチ設定によってネットワークポートの到達可能性が変わり、ネットワークポートが別のブロードキャストドメインに属している場合は、次のトピックを参照してください。

"ポートの到達可能性を修復"

または、コマンドまたは `network port broadcast-domain remove-ports`コマンドを使用して、ブロードキャストドメインに対してポートを手動で追加または削除することもできます `network port broadcast-domain add-ports`。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- ブロードキャストドメインに追加するポートは、別のブロードキャストドメインに属していないポートにする必要があります。
- すでにインターフェイスグループに属しているポートを個別にブロードキャストドメインに追加することはできません。

タスクの内容

ネットワークポートの追加と削除には、次のルールが適用されます。

ポートの追加	ポートの削除
ネットワークポート、VLAN、インターフェイスグループ（ifgrp）のいずれかです。	N/A
ポートは、ブロードキャストドメインのシステム定義のフェイルオーバーグループに追加されます。	ポートはブロードキャストドメインのすべてのフェイルオーバーグループから削除されます。

ポートのMTUは、ブロードキャストドメインに設定されているMTU値に更新されます。	ポートのMTUは変更されません。
ポートのIPspaceがブロードキャストドメインのIPspaceの値に更新されます。	ポートはブロードキャストドメイン属性のない「Default」IPspaceに移動されます。

インターフェイスグループの最後のメンバーポートをコマンドを使用して削除する `network port ifgrp remove-port`と、そのインターフェイスグループポートがブロードキャストドメインから削除されます。これは、ブロードキャストドメインに空のインターフェイスグループポートが存在できないためです。の詳細については `network port ifgrp remove-port`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用して、ブロードキャストドメインに現在割り当てられているポートまたは割り当てられていないポートを表示します `network port show`。
2. ブロードキャストドメインにネットワークポートを追加または削除します。

状況	使用方法
ブロードキャストドメインにポートを追加する	`network port broadcast-domain add-ports`
ブロードキャストドメインからポートを削除する	`network port broadcast-domain remove-ports`

3. ポートがブロードキャストドメインに対して追加または削除されたことを確認します。

   `network port show`

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

ポートの追加と削除の例

次のコマンドは、Default IPspaceのブロードキャスト ドメインbcast1に、ノードcluster-1-01のポートe0gと、ノードcluster-1-02のe0gを追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

次のコマンドは、Cluster IPspaceのブロードキャスト ドメインClusterに、クラスタ ポートを2つ追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

次のコマンドは、Default IPspaceのブロードキャスト ドメインbcast1から、ノードcluster1-01のポートe0eを削除します。

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

の詳細については `network port broadcast-domain remove-ports`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "ONTAPコマンド リファレンス"

ONTAPポートの到達可能性を修復

ブロードキャストドメインが自動的に作成されます。ただし、ポートを再接続した場合やスイッチの設定を変更した場合は、ポートを別のブロードキャストドメイン（新規または既存）に修復しなければならないことがあります。

ONTAPは、ブロードキャストドメインコンスティチュエント（イーサネットポート）のレイヤ2の到達可能性に基づいて、ネットワーク配線の問題を自動的に検出し、解決策を提案します。

の配線が正しくないと、ブロードキャストドメインポートが予期せず割り当てられる可能性があります。ONTAP 9 .10.1以降では、クラスタのセットアップ後や新しいノードが既存のクラスタに追加されたときに、クラスタでポートに到達できるかどうかを確認することで、ネットワーク配線の問題がないかどうかを自動的にチェックします。

System Manager

ポートの到達可能性の問題が検出された場合、System Managerでは修復処理を実行して問題を解決することを推奨します。

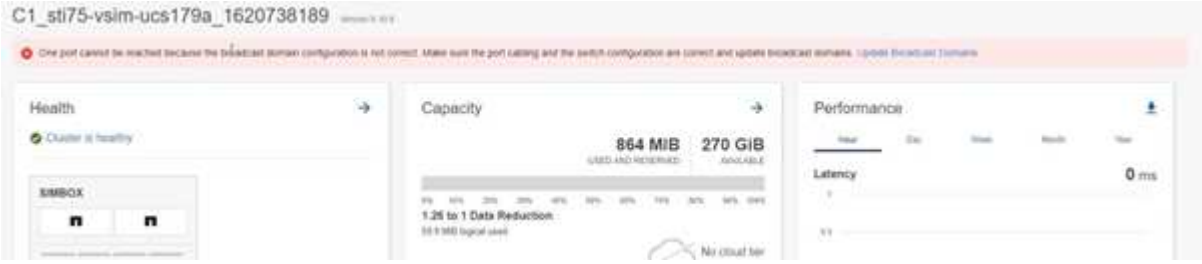
クラスタのセットアップが完了すると、ネットワーク配線の問題がダッシュボードに報告されます。

新しいノードをクラスタに追加すると、[Nodes]ページにネットワーク配線の問題が表示されます。

ネットワーク配線の健全性は、ネットワークダイアグラムで確認することもできます。ポートの到達可能性の問題は、ネットワークダイアグラムに赤いエラーアイコンで示されます。

クラスタのセットアップ後

クラスタのセットアップ後にネットワーク配線の問題が検出されると、ダッシュボードにメッセージが表示されます。



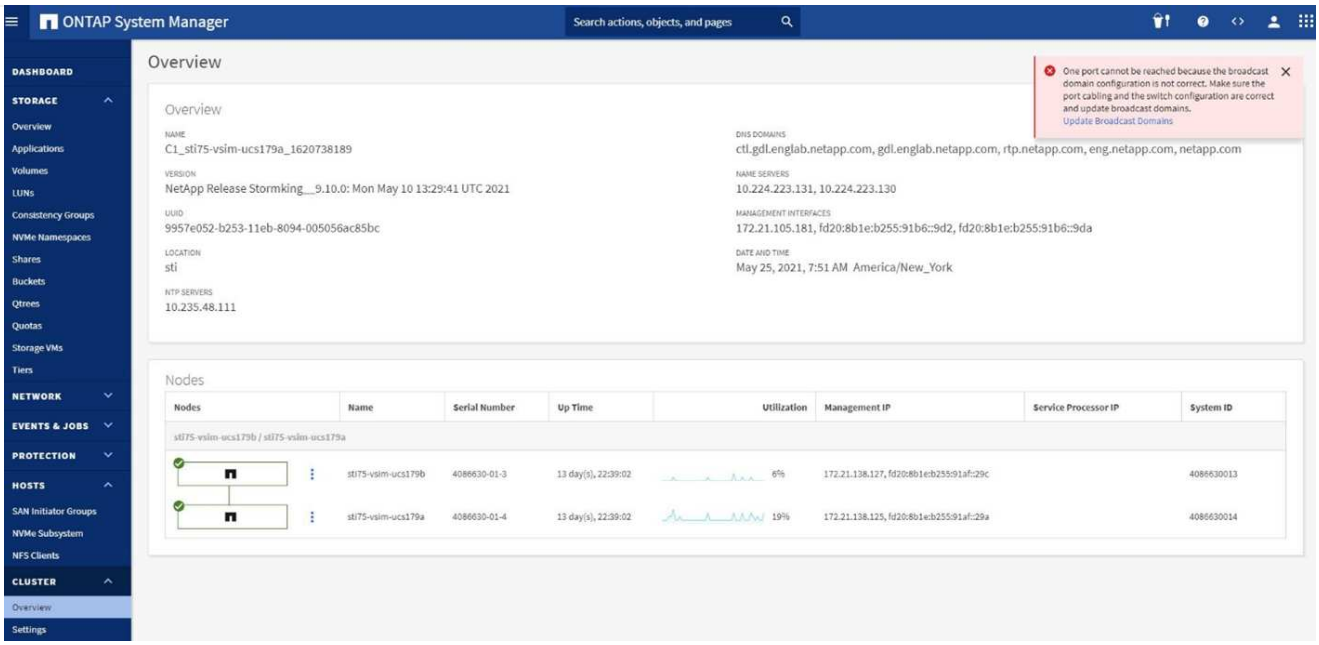
手順

1. メッセージに記載されているように配線を修正します。
2. リンクをクリックして[Update Broadcast Domains]ダイアログを起動します。[ブロードキャストドメインの更新]ダイアログが開きます。

ダイアログ"]
3. ポートに関する情報（ノード、問題、現在のブロードキャストドメイン、想定されるブロードキャストドメインなど）を確認します。
4. 修復するポートを選択し、 [* Fix] をクリックします。ポートは現在のブロードキャストドメインから想定されるブロードキャストドメインに移動されます。

ノードの追加後

新しいノードをクラスタに追加したあとにネットワーク配線の問題が検出されると、[Nodes]ページにメッセージが表示されます。



手順

1. メッセージに記載されているように配線を修正します。
2. リンクをクリックして[Update Broadcast Domains]ダイアログを起動します。[ブロードキャストドメインの更新]ダイアログが開きます。
ダイアログ"]

3. ポートに関する情報（ノード、問題、現在のブロードキャストドメイン、想定されるブロードキャストドメインなど）を確認します。
4. 修復するポートを選択し、 [* Fix] をクリックします。ポートは現在のブロードキャストドメインから想定されるブロードキャストドメインに移動されます。

CLI

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

タスクの内容

ONTAPで検出されたレイヤ2の到達可能性に基づいて、ポートのブロードキャストドメイン設定を自動的に修復するコマンドを使用できます。

手順

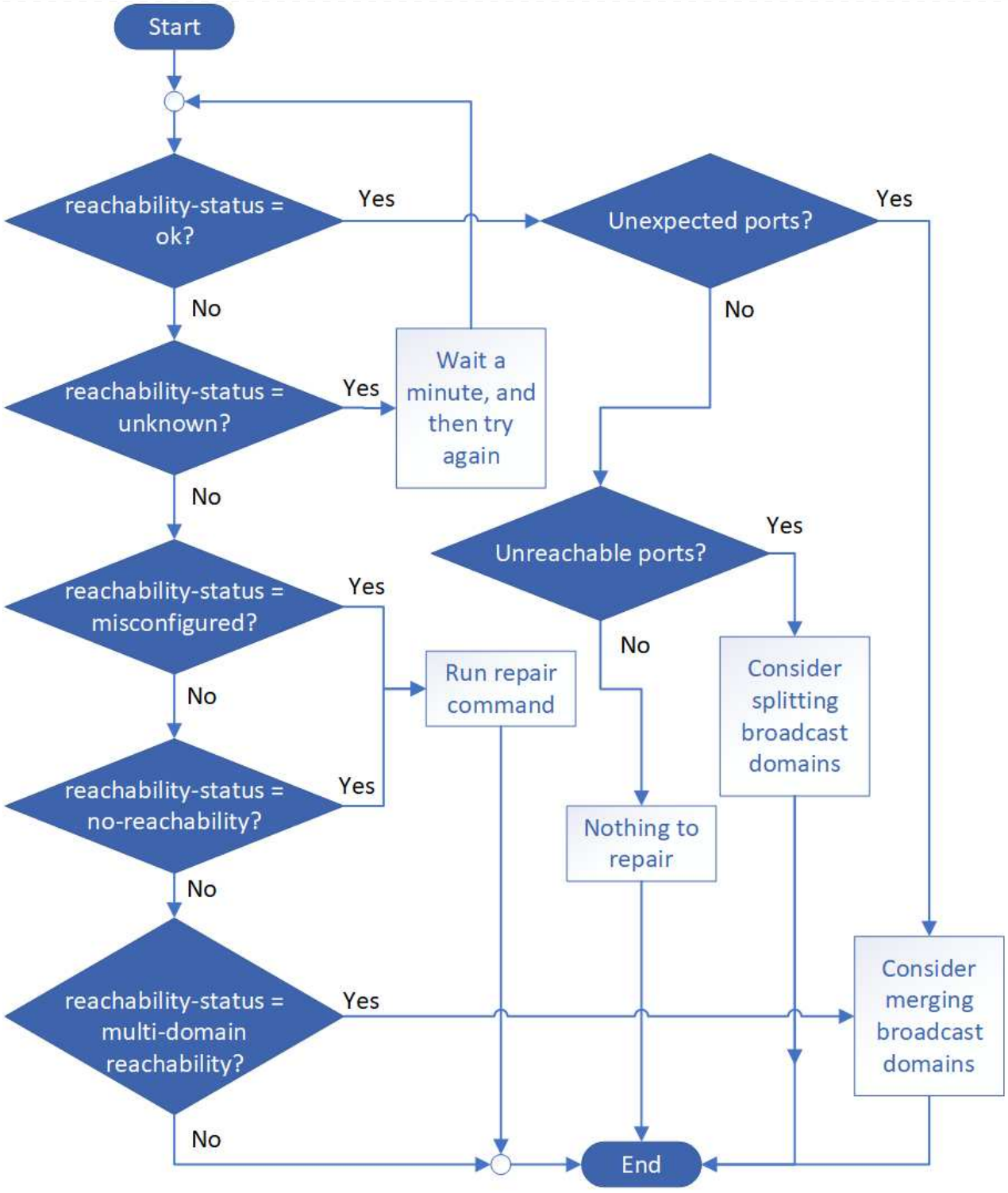
1. スイッチの構成とケーブル接続を確認します。
2. ポートの到達可能性を確認します。

   ```
   network port reachability show -detail -node -port
   ```

   コマンドの出力に到達可能性の結果が表示されます。

   の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。

3. 次のデシジョン ツリーと表を参照して、到達可能性の結果を理解し、次に実行する手順を確認します。



プレゼンスステータス	説明

OK	ポートに割り当てられているブロードキャストドメインにレイヤ 2 の到達可能性があります。到達可能性ステータスが「ok」で、「予期しないポート」がある場合は、1つ以上のブロードキャストドメインをマージすることを検討してください。詳細については、次の _unexpected ports_row を参照してください。 到達可能性ステータスが「ok」で、到達不能なポートがある場合は、1つ以上のブロードキャストドメインをスプリットすることを検討してください。詳細については、次の _Unreachable Ports_row を参照してください。 到達可能性ステータスが「ok」で、予期しないポートや到達不能なポートがない場合、設定は正しいです。
予期しないポートです	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、ポートに割り当てられているブロードキャストドメインを1つ以上のブロードキャストドメインにマージする必要がないかどうかを確認します。 詳細については、を参照してください "ブロードキャストドメインのマージ"。
到達不能ポート	1 つのブロードキャストドメインが 2 つの異なる到達可能性セットにパーティショニングされている場合は、ブロードキャストドメインをスプリットして ONTAP 構成を物理ネットワークトポロジと同期できます。 通常、到達不能なポートのリストには、物理的な設定とスイッチの設定に間違いがないことを確認したあとに、これらのポートを別のブロードキャストドメインに分割する必要があります。 詳細については、を参照してください "ブロードキャストドメインのスプリット"。
誤設定 - 到達可能性	ポートに割り当てられているブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、到達可能なブロードキャストドメインにポートが割り当てられます。 `network port reachability repair -node -port`

到達不能	既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、自動的にデフォルトIPspace内に作成された新しいブロードキャストドメインにポートが割り当てられます。 `network port reachability repair -node -port` *注：*すべてのインターフェイスグループ（ifgrp）メンバーポートがレポートされた場合、 `no-reachability`メンバーポートごとにコマンドを実行する `network port reachability repair`と、各ポートが`ifgrp`から削除されて新しいブロードキャストドメインに配置され、`ifgrp`自体が削除されます。コマンドを実行する前に `network port reachability repair`、物理ネットワークトポロジに基づいて、ポートに到達可能なブロードキャストドメインが想定どおりであることを確認してください。 の詳細については `network port reachability repair`、を"ONTAPコマンド リファレンス"参照してください。
multi-domain-reachable	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、ポートに割り当てられているブロードキャストドメインを1つ以上のブロードキャストドメインにマージする必要がないかどうかを確認します。 詳細については、を参照してください "ブロードキャストドメインのマージ"。
不明	reachable-status が「 unknown 」の場合は、数分待ってからもう一度コマンドを実行してください。

ポートを修理したら、削除されたLIFとVLANがないか確認します。ポートがインターフェイスグループに属していた場合は、そのインターフェイスグループの状況についても理解しておく必要があります。

LIF

ポートが修復されて別のブロードキャスト ドメインに移されると、そのポートに設定されていたLIFには新しいホーム ポートが自動的に割り当てられます。このホーム ポートは、同じノード上の同じブロードキャスト ドメインから選択されます（可能な場合）。または別のノードからホーム ポートが選択されることもあります。適切なホーム ポートがない場合、ホーム ポートはクリアされます。

LIFのホーム ポートが別のノードに移された場合、またはクリアされた場合、そのLIFは「孤立状態」とみなされます。孤立状態のLIFは次のコマンドで確認できます。

```
displaced-interface show
```

孤立状態のLIFがある場合は、次のいずれかを行う必要があります。

- 孤立状態のLIFのホームをリストアする。

  ```
  displaced-interface restore
  ```

- LIFのホームを手動で設定する。

  ```
  network interface modify -home-port -home-node
  ```

  の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

- 現在設定されているLIFのホームに問題がなければ、「displaced-interface」テーブルからエントリを削除する。

  ```
  displaced-interface delete
  ```

VLAN

修復されたポートにVLANが設定されていた場合、それらのVLANは自動的に削除されますが、「削除」されたことも記録されます。削除されたVLANは次のとおりです。

```
displaced-vlans show
```

削除されたVLANがある場合は、次のいずれかを実行する必要があります。

- VLANを別のポートにリストアします。

  ```
  displaced-vlans restore
  ```

- 「displaced-VLANs」テーブルからエントリを削除します。

  ```
  displaced-vlans delete
  ```

インターフェイスグループ

修復されたポートがインターフェイスグループに属していた場合は、そのインターフェイスグループから削除されます。インターフェイスグループに割り当てられていた唯一のメンバーポートであった場合は、インターフェイスグループ自体が削除されます。

関連情報

- "Verify your network configuration after upgrading"
- "ネットワーク ポートの到達可能性の監視"
- "ONTAPコマンド リファレンス"

ONTAPブロードキャストドメインをIPspaceに移動します。

ONTAP 9.8以降では、レイヤ2の到達可能性に基づいてシステムで作成されたブロードキャストドメインを、作成したIPspaceに移動できます。

ブロードキャストドメインを移動する前に、ブロードキャストドメイン内のポートに到達できるかどうかを確認する必要があります。

ポートの自動スキャンでは、相互にアクセスできるポートを特定して同じブロードキャストドメインに配置できますが、このスキャンでは適切なIPspaceを特定できません。ブロードキャストドメインがデフォルト以外

のIPspaceに属している場合は、このセクションの手順に従って手動で移動する必要があります。

開始する前に

ブロードキャストドメインは、クラスタの作成時および追加時に自動的に設定されます。ONTAPでは、「default」ブロードキャストドメインとは、クラスタに最初に作成されたノード上の管理インターフェイスのホームポートへレイヤ2で接続されている一連のポートを指します。他のブロードキャストドメインも必要に応じて作成され、「 * default-1 * 」、「 * default-2 * 」などの名前が付けられます。

既存のクラスタにノードを追加すると、そのネットワークポートはレイヤ2の到達可能性に基づいて既存のブロードキャストドメインに自動的に追加されます。既存のブロードキャストドメインに到達できない場合、ポートは1つ以上の新しいブロードキャストドメインに配置されます。

タスクの内容

- クラスタLIFが設定されたポートは、自動的に「Cluster」IPspaceに配置されます。
- ノード管理LIFのホームポートに到達できるポートは、「Default」ブロードキャストドメインに配置されます。
- その他のブロードキャストドメインは、クラスタの作成時または追加時にONTAPによって自動的に作成されます。
- VLANとインターフェイスグループを追加すると、作成してから約1分後に適切なブロードキャストドメインに自動的に配置されます。

手順

1. ブロードキャストドメイン内のポートに到達できるかどうかを確認します。ONTAPはレイヤ2の到達可能性を自動的に監視します。次のコマンドを使用して、各ポートがブロードキャストドメインに追加され、到達可能性が「ok」になっていることを確認します。

   ```
   network port reachability show -detail
   ```

   の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。

2. 必要に応じて、ブロードキャストドメインを他のIPspaceに移動します。

   ```
   network port broadcast-domain move
   ```

   たとえば、ブロードキャストドメインを「Default」から「ips1」に移動する場合は、次の手順を実行します。

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

関連情報

- "ネットワークポートのブロードキャストドメインの移動"

ONTAPブロードキャストドメインのスプリット

物理的なネットワーク接続やスイッチ設定によってネットワークポートの到達可能性が変わり、単一のブロードキャストドメインに設定されていたネットワークポートのグループが到達可能性の異なる2つのグループに分割された場合は、ブロードキャストドメイ

ンをスプリットしてONTAP設定を物理的なネットワークトポロジと同期できます。

> ONTAP 9.7以前のバージョンでは、ブロードキャストドメインのスプリット手順が異なります。ONTAP 9.7以前を実行するネットワークでブロードキャストドメインをスプリットする必要がある場合は、を参照してください"ブロードキャストドメインのスプリット（ONTAP 9 .7以前）"。

ネットワークポートのブロードキャストドメインが到達可能性の複数のセットに分割されているかどうかを確認するには、コマンドを使用し `network port reachability show -details`て、相互に接続されていないポート（「`Unreachable ports`」）に注意してください。一般に、到達不能ポートのリストでは、物理ポートとスイッチの設定が正確であることを確認したあとに、別のブロードキャストドメインにスプリットする必要があるポートを定義します。の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

ブロードキャストドメインを2つのブロードキャストドメインにスプリットします。

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name`は、ブロードキャストドメインが配置されているIPspaceの名前です。
- -`broadcast-domain`は、スプリットするブロードキャストドメインの名前です。
- -`new-broadcast-domain`は、作成する新しいブロードキャストドメインの名前です。
- -`ports`は、新しいブロードキャストドメインに追加するノードの名前とポートです。

関連情報

- "ネットワークポートのブロードキャストドメインのスプリット"

ONTAPブロードキャストドメインのマージ

物理的なネットワーク接続またはスイッチ設定によってネットワークポートの到達可能性が変わり、複数のブロードキャストドメインに設定されていた2つのグループのネットワークポートがすべて到達可能性を共有するようになった場合は、2つのブロードキャストドメインをマージしてONTAP設定を物理的なネットワークトポロジに同期できます。

> ONTAP 9.7以前のバージョンでは、ブロードキャストドメインのマージ手順が異なります。ONTAP 9.7以前を実行しているネットワークのブロードキャストドメインをマージする必要がある場合は、を参照してください"ブロードキャストドメインのマージ（ONTAP 9.7以前）"。

複数のブロードキャストドメインが1つの到達可能性セットに属しているかどうかを確認するには、`network port reachability show -details`コマンドを実行し、別のブロードキャストドメインに設定されているポートのうち、実際に相互に接続されているポート（「予期しないポート」）に注目してください。通常、予期しないポートのリストは、物理構成とスイッチ構成が正確であることを確認した後、ブロードキャストドメインに統合する必要があるポートのセットを定義します。

の詳細については `network port reachability show`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1つのブロードキャストドメインのポートを既存のブロードキャストドメインにマージします。

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name`は、ブロードキャストドメインのあるIPspaceの名前です。
- `-broadcast-domain`は、マージするブロードキャストドメインの名前です。
- `-into-broadcast-domain`は、追加のポートを受け取るブロードキャストドメインの名前です。

関連情報

- "network port broadcast-domain-merge"

ONTAPブロードキャストドメインのポートのMTU値を変更する

あるブロードキャストドメインのMTU値を変更して、そのブロードキャストドメイン内のすべてのポートのMTU値を変更できます。これは、ネットワークで行われたトポロジの変更をサポートするために実行できます。

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインポートのMTU値を変更する手順が異なります。ONTAP 9.7以前を実行しているネットワークでブロードキャストドメインポートのMTU値を変更する必要がある場合は、を参照してください"ブロードキャストドメイン（ONTAP 9 .7以前）のポートのMTU値を変更する"。

開始する前に

MTU値は、管理トラフィックを処理するe0Mポートを除き、そのレイヤ2ネットワークに接続されているすべてのデバイスで同じである必要があります。

タスクの内容

MTU値を変更すると、影響を受けるポートを経由するトラフィックが一時的に中断されます。プロンプトが表示され、MTUを変更するには「y」と入力する必要があります。

ステップ

ブロードキャストドメインのすべてのポートのMTU値を変更します。

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain`は、ブロードキャストドメインの名前です。
- `mtu`はIPパケットのMTUサイズです。通常は1500と9000です。

- `ipspace`は、このブロードキャストドメインが配置されているIPspaceの名前です。このオプションの値を指定しないかぎり、「Default」IPspaceが使用されます。次のコマンドは、ブロードキャストドメインbcast1のすべてのポートのMTUを9000に変更します。

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

関連情報

- "network port broadcast-domain modify"

ONTAPブロードキャストドメインの表示

クラスタ内の各IPspace内のブロードキャストドメインのリストを表示できます。この出力には、各ブロードキャストドメインのポートとMTU値のリストも表示されます。

ブロードキャストドメインの表示手順は、ONTAP 9.7以前のバージョンで異なります。ONTAP 9.7以前を実行しているネットワークのブロードキャストドメインを表示する必要がある場合は、を参照してください"ブロードキャストドメインを表示する（ONTAP 9.7以前）"。

ステップ

クラスタのブロードキャストドメインと関連付けられているポートを表示します。

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

次のコマンドは、クラスタ内のすべてのブロードキャストドメインと関連付けられているポートを表示します。

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

次のコマンドは、default-1ブロードキャストドメインのポートのうち、更新ステータスがerrorになっている（ポートを適切に更新できなかった）ポートを表示します。

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Default Default-1    1500
                           cluster-1-02:e0g       error
```

関連情報

- "network port broadcast-domain show"

ONTAPブロードキャストドメインの削除

不要になったブロードキャストドメインは削除できます。これにより、指定したブロードキャストドメインに関連付けられているポートが「デフォルト」のIPspaceに移動されます。

開始する前に

削除するブロードキャストドメインに、関連付けられているサブネット、ネットワークインターフェイス、またはSVMがないようにします。

タスクの内容

- システムで作成された「Cluster」ブロードキャストドメインは削除できません。
- ブロードキャストドメインを削除すると、そのブロードキャストドメインに関連するフェイルオーバーグループがすべて削除されます。

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

System Manager

- ONTAP 9.12.0以降では、System Managerを使用してブロードキャストドメイン*を削除できます

ブロードキャストドメインにポートが含まれている場合、またはブロードキャストドメインがサブネットに関連付けられている場合は、deleteオプションは表示されません。

手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン*]を選択します。
2. 削除するブロードキャストドメインの横にある*> Delete *を選択します ⋮ 。

CLI

*ブロードキャストドメイン*を削除するには、CLIを使用してください

ステップ

ブロードキャストドメインを削除します。

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

次のコマンドは、ipspace1というIPspaceのブロードキャストドメインdefault-1を削除します。

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

関連情報

- "network port broadcast-domain delete"

フェイルオーバーグループとポリシー

ONTAPネットワークでのLIFフェイルオーバーの詳細

LIFのフェイルオーバーとは、LIFの現在のポートでリンク障害が発生した場合に、別のネットワークポートにLIFを自動的に移行する機能です。これは、SVMとの接続の高可用性を実現するための重要なコンポーネントです。LIFフェイルオーバーを設定するには、フェイルオーバーグループを作成し、フェイルオーバーグループを使用するようにLIFを変更して、フェイルオーバーポリシーを指定します。

フェイルオーバーグループには、クラスタ内の1つ以上のノードの一連のネットワークポート（物理ポート、VLAN、およびインターフェイスグループ）が含まれます。フェイルオーバーグループに含まれるネットワークポートによって、LIFで使用可能なフェイルオーバーターゲットが定義されます。フェイルオーバーグループには、クラスタ管理LIF、ノード管理LIF、クラスタ間LIF、およびNASデータLIFを割り当てることができます。

> LIFに有効なフェイルオーバーターゲットが設定されていないと、LIFがフェイルオーバーしようとしたときにシステムが停止します。フェイルオーバーの設定を確認するには、コマンドを使用し `network interface show -failover`ます。の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ブロードキャストドメインを作成すると、同じネットワークポートを含む同じ名前のフェイルオーバーグループが自動的に作成されます。このフェイルオーバーグループはシステムによって自動的に管理されます。つまり、ブロードキャストドメインのポートが追加または削除されると、そのフェイルオーバーグループのポートも自動的に追加または削除されます。これは、管理者が自分でフェイルオーバーグループを管理する必要がない場合に効率的に機能するためです。

ONTAPフェイルオーバーグループを作成する

ネットワークポートのフェイルオーバーグループを作成して、 LIF の現在のポートでリンク障害が発生した場合に、 LIF が別のポートに自動的に移行できるようにします。これにより、システムのネットワークトラフィックがクラスタ内の使用可能な他のポートに再ルーティングされます。

タスクの内容

グループを作成し、そのグループにポートを追加するには、コマンドを使用し `network interface failover-groups create`ます。

- フェイルオーバーグループに追加できるポートは、ネットワークポート、 VLAN 、インターフェイスグループ（ ifgrp ）です。
- フェイルオーバーグループに追加するポートは、すべて同じブロードキャストドメインに属している必要があります。
- 1 つのポートを複数のフェイルオーバーグループに含めることができます。
- 異なる VLAN またはブロードキャストドメインに LIF がある場合は、 VLAN またはブロードキャストドメインごとにフェイルオーバーグループを設定する必要があります。
- フェイルオーバーグループは、 SAN の iSCSI 環境と FC 環境には適用されません。

ステップ

フェイルオーバーグループを作成します。

```
network interface failover-groups create -vserver vserver_name -failover-group
failover_group_name -targets ports_list
```

- `*vserver_name*`は、フェイルオーバーグループを使用できるSVMの名前です。
- `*failover_group_name*`は、作成するフェイルオーバーグループの名前です。
- `*ports_list*`は、フェイルオーバーグループに追加するポートのリストです。node_name > ： < port_number > という形式でポートを指定してください。たとえば、 node1 ： e0c のようになります。

次のコマンドは、 SVM vs3 にフェイルオーバーグループ fg3 を作成してポートを 2 つ追加します。

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

終了後

- フェイルオーバーグループを作成したら、 LIF にフェイルオーバーグループを適用する必要があります。
- 有効なフェイルオーバーターゲットのないフェイルオーバーグループを LIF に設定すると、警告メッセージが表示されます。

  有効なフェイルオーバーターゲットのないLIFがフェイルオーバーしようとすると、システムが停止する可能性があります。

- の詳細については `network interface failover-groups create`、を"ONTAPコマンド リファレンス"参照してください。

LIFのONTAPフェイルオーバーを設定します。

フェイルオーバーポリシーとフェイルオーバーグループをLIFに適用することで、ネットワークポートの特定のグループにLIFをフェイルオーバーするように設定できます。また、LIFの別のポートへのフェイルオーバーを無効にすることもできます。

タスクの内容

- LIFを作成すると、LIFのフェイルオーバーがデフォルトで有効になり、使用可能なターゲットポートのリストは、LIFのタイプとサービスポリシーに基づいたデフォルトのフェイルオーバーグループとフェイルオーバーポリシーによって決まります。

  9.5以降では、LIFを使用できるネットワークサービスを定義するサービスポリシーをLIFに指定できます。一部のネットワークサービスでは、LIFのフェイルオーバーが制限されます。

  > フェイルオーバーをさらに制限するようにLIFのサービスポリシーを変更すると、LIFのフェイルオーバーポリシーはシステムによって自動的に更新されます。

- LIFのフェイルオーバーの動作を変更するには、network interface modifyコマンドの-failover-groupパラメータと-failover-policyパラメータの値を指定します。
- LIFを変更すると、LIFに有効なフェイルオーバーターゲットがなくなるため、警告メッセージが表示されます。

  有効なフェイルオーバーターゲットのないLIFがフェイルオーバーしようとすると、システムが停止する可能性があります。

- All-Flash SAN Array（ASA）プラットフォームでは、Storage.11.1以降で、新規に作成したONTAP 9 VMに新しく作成したiSCSI LIFでiSCSI LIFのフェイルオーバーが自動的に有効になります。

  また、"既存のiSCSI LIFでiSCSI LIFフェイルオーバーを手動で有効にする"ONTAP 9 .11.1以降にアップグレードする前に作成されたLIFを指定することもできます。

- 次に、-failover-policyの設定が、フェイルオーバーグループから選択されるターゲットポートに与える影

響を示します。

> iSCSI LIFのフェイルオーバーの場合は、フェイルオーバーポリシー `sfo-partner-only`と`disabled`のみが `local-only`サポートされます。

- `broadcast-domain-wide`フェイルオーバーグループ内のすべてのノードのすべてのポートに適用されます。
- `system-defined`LIFのホームノードおよびクラスタ内の他の1つのノード（通常はSFOパートナー以外のノード（存在する場合））のポートにのみ適用されます。
- `local-only`LIFのホームノードのポートにのみ適用されます。
- `sfo-partner-only`LIFのホームノードとそのSFOパートナーのポートにのみ適用されます。
- `disabled`LIFにフェイルオーバーが設定されていないことを示します。

手順

既存のインターフェイスのフェイルオーバーを設定します。

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

フェイルオーバーの設定例、および無効化の例

次のコマンドは、フェイルオーバーポリシーをbroadcast-domain-wideに設定し、SVM vs3のdata1というLIFのフェイルオーバーターゲットとして、フェイルオーバーグループfg3のポートを使用します。

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

次のコマンドは、SVM vs3のdata1というLIFのフェイルオーバーを無効にします。

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

関連情報

- "ネットワークインターフェイス"

フェイルオーバーグループとポリシーの管理用ONTAPコマンド

フェイルオーバーグループを管理するには、コマンドを使用し `network interface failover-groups`ます。LIFに適用されるフェイルオーバーグループとフェイルオーバーポリシーを管理するには、コマンドを使用し `network interface modify`ます。

状況	使用するコマンド
フェイルオーバーグループにネットワークポートを追加する	`network interface failover-groups add-targets`
フェイルオーバーグループからネットワークポートを削除する	`network interface failover-groups remove-targets`
フェイルオーバーグループのネットワークポートを変更する	`network interface failover-groups modify`
現在のフェイルオーバーグループを表示します。	`network interface failover-groups show`
LIFのフェイルオーバーを設定する	`network interface modify -failover -group -failover-policy`
各LIFで使用されているフェイルオーバーグループとフェイルオーバーポリシーを表示する	`network interface show -fields failover-group, failover-policy`
フェイルオーバーグループの名前を変更します	`network interface failover-groups rename`
フェイルオーバーグループを削除する	`network interface failover-groups delete`

フェイルオーバーグループを変更して、クラスタ内のどのLIFにも有効なフェイルオーバーターゲットが設定されないようにすると、LIFがフェイルオーバーしようとしたときにシステムが停止する可能性があります。

関連情報

- "ネットワークインターフェイス"

サブネット（クラスタ管理者のみ）

ONTAPネットワークのサブネットについて

サブネットを使用すると、ONTAPネットワーク設定用のIPアドレスの特定のブロックまたはプールを割り当てることができます。IPアドレスとネットワーク マスクの値を指定しなくても、サブネット名を指定して簡単にLIFを作成できるようになります。

サブネットはブロードキャスト ドメイン内に作成され、同じレイヤ3サブネットに属するIPアドレスのプールを含んでいます。サブネット内のIPアドレスは、LIFの作成時にブロードキャスト ドメインのポートに割り当てられます。LIFを削除すると、そのIPアドレスはサブネット プールに返され、以降のLIFで使用できるようになります。

IPアドレスの管理が容易になり、LIFを簡単な手順で作成できるようになるため、サブネットを使用することをお勧めします。さらに、サブネットを定義するときにゲートウェイを指定した場合、そのサブネットを使用してLIFを作成すると、そのゲートウェイへのデフォルト ルートがSVMに自動的に追加されます。

ONTAPネットワークのサブネットを作成する

サブネットを作成してIPv4またはIPv6アドレスの特定のブロックを割り当て、あとでSVMのLIFを作成するときに使用することができます。

これにより、LIFごとにIPアドレスやネットワークマスク値を指定する代わりにサブネット名を指定することで、LIFを簡単に作成できます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

サブネットを追加するブロードキャストドメインとIPspaceがすでに存在している必要があります。

タスクの内容

- サブネット名はすべてIPspace内で一意である必要があります。
- IPアドレスの範囲をサブネットに追加する場合は、異なるサブネットまたはホストが同じIPアドレスを使用しないように、ネットワーク内でIPアドレスが重複しないようにする必要があります。
- サブネットを定義するときにゲートウェイを指定した場合は、そのサブネットを使用してLIFを作成するときに、そのゲートウェイへのデフォルトルートがSVMに自動的に追加されます。サブネットを使用しない場合や、サブネットを定義するときにゲートウェイを指定しない場合は、コマンドを使用してSVMにルートを手動で追加する必要が `route create`あります。
- NetAppでは、データSVMのすべてのLIFに対してサブネットオブジェクトを作成することを推奨しています。これは特にMetroCluster構成で重要です。各サブネットオブジェクトにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してONTAPがデスティネーションクラスタのフェイルオーバーターゲットを決定できます。

手順

サブネットは、ONTAP System ManagerまたはONTAP CLIで作成できます。

System Manager

ONTAP 9.12.0以降では、System Managerを使用してサブネットを作成できます。

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. をクリックし + Add てサブネットを作成します。
3. サブネットに名前を付けます。
4. サブネットのIPアドレスを指定します。
5. サブネット マスクを設定します。
6. サブネットを構成するIPアドレスの範囲を定義します。
7. 必要に応じて、ゲートウェイを指定します。
8. サブネットが属するブロードキャスト ドメインを選択します。
9. 変更を保存します。
   a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます。
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. OK *をクリックすると、既存のLIFがサブネットに関連付けられます。

CLI

CLIを使用してサブネットを作成してください。

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name`は、作成するレイヤ3サブネットの名前です。

  名前には、「Mgmt」のようなテキスト文字列を使用することも、192.0.2.0/24のような特定のサブネットIP値を使用することもできます。

- `broadcast_domain_name`は、サブネットが配置されるブロードキャストドメインの名前です。
- `ipspace_name`は、ブロードキャストドメインが属するIPspaceの名前です。

  このオプションの値を指定しないかぎり、「Default」IPspaceが使用されます。

- `subnet_address`は、サブネットのIPアドレスとマスクです。たとえば、192.0.2.0/24のように指定します。
- `gateway_address`は、サブネットのデフォルトルートのゲートウェイです。たとえば、192.0.2.1のように指定します。
- `ip_address_list`は、サブネットに割り当てるIPアドレスのリストまたは範囲です。

個 々 のアドレス、IPアドレスの範囲、またはその組み合わせをカンマで区切って指定できます。

- オプションの値 `true`を設定できます `-force-update-lif-associations`。

  指定した範囲のIPアドレスを現在使用しているサービスプロセッサまたはネットワークインターフェイスがある場合、このコマンドは失敗します。この値をtrueに設定すると、手動でアドレスを指定したインターフェイスが現在のサブネットに関連付けられ、コマンドが成功します。

次のコマンドは、Default IPspaceのブロードキャストドメインdefault-1にサブネットsub1を作成します。IPv4サブネットのIPアドレスとマスク、ゲートウェイ、およびIPアドレスの範囲を追加します。

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

次のコマンドは、「Default」IPspaceのブロードキャストドメインDefaultにサブネットsub2を作成します。IPv6アドレスの範囲を追加します。

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

終了後

サブネット内のアドレスを使用して、SVMとインターフェイスをIPspaceに割り当てることができます。

既存のサブネットの名前を変更する必要がある場合は、コマンドを使用し `network subnet rename`ます。

の詳細については `network subnet rename`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークのサブネットに対してIPアドレスを追加または削除する

最初にサブネットを作成するときにIPアドレスを追加したり、既存のサブネットにIPアドレスを追加したりできます。また、既存のサブネットからIPアドレスを削除することもできます。これにより、SVMに必要なIPアドレスだけを割り当てることができます。

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

System Manager

- ONTAP 9.12.0以降では、System Managerを使用して、サブネット*に対してIPアドレスを追加または削除できます

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. 変更するサブネットの横にある*>[編集]*を選択します ⋮ 。
3. IPアドレスを追加または削除します。
4. 変更を保存します。
   a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます。
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. OK *をクリックすると、既存のLIFがサブネットに関連付けられます。

CLI

- CLIを使用して、IPアドレスをサブネットに追加したり、サブネットから削除したりします。*

タスクの内容

IPアドレスを追加するときに、追加する範囲のIPアドレスを使用しているサービスプロセッサまたはネットワークインターフェイスがあるとエラーが表示されます。手動でアドレスを指定したインターフェイスを現在のサブネットに関連付ける場合は、このオプションをに `true`設定し `-force-update-lif-associations`ます。

IPアドレスを削除するときに、削除するIPアドレスを使用しているサービスプロセッサまたはネットワークインターフェイスがあるとエラーが表示されます。サブネットから削除したIPアドレスをインターフェイスで引き続き使用するには、オプションをに `true`設定し `-force-update-lif-associations`ます。

ステップ

サブネットのIPアドレスを追加または削除します。

状況	使用するコマンド
サブネットに IP アドレスを追加する	network subnet add-ranges
サブネットから IP アドレスを削除します	network subnet remove-ranges

次のコマンドは、192.0.2.82~192.0.2.85のIPアドレスをサブネットsub1に追加します。

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

次のコマンドは、IPアドレス198.51.100.9をサブネットsub3から削除します。

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

現在の範囲が1～10および20～40で、11～19および41～50（基本的には1～50）を追加する場合は、次のコマンドを使用して既存のアドレス範囲と重複することができます。このコマンドは新しいアドレスのみを追加し、既存のアドレスには影響しません。

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

および `network subnet remove-ranges`の詳細については `network subnet add-ranges`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークのサブネットプロパティの変更

既存のサブネットのサブネットアドレスとマスク値、ゲートウェイアドレス、またはIPアドレスの範囲を変更できます。

タスクの内容

- IPアドレスを変更する場合は、異なるサブネットまたはホストが同じIPアドレスを使用しないように、ネットワーク内でIPアドレスが重複しないようにする必要があります。
- ゲートウェイのIPアドレスを追加または変更した場合、LIFを作成するときに、変更したゲートウェイがサブネットを使用して新しいSVMに適用されます。SVMのゲートウェイへのルートがない場合は、デフォルトルートが作成されます。ゲートウェイのIPアドレスを変更した場合は、SVMに新しいルートを手動で追加しなければならないことがあります。

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

System Manager

- ONTAP 9.12.0以降では、System Managerを使用してサブネットのプロパティを変更できます*

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. 変更するサブネットの横にある*>[編集]*を選択します。
3. 変更を行います。
4. 変更を保存します。
   a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます。
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. OK *をクリックすると、既存のLIFがサブネットに関連付けられます。

CLI

- CLIを使用して、サブネットのプロパティを変更します。*

ステップ

サブネットのプロパティを変更します。

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name`は、変更するサブネットの名前です。
- `ipspace`は、サブネットのあるIPspaceの名前です。
- `subnet`は、サブネットの新しいアドレスとマスクです（該当する場合）。たとえば、192.0.2.0/24のように指定します。
- `gateway`は、サブネットの新しいゲートウェイです（該当する場合）。たとえば、192.0.2.1のように指定します。「 * 」と入力すると、ゲートウェイのエントリが削除されます。
- `ip_ranges`は、サブネットに割り当てる新しいIPアドレスのリストまたは範囲です（該当する場合）。IPアドレスには、個 々 のアドレス、IPアドレスの範囲、またはその組み合わせをカンマで区切って指定できます。ここで指定した範囲を使用すると、既存のIPアドレスが置き換えられます。
- `force-update-lif-associations`は、IPアドレス範囲を変更する場合に必要です。IP アドレスの範囲を変更する場合、このオプションの値を * true * に設定できます。指定した範囲のIPアドレスを使用しているサービスプロセッサまたはネットワークインターフェイスがある場合、このコマンドは失敗します。この値を * true に設定すると、手動でアドレスが指定されているインターフェイスが現在のサブネットに関連付けられ、コマンドは問題なく実行されます。

次のコマンドは、サブネットsub3のゲートウェイIPアドレスを変更します。

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

の詳細については `network subnet modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークのサブネットを表示する

IPspace内の各サブネットに割り当てられているIPアドレスのリストを表示できます。この出力には、各サブネットで使用可能なIPアドレスの総数、および現在使用されているアドレスの数も表示されます。

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

System Manager

- ONTAP 9.12.0以降では、System Managerでサブネットを表示できます*

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. サブネットのリストを表示します。

CLI

- CLIを使用してサブネット*を表示します

ステップ

サブネットのリスト、およびそれらのサブネットで使用されている関連付けられたIPアドレス範囲を表示します。

```
network subnet show
```

次のコマンドは、サブネットとサブネットのプロパティを表示します。

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name    Subnet          Domain    Gateway       Total   Ranges
------  --------------- --------- ------------ --------
-----------------------
sub1    192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3    198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

の詳細については `network subnet show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークからサブネットを削除する

サブネットが不要になり、そのサブネットに割り当てられていたIPアドレスの割り当てを解除するには、サブネットを削除します。

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

System Manager

- ONTAP 9.12.0以降では、System Managerを使用してサブネット*を削除できます

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. 削除するサブネットの横にある*> Delete *を選択します ⋮ 。
3. 変更を保存します。

CLI

- CLIを使用してサブネット*を削除してください

タスクの内容

指定した範囲のIPアドレスを現在使用しているサービスプロセッサまたはネットワークインターフェイスがあると、エラーが表示されます。サブネットを削除したあともインターフェイスでIPアドレスを使用する場合は、-force-update-lif-associationsオプションをtrueに設定して、サブネットとLIFの関連付けを解除します。

ステップ

サブネットを削除します。

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

次のコマンドは、ipspace1というIPspaceのサブネットsub1を削除します。

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

の詳細については `network subnet delete`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワーク用のSVMの作成

クライアントにデータを提供するには、SVMを作成する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- SVMルートボリュームに設定するセキュリティ形式を確認しておく必要があります。

  このSVMにHyper-V over SMBまたはSQL Server over SMBソリューションを実装する場合は、ルートボリュームにNTFSセキュリティ形式を使用する必要があります。Hyper-VファイルまたはSQLデータベースフ

ァイルを格納するボリュームは、作成時にNTFSセキュリティに設定する必要があります。ルートボリュームのセキュリティ形式をNTFSに設定すると、UNIXセキュリティ形式またはmixedセキュリティ形式のデータボリュームを誤って作成しないようになります。

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

System Manager

System Managerを使用してStorage VMを作成できます。

手順

1. Storage VM*を選択します。
2. をクリック + Add してStorage VMを作成します。
3. Storage VMに名前を付けます。
4. アクセスプロトコルを選択します。
   - SMB / CIFS、NFS
   - iSCSI
   - FC
   - NVMe
     i. SMB / CIFSの有効化*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
管理者名	SMB / CIFS Storage VMの管理者ユーザ名を指定してください。
パスワード	SMB / CIFS Storage VMの管理者パスワードを指定してください。
サーバ名	SMB / CIFS Storage VMのサーバ名を指定してください。
Active Directoryドメイン	SMB / CIFS Storage VMにユーザ認証を提供するActive Directoryドメインを指定してください。
組織単位	SMB / CIFSサーバに関連付けられたActive Directoryドメイン内の組織単位を指定します。デフォルト値は「CN=Computers」で、変更できます。
Storage VM内の共有へのアクセス時にデータを暗号化する	SMB 3.0を使用してデータを暗号化し、SMB / CIFS Storage VM内の共有に対する不正なファイルアクセスを防止するには、このチェックボックスを選択します。
ドメイン	SMB / CIFS Storage VMに対して表示されているドメインを追加、削除、または順序変更する。
ネームサーバ	SMB / CIFS Storage VMのネームサーバの追加、削除、または順序変更

デフォルト言語	Storage VMとそのボリュームのデフォルトの言語エンコード設定を指定します。Storage VM内の個々のボリュームの設定を変更する場合はCLIを使用してください。
ネットワークインターフェイス	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage VM管理用のネットワークインターフェイスを追加するかどうかを指定します。

1. Enable NFS（FCの有効化）を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
Allow NFS client accessチェックボックス	NFS Storage VMに作成されたすべてのボリュームで、ルートボリュームパス「/」を使用してマウントとトラバースを行う必要がある場合は、このチェックボックスを選択します。中断のないマウントトラバーサルを許可するには、エクスポートポリシー「default」にルールを追加してください。

ルール	をクリックし + Add てルールを作成します。 • クライアント仕様：ホスト名、IPアドレス、ネットグループ、またはドメインを指定します。 • Access Protocols：次のオプションを組み合わせて選択します。 ◦ SMB / CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • アクセスの詳細：各タイプのユーザについて、読み取り専用、読み取り/書き込み、またはスーパーユーザのいずれかのアクセスレベルを指定します。ユーザタイプは次のとおりです。 ◦ すべて ◦ all（匿名ユーザとして） ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM ルールを保存します。
デフォルト言語	Storage VMとそのボリュームのデフォルトの言語エンコード設定を指定します。Storage VM内の個々のボリュームの設定を変更する場合はCLIを使用してください。
ネットワークインターフェイス	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。

管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage VM管理用のネットワークインターフェイスを追加するかどうかを指定します。

1. [Enable iSCSI*]を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
ネットワークインターフェイス	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage VM管理用のネットワークインターフェイスを追加するかどうかを指定します。

1. Enable FC（FCの有効化）を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
FCポートを設定	Storage VMに含めるノードのネットワークインターフェイスを選択してください。ノードごとに2つのネットワークインターフェイスを推奨します。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage VM管理用のネットワークインターフェイスを追加するかどうかを指定します。

1. [NVMe/FCを有効にする]*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明

FCポートを設定	Storage VMに含めるノードのネットワークインターフェイスを選択してください。ノードごとに2つのネットワークインターフェイスを推奨します。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage VM管理用のネットワークインターフェイスを追加するかどうかを指定します。

1. [NVMe/TCPを有効にする]*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
ネットワークインターフェイス	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage VM管理用のネットワークインターフェイスを追加するかどうかを指定します。

1. 変更を保存します。

CLI

サブネットを作成するには、ONTAP CLIを使用してください。

手順

1. SVMのルートボリュームを格納するためのアグリゲートを決定します。

   ```
   storage aggregate show -has-mroot false
   ```

   ルートボリュームを格納するための1GB以上の空きスペースがあるアグリゲートを選択する必要があります。SVMでNASの監査を設定する場合は、ルートアグリゲートに少なくとも3GBの追加の空きスペースと、監査を有効にしたときに監査ステージングボリュームの作成に使用される追加のスペースが必要です。

既存のSVMでNASの監査がすでに有効になっている場合は、アグリゲートの作成が完了した直後にアグリゲートのステージングボリュームが作成されます。

2. SVMのルートボリュームを作成するアグリゲートの名前を控えます。
3. SVMを作成するときに言語を指定する予定であり、使用する値がわからない場合は、指定する言語の値を確認し、その値を控えます。

   ```
   vserver create -language ?
   ```

4. SVMを作成するときにSnapshotポリシーを指定する予定であり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用するSnapshotポリシーの名前を確認して、その名前を控えます。

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. SVMを作成するときにクォータポリシーを指定する予定であり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用するクォータポリシーの名前を確認して、その名前を控えます。

   ```
   volume quota policy show -vserver vserver_name
   ```

6. SVMを作成します。

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. SVMの設定が正しいことを確認します。

   ```
   vserver show -vserver vs1
   ```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

この例では、コマンドはIPspace「ipspace1」に「vs1」という名前のSVMを作成します。ルートボリュームは「vs1_root」という名前で、NTFSセキュリティ形式でaggr3に作成されます。

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

論理インターフェイス（LIF）

LIFの概要

ONTAPクラスタのLIF設定の詳細

LIF（論理インターフェイス）は、クラスタ内のノードへのネットワークアクセスポイントを表します。LIFは、クラスタでネットワーク経由の通信の送受信に使用するポートに設定できます。

クラスタ管理者は、LIFを作成、表示、変更、移行、リバート、削除できます。SVM管理者は、SVMに関連付

けられているLIFだけを表示できます。

LIFは、サービスポリシー、ホームポート、ホームノード、フェイルオーバー先のポートのリスト、ファイアウォールポリシーなどの特性が関連付けられているIPアドレスまたはWWPNです。LIFは、クラスタでネットワーク経由の通信の送受信に使用するポートに設定できます。

> ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

LIFは次のポートでホストできます。

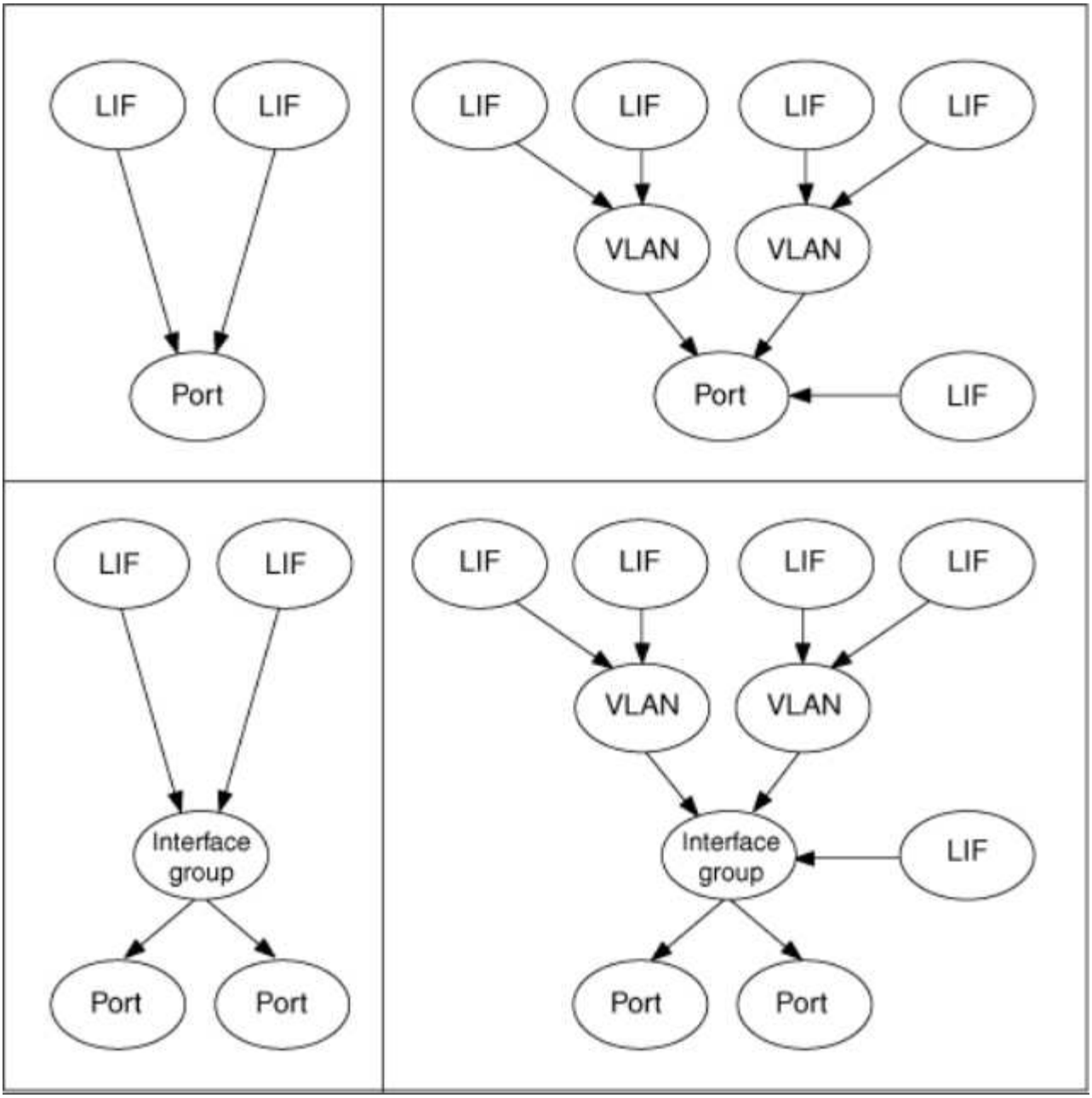
- インターフェイスグループに属していない物理ポート
- インターフェイスグループ
- VLAN
- VLANをホストする物理ポートまたはインターフェイスグループ
- 仮想IP（VIP）ポート

  ONTAP 9 5以降では、VIP LIFがサポートされ、VIPポートでホストされます。

LIFでFCなどのSANプロトコルを設定する際には、WWPNに関連付けられます。

"SAN管理"

次の図に、ONTAPシステムのポート階層を示します。



LIFのフェイルオーバーとギブバック

LIFのフェイルオーバーが発生すると、LIFがホーム ノードまたはポートからHAパートナー ノードまたはポートに移動します。LIFのフェイルオーバーは、物理イーサネット リンクが停止した場合や、ノードがレプリケートされたデータベース（RDB）クォーラムのメンバーでなくなった場合などの特定のイベント時に、ONTAPで自動的にトリガーすることも、クラスタ管理者が手動で開始することもできます。LIFのフェイルオーバーが発生した場合、フェイルオーバーの原因が解決されるまで、ONTAPはパートナー ノードで通常の動作を継続します。ホーム ノードまたはポートの健全性が回復すると、LIFはHAパートナーからホーム ノードまたはポートにリバートされます。このリバートはギブバックと呼ばれます。

LIFのフェイルオーバーとギブバックのためには、各ノードのポートが同じブロードキャスト ドメインに属している必要があります。各ノードの関連するポートが同じブロードキャスト ドメインに属していることを確認するには、以下を参照してください。

- ONTAP 9 .8以降："ポートの到達可能性を修復"

- ONTAP 9 .7以前："ブロードキャストドメインのポートを追加または削除します。"

LIFのフェイルオーバーが（自動または手動で）有効になっているLIFの場合は、次の点に注意してください。

- データサービスポリシーを使用するLIFでは、フェイルオーバーポリシーの制限を確認できます。
  - ONTAP 9 .6以降："ONTAP 9 .6以降のLIFとサービスポリシー"
  - ONTAP 9 .5以前："ONTAP 9 .5以前のLIFのロール"
- LIFの自動リバートは、自動リバートがに設定されていて、LIFのホームポートが正常に機能していてLIFをホストできる場合に実行され `true`ます。
- 計画的または計画外のノードのテイクオーバーでは、テイクオーバーされたノードのLIFがHAパートナーにフェイルオーバーされます。LIFのフェイルオーバー先のポートは、VIF Managerによって決まります。
- フェイルオーバーが完了すると、LIFは正常に動作します。
- 自動リバートがに設定されている場合、ギブバックが開始されると、LIFはホームノードとホームポートにリバート `true`されます。
- 1つ以上のLIFをホストしているポートでイーサネットリンクが停止すると、VIF ManagerはLIFを停止しているポートから同じブロードキャストドメイン内の別のポートに移行します。新しいポートは、同じノードまたはそのHAパートナーに配置できます。リンクがリストアされたあとにauto-revertがに設定されている場合、 `true`VIF ManagerはLIFをそれぞれのホームノードとホームポートにリバートします。
- ノードがレプリケートされたデータベース（RDB）クォーラムのメンバーでなくなると、VIF ManagerはLIFをクォーラムのノードからHAパートナーに移行します。ノードがクォーラムに復帰し、自動リバートがに設定されている場合は `true`、VIF ManagerによってLIFがホームノードとホームポートにリバートされます。

ポートタイプと**ONTAP LIF**の互換性について

LIFにはさまざまな特性を持たせて、さまざまなポートタイプをサポートできます。

クラスタ間LIFと管理LIFが同じサブネットに設定されている場合、管理トラフィックが外部のファイアウォールによってブロックされ、AutoSupport接続とNTP接続が失敗することがあります。コマンドを実行してクラスタ間LIFを切り替えることで、システムをリカバリでき `network interface modify -vserver *vserver name* -lif *intercluster LIF* -status-admin up|down`ます。ただし、この問題を回避するには、インタークラスタLIFと管理LIFを別 々 のサブネットに設定する必要があります。

LIF	説明
Data LIF	Storage Virtual Machine（SVM）に関連付けられたLIFで、クライアントとの通信に使用します。1つのポートに複数のデータLIFを設定できます。これらのインターフェイスは、クラスタ全体で移行またはフェイルオーバーできます。ファイアウォールポリシーをmgmtに変更すると、データLIFをSVM管理LIFとして使用できます。データLIFは、NIS、LDAP、Active Directory、WINS、およびDNSの各サーバに対するセッションで使用されます。

クラスタLIF	クラスタ内のノード間のトラフィックに使用されるLIFです。クラスタLIFは、常にクラスタポートに作成する必要があります。クラスタLIFは、同じノードのクラスタポート間でフェイルオーバーできますが、リモートノードに移行またはフェイルオーバーすることはできません。新しいノードがクラスタに追加されると、IPアドレスが自動的に生成されます。ただし、クラスタLIFにIPアドレスを手動で割り当てる場合は、新しいIPアドレスが既存のクラスタLIFと同じサブネット範囲にあることを確認する必要があります。
クラスタ管理LIF	クラスタ全体に対する単一の管理インターフェイスを提供するLIFです。クラスタ管理LIFは、クラスタ内の任意のノードにフェイルオーバーできます。クラスタポートまたはクラスタ間ポートにはフェイルオーバーできない
クラスタ間LIF	クラスタ間の通信、バックアップ、およびレプリケーションに使用されるLIFです。クラスタピア関係を確立する前に、クラスタ内の各ノードにクラスタ間LIFを作成する必要があります。これらのLIFは、同じノード内のポートにのみフェイルオーバーできます。クラスタ内の別のノードに移行またはフェイルオーバーすることはできません。
ノード管理LIF	クラスタ内の特定のノードを管理するために専用のIPアドレスを提供するLIFです。クラスタの作成時またはクラスタへのノードの追加時に作成されます。これらのLIFは、クラスタからノードにアクセスできなくなった場合など、システムのメンテナンスに使用されます。
VIP LIF	VIP LIFは、VIPポート上に作成された任意のデータLIFです。詳細については、を参照してください"仮想IP（VIP）LIFの設定"。

関連情報

- "network interface modify"

ONTAPのバージョンでサポートされる**LIF**のサービスポリシーとロール

時間の経過とともに、LIFでサポートされるトラフィックのタイプのONTAPによる管理方法が変わりました。

- ONTAP 9 .5以前のリリースでは、LIFのロールとファイアウォールサービスが使用されます。
- ONTAP 9 .6以降のリリースでは、LIFのサービスポリシーを使用します。
  - ONTAP 9 .5リリースで、LIFサービスポリシーが導入されました。
  - ONTAP 9 .6は、LIFのロールをLIFのサービスポリシーに置き換えました。
  - ファイアウォールサービスをONTAP 9のサービスポリシーに置き換えました。

設定する方法は、使用するONTAPのリリースによって異なります。

詳細については、以下を参照してください。

- ファイアウォールポリシーについては、を参照してください"コマンド：firewall-policy-show"。
- LIFのロールについては、を参照し"LIFのロール（ONTAP 9.5以前）"てください。
- LIFサービスポリシーについては、を参照し"LIFとサービスポリシー（ONTAP 9 .6以降）"てください。

ONTAP LIFとサービスポリシーの詳細

LIFのロールやファイアウォールポリシーの代わりに、LIFでサポートされるトラフィックの種類を決定するサービスポリシーをLIFに割り当てることができます。サービスポリシーは、LIFでサポートされる一連のネットワークサービスを定義します。ONTAPには、LIFに関連付けることができる一連の組み込みのサービスポリシーが用意されています。

ONTAP 9.7以前のバージョンでは、ネットワークトラフィックの管理方法が異なります。ONTAP 9.7以前を実行しているネットワークでトラフィックを管理する必要がある場合は、を参照してください"LIFのロール（ONTAP 9.5以前）"。

サービスポリシーとその詳細を表示するには、次のコマンドを使用します。
`network interface service-policy show`

の詳細については `network interface service-policy show`、を"ONTAPコマンド リファレンス"参照してください。

特定のサービスにバインドされていない機能では、システム定義の動作を使用してアウトバウンド接続用のLIFが選択されます。

サービスポリシーが空のLIF上のアプリケーションが予期せず動作することがあります。

システムSVMのサービスポリシー

管理SVMとシステムSVMには、管理LIFやクラスタ間LIFなど、そのSVMのLIFに使用できるサービスポリシーが含まれています。これらのポリシーは、IPspaceの作成時にシステムによって自動的に作成されます。

次の表に、ONTAP 9.12.1以降のシステムSVMのLIFの組み込みのポリシーを示します。それ以外のリリースの場合は、次のコマンドを使用してサービスポリシーとその詳細を表示します。

`network interface service-policy show`

ポリシー	付属サービス	同等のロール	説明
デフォルト - intercluster	インタークラスタコア、管理 - https ： //	クラスタ間	クラスタ間トラフィックを処理する LIF で使用されます。注：サービス intercluster-core は、 net-intercluster サービスポリシーという名前で ONTAP 9.5 から提供されています。
default-route-announce	management-bgp	-	BGP ピア接続を処理する LIF で使用されます。注： ONTAP 9.5 では net-route-announce サービスポリシーという名前で提供されています。

default-management	management-core 、management-https、management-http、management-ssh、management-autosupport、management-ems 、management-dns-client、management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	ノード管理、またはクラスタ管理	システムを対象としたこの管理ポリシーを使用して、システムSVMが所有するノードとクラスタを対象とした管理LIFを作成します。これらのLIFは、DNS、AD 、LDAP、またはNISサーバへのアウトバウンド接続に使用できるだけでなく、システム全体の代わりに実行されるアプリケーションをサポートするための追加の接続にも使用できます。ONTAP 9.12.1以降では、サービスを使用して、監査ログをリモートsyslogサーバに転送するために使用するLIFを制御でき `management-log-forwarding`ます。

次の表に、ONTAP 9.11.1以降のシステムSVMでLIFが使用できるサービスを示します。

サービス	フェイルオーバーの制限	説明
intercluster-core	home-node-only	中核となるクラスタ間サービス
管理コア	-	中核となる管理サービス
management-ssh	-	SSH管理アクセス用のサービス
Management - http ： //	-	HTTP管理アクセス用のサービス
管理 - HTTPS	-	HTTPS管理アクセス用のサービス
management-autosupport	-	AutoSupport ペイロードの送信に関連するサービス
management-bgp	home-port - Only （ホームポートのみ）	BGP ピアのやり取りに関連するサービス
backup-ndmp-control の実行	-	NDMP バックアップ制御のためのサービス
管理 - EMS	-	管理メッセージアクセス用のサービス
management-ntp-client	-	ONTAP 9.10.1で導入されました。NTPクライアントアクセス用のサービス。
management-ntp-server	-	ONTAP 9.10.1で導入されました。NTPサーバ管理アクセス用のサービス

管理 - portmap	-	portmap 管理用のサービス
management-srsh -server です	-	rsh サーバ管理のためのサービス
management-snmp-server	-	SNMP サーバ管理用のサービス
management-telnet-server	-	Telnet サーバ管理用のサービス
管理-ログ転送	-	ONTAP 9.12.1で導入されました。監査ログ転送用のサービス

データ**SVM**のサービス ポリシー

すべてのデータSVMに、そのSVMのLIFで使用できるサービス ポリシーが含まれています。

次の表に、ONTAP 9.11.1以降のデータSVM内のLIFの組み込みのポリシーを示します。それ以外のリリースの場合は、次のコマンドを使用してサービスポリシーとその詳細を表示します。

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

ポリシー	付属サービス	同等のデータプロトコル	説明
default-management	data-core 、management-https、management-http、management-ssh、management-dns-client 、management-ad-client、management-ldap-client 、management-nis-client	なし	このSVMを対象とした管理ポリシーを使用して、データSVMが所有するSVM管理LIFを作成します。これらのLIFを使用して、SVM管理者にSSHまたはHTTPSアクセスを提供できます。必要に応じて、これらのLIFを外部DNS、AD、LDAP、またはNISサーバへのアウトバウンド接続に使用できます。
default-data-blocks（デフォルトデータブロック）	データコア、データ- iSCSI	iSCSI	ブロックベースのSANデータトラフィックを処理するLIFで使用されます。ONTAP 9.10.1以降では、「default-data-blocks」ポリシーは廃止されました。代わりに「default-data-iscsi」サービスポリシーを使用してください。

default-data-files の形式で指定します	data-core、data-fpolicy-client、data-dns-server 、FlexCache data-cifs、data-nfs 、management-dns-client、management-ad-client 、management-ldap-client 、management-nis-client	NFS 、 CIFS 、 fcache	default-data-filesポリシーを使用して、ファイルベースのデータプロトコルをサポートするNAS LIFを作成します。SVM内にLIFが1つしかない場合もあるため、このポリシーでは、LIFを外部のDNS、AD 、LDAP、またはNISサーバへのアウトバウンド接続に使用できるようにします。これらの接続で管理LIFのみを使用する場合は、これらのサービスをこのポリシーから削除できます。
default-data-iscsi	データコア、データ- iSCSI	iSCSI	iSCSIデータトラフィックを処理するLIFで使用されます。
default-data-nvme-tcpです	データコア、データNVMe - TCP	nvme-tcpが表示されます	NVMe/FCデータトラフィックを処理するLIFで使用します。

次の表に、データSVMで使用できる各サービスを、ONTAP 9.11.1以降のLIFのフェイルオーバーポリシーに適用される制限とともに示します。

サービス	フェイルオーバーの制限	説明
management-ssh	-	SSH管理アクセス用のサービス
Management - http ： //	-	ONTAP 9.10.1 Services for HTTP管理アクセスで導入されました
管理 - HTTPS	-	HTTPS管理アクセス用のサービス
管理 - portmap	-	portmap 管理アクセス用のサービス
management-snmp-server	-	SNMPサーバ管理アクセス用のONTAP 9.10.1サービスで導入されました
データコア	-	コアデータサービス
データ- NFS	-	NFSデータサービス
データ- CIFS	-	CIFSデータサービス
Data FlexCache	-	FlexCache データサービス

データ - iSCSI	AFF / FASの場合はホームポートのみ、ASAの場合はSFOパートナーのみ	iSCSI データサービス
backup-ndmp-control の実行	-	ONTAP 9.10.1 Backup NDMPでデータサービスの制御が導入されました
data-dns-server	-	ONTAP 9.10.1で導入されたDNSサーバデータサービス
data-fpolicy-client	-	ファイルスクリーニングポリシーデータサービス
data-nvme-tcp を選択します	home-port - Only （ホームポートのみ）	ONTAP 9.10.1でNVMe TCPデータサービスが導入されました
data-s3-server のように指定します	-	Simple Storage Service （ S3 ）サーバデータサービス

データSVM内のLIFへのサービスポリシーの割り当てについて理解しておく必要があります。

- データサービスのリストを指定してデータSVMを作成すると、指定したサービスを使用して、そのSVMに組み込みの「default-data-files」および「default-data-blocks」サービスポリシーが作成されます。
- データサービスのリストを指定せずにデータSVMを作成すると、そのSVMに組み込みの「default-data-files」サービスポリシーと「default-data-blocks」サービスポリシーが、デフォルトのデータサービスのリストを使用して作成されます。

  デフォルトのデータサービスのリストには、iSCSI、NFS、NVMe、SMB、FlexCacheの各サービスが含まれています。

- データプロトコルのリストを指定してLIFを作成すると、指定したデータプロトコルに相当するサービスポリシーがLIFに割り当てられます。
- 同等のサービスポリシーが存在しない場合は、カスタムサービスポリシーが作成されます。
- サービスポリシーやデータプロトコルのリストを指定せずにLIFを作成した場合、デフォルトでdefault-data-filesサービスポリシーがLIFに割り当てられます。

data-coreサービス

data-coreサービスを使用すると、LIFのロール（ONTAP 9で廃止）ではなくサービスポリシーを使用してLIFを管理するようにアップグレードされたクラスタで、以前にdataロールのLIFを使用していたコンポーネントが想定どおりに動作するようになります。

data-coreをサービスとして指定してもファイアウォールのポートは開かれませんが、データSVMのすべてのサービスポリシーにこのサービスを含める必要があります。たとえば、default-data-filesサービスポリシーには、デフォルトで次のサービスが含まれています。

- データコア
- データ- NFS

- データ- CIFS
- Data FlexCache

data-coreサービスは、LIFを使用するすべてのアプリケーションが想定どおりに動作するようにポリシーに含める必要がありますが、残りの3つのサービスは必要に応じて削除できます。

クライアント側の**LIF**サービス

ONTAP 9 .10.1以降では、ONTAPは複数のアプリケーションに対してクライアント側のLIFサービスを提供します。これらのサービスは、各アプリケーションの代わりにアウトバウンド接続に使用するLIFを制御します。

次の新しいサービスを使用すると、特定のアプリケーションのソースアドレスとして使用するLIFを管理者が制御できます。

サービス	SVM の制限事項	説明
management-ad-client	-	ONTAP 9.11.1以降では、ONTAP は外部ADサーバへのアウトバウンド接続にActive Directoryクライアントサービスを提供します。
management-dns-client	-	ONTAP 9.11.1以降では、ONTAPは外部のDNSサーバへのアウトバウンド接続用にDNSクライアントサービスを提供しています。
管理-LDAPクライアント	-	ONTAP 9.11.1以降では、ONTAPは外部のLDAPサーバへのアウトバウンド接続用にLDAPクライアントサービスを提供しています。
management-nis-client	-	ONTAP 9.11.1以降では、ONTAPは外部のNISサーバへのアウトバウンド接続用にNISクライアントサービスを提供しています。
management-ntp-client	システムのみ	ONTAP 9.10.1以降では、ONTAPは外部のNTPサーバへのアウトバウンド接続用にNTPクライアントサービスを提供しています。
data-fpolicy-client	データ専用	ONTAP 9.8 以降では、 ONTAP はアウトバウンド FPolicy 接続のクライアントサービスを提供します。

新しいサービスはそれぞれ自動的に組み込みのサービスポリシーの一部に含まれますが、管理者はそれらのサービスを組み込みのポリシーから削除したり、カスタムポリシーに追加して、各アプリケーションの代わりにアウトバウンド接続に使用するLIFを制御したりすることができます。

関連情報

- "network interface service-policy showの略"

LIFの管理

ONTAPクラスタのLIFサービスポリシーを設定する

LIFのサービスポリシーを設定して、LIFを使用する単一のサービスまたは一連のサービスを指定できます。

LIFのサービスポリシーを作成します。

LIFのサービスポリシーを作成できます。1つ以上のLIFにサービスポリシーを割り当てることで、1つまたは一連のサービスのトラフィックをLIFで伝送できるようにすることができます。

このコマンドを実行するには、高度なPrivilegesが必要です `network interface service-policy create`。

タスクの内容

データSVMとシステムSVMの両方のデータトラフィックと管理トラフィックの管理に組み込みのサービスとサービスポリシーを使用できます。ほとんどのユースケースでは、カスタムサービスポリシーを作成するのではなく、組み込みのサービスポリシーを使用して問題を解決できます。

これらの組み込みのサービスポリシーは、必要に応じて変更できます。

手順

1. クラスタで使用可能なサービスを表示します。

   ```
   network interface service show
   ```

   サービスとは、LIFがアクセスするアプリケーションと、クラスタが提供するアプリケーションのことです。各サービスには、アプリケーションがリスンしているTCPおよびUDPポートが0個以上含まれています。

   次の追加データサービスと管理サービスを使用できます。

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. クラスタ内のサービスポリシーを表示します。

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. サービスポリシーを作成します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- 「service_name」には、ポリシーに含めるサービスのリストを指定します。
- 「ip_address/mask」には、サービスポリシー内のサービスへのアクセスを許可するアドレスのサブネットマスクのリストを指定します。デフォルトでは、指定されたすべてのサービスが、すべてのサブネットからのトラフィックを許可するデフォルトの許可アドレスリスト0.0.0.0/0で追加されます。デフォルト以外の許可アドレスリストを指定すると、ポリシーを使用するLIFは、指定したマスクのいずれにも一致しないソースアドレスからの要求をすべてブロックするように設定されます。

  次の例は、_nfs_or_SMB_servicesを含むSVM用のデータサービスポリシーsvm1_data_policy__を作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

次の例は、クラスタ間サービスポリシーを作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. サービスポリシーが作成されたことを確認します。

```
cluster1::> network interface service-policy show
```

次の出力は、使用可能なサービスポリシーを示しています。

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

終了後

LIFの作成時または既存のLIFの変更時に、サービスポリシーを割り当てます。

LIFへのサービスポリシーの割り当て

LIFへのサービスポリシーの割り当ては、LIFの作成時または変更時に実行できます。サービスポリシーは、LIFで使用できる一連のサービスを定義します。

タスクの内容

管理SVMとデータSVMのLIFにサービスポリシーを割り当てることができます。

ステップ

サービスポリシーをいつLIFに割り当てるかに応じて、次のいずれかの操作を実行します。

状況	サービスポリシーを割り当てています ...
LIFの作成	network interface create -vserver SVM_name -lif <LIF_name> -home-node <node_name > -home-port <port_name> ｛ （ -address <IP_address> -netmask <IP_address> ） -subnet-name <subnet_name> ｝ -service-policy <service_policy_name>
LIFの変更	network interface modify -vserver <svm_name> -lif <lif_name> -service -policy <service_policy_name>

LIFのサービスポリシーを指定する場合、LIFのデータプロトコルとロールを指定する必要はありません。ロールとデータプロトコルを指定してLIFを作成することもできます。

サービスポリシーは、サービスポリシーの作成時に指定したものと同じSVM内のLIFでのみ使用できます。

例

次の例は、LIFのサービスポリシーをdefault-managementに変更する方法を示しています。

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

LIFのサービスポリシーの管理用コマンド

LIFのサービスポリシーを管理するには、コマンドを使用し `network interface service-policy`ます。

の詳細については `network interface service-policy`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

アクティブなSnapMirror関係にあるLIFのサービスポリシーを変更すると、レプリケーションスケジュールが中断されます。LIFをクラスタ間から非クラスタ間（またはその逆）に変換した場合、変更はピアクラスタにレプリケートされません。LIFサービスポリシーの変更後にピアクラスタを更新するには、最初にこの処理を実行し `snapmirror abort`てレプリケーション関係を再同期するください。

状況	使用するコマンド
サービスポリシーを作成する（advanced権限が必要）	`network interface service-policy create`
既存のサービスポリシーにサービスエントリを追加する（advanced権限が必要）	`network interface service-policy add-service`
既存のサービスポリシーのクローンを作成する（advanced権限が必要）	`network interface service-policy clone`
既存のサービスポリシーのサービスエントリを変更する（advanced権限が必要）	`network interface service-policy modify-service`
既存のサービスポリシーからサービスエントリを削除する（advanced権限が必要）	`network interface service-policy remove-service`
既存のサービスポリシーの名前を変更する（advanced権限が必要）	`network interface service-policy rename`
既存のサービスポリシーを削除する（advanced権限が必要）	`network interface service-policy delete`
組み込みのサービスポリシーを元の状態にリストアする（advanced権限が必要）	`network interface service-policy restore-defaults`
既存のサービスポリシーを表示する	`network interface service-policy show`

関連情報

- "network interface service showの略"
- "network interface service-policy"
- "スナップミラーの中止"

ONTAP LIFの作成

SVMは、1つ以上のネットワーク論理インターフェイス（LIF）を介してクライアントにデータを提供します。データへのアクセスに使用するポートにLIFを作成する必要があります。LIF（ネットワークインターフェイス）は、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

ベストプラクティス

ONTAPに接続されたスイッチポートは、LIFの移行時の遅延を軽減するために、スパニングツリーエッジポートとして設定する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 基盤となる物理または論理ネットワークポートの管理ステータスがupに設定されている必要があります。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。作成するには、System Managerまたはコマンドを使用し `network subnet create`ます。

  の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

- LIFで処理されるトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9 .5以前では、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- NASプロトコルとSANプロトコルを同じLIFに割り当てることはできません。

  サポートされるプロトコルはSMB、NFS、FlexCache、iSCSI、およびFCです。iSCSIおよびFCを他のプロトコルと組み合わせることはできません。ただし、NASプロトコルとイーサネットベースのSANプロトコルは、同じ物理ポート上に存在できます。

  - SMBトラフィックを伝送するLIFを、ホームノードに自動的にリバートするように設定しないでください。この推奨事項は、Hyper-V over SMBまたはSQL Server over SMBでノンストップオペレーションを実現するソリューションをSMBサーバでホストする場合に必須です。
- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- SVMで使用するすべてのネームマッピングサービスとホスト名解決サービス（DNS、NIS、LDAP、Active Directoryなど）が、SVMのデータトラフィックを処理する少なくとも1つのLIFから到達可能でなければなりません。
- クラスタ内のノード間トラフィックを処理するLIFは、管理トラフィックを処理するLIFまたはデータトラフィックを処理するLIFと同じサブネット上には配置できません。
- 有効なフェイルオーバーターゲットのないLIFを作成すると、警告メッセージが表示されます。
- クラスタに多数のLIFがある場合は、クラスタでサポートされるLIFの容量を確認できます。
  - System Manager：ONTAP 9.12.0以降では、ネットワークインターフェイスグリッドのスループットを表示します。
  - CLI：コマンドを使用し、各ノードでサポートされるLIFの容量を `network interface capacity details show`コマンド（advanced権限レベル）で確認し `network interface capacity show`ます。

    および `network interface capacity details show`の詳細については `network interface capacity show`、を"ONTAPコマンド リファレンス"参照してください。

- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、同じサブネットにすでに設定されている他のLIFと同じブロードキャストドメイン内の指定したホームノード上の任意のポートを自動的に選択します。

  ONTAP 9 .4以降では、FC-NVMeがサポートされます。FC-NVMe LIFを作成する場合は、次の点に注意してください。

  - LIFを作成するFCアダプタでNVMeプロトコルがサポートされている必要があります。

◦ データLIFで使用できるデータプロトコルはFC-NVMeのみです。

- SANをサポートするStorage Virtual Machine（SVM）ごとに、管理トラフィックを処理するLIFを1つ設定する必要があります。
- NVMe LIFとネームスペースは同じノードでホストされている必要があります。
- データトラフィックを処理するNVMe LIFは、ノードのSVMごとに最大2つ設定できます。
- サブネットを使用してネットワークインターフェイスを作成すると、選択したサブネットから使用可能なIPアドレスがONTAPによって自動的に選択され、ネットワークインターフェイスに割り当てられます。サブネットが複数ある場合はサブネットを変更できますが、IPアドレスは変更できません。
- ネットワークインターフェイス用にSVMを作成（追加）するときに、既存のサブネットと同じ範囲のIPアドレスを指定することはできません。サブネットの競合エラーが表示されます。この問題は、SVM設定やクラスタ設定でクラスタ間ネットワーク インターフェイスを作成または変更する場合など、ネットワークインターフェイスの他のワークフローでも発生します。
- .10.1以降では、CLIコマンドにONTAP 9 `network interface` over RDMA構成のパラメータが含まれて`-rdma-protocols`います。ONTAP 9.12.1以降では、NFS over RDMA構成用のネットワークインターフェイスの作成がSystem Managerでサポートされています。詳細については、を参照してください NFS over RDMA用にLIFを設定します。
- ONTAP 9 .11.1以降では、オールフラッシュSANアレイ（ASA）プラットフォームでiSCSI LIFの自動フェイルオーバーを使用できます。

  指定したSVMにiSCSI LIFがない場合、または指定したSVMの既存のすべてのiSCSI LIFですでにiSCSI LIFのフェイルオーバーが有効になっている場合は、新しく作成したiSCSI LIFでiSCSI LIFのフェイルオーバーが自動的に有効になります（フェイルオーバーポリシーがに設定され、auto-revertの値がに `true`設定`sfo-partner-only`されます）。

  ONTAP 9 .11.1以降にアップグレードしたあとに、iSCSI LIFのフェイルオーバー機能が有効になっていないSVMに既存の(`disabled`iSCSI LIFがある場合に、同じSVMに新しいiSCSI LIFを作成すると、SVM内の既存のiSCSI LIFのフェイルオーバーポリシーが新しいiSCSI LIFで同じとみなされます）。

  "ASAプラットフォームでのiSCSI LIFフェイルオーバー"

ONTAP 9 .7以降では、ONTAPの同じサブネットにすでにLIFが1つでも存在していれば、LIFのホームポートが自動的に選択されます。ONTAPは、そのサブネット内の他のLIFと同じブロードキャストドメイン内のホームポートを選択します。ホームポートは指定できますが、指定したIPspaceの該当するサブネットにLIFがない場合は必須ではありません。

ONTAP 9 .12.0以降では、使用するインターフェイス（System ManagerまたはCLI）によって実行する手順が異なります。

System Manager

- System Managerを使用して、ネットワークインターフェイスを追加*

手順

1. Network > Overview > Network Interfaces *を選択します。
2. を選択します + Add 。
3. 次のいずれかのインターフェイスロールを選択します。
   a. データ
   b. Intercluster
   c. SVM Management
4. プロトコルを選択します。
   a. SMB/CIFS and NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe / TCP
5. LIFに名前を付けるか、前の選択で生成した名前をそのまま使用します。
6. ホームノードをそのまま使用するか、ドロップダウンを使用して選択します。
7. 選択したSVMのIPspaceで少なくとも1つのサブネットが設定されている場合は、サブネットのドロップダウンが表示されます。
   a. サブネットを選択した場合は、ドロップダウンからサブネットを選択します。
   b. サブネットなしで続行すると、ブロードキャストドメインのドロップダウンが表示されます。
      i. IPアドレスを指定します。IPアドレスが使用中の場合は、警告メッセージが表示されます。
      ii. サブネット マスクを指定します。
8. ホーム ポートをブロードキャスト ドメインから自動で選択するか（推奨）、ドロップダウン メニューから選択します。ホーム ポートのオプションは、ブロードキャスト ドメインとサブネットの選択に基づいて表示されます。
9. ネットワーク インターフェイスを保存します。

CLI

- CLIを使用してLIFを作成してください*

手順

1. LIFに使用するブロードキャストドメインポートを決定します。

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

の詳細については `network port broadcast-domain show`、を"ONTAPコマンド リファレンス"参照してください。

2. LIFに使用するサブネットに未使用のIPアドレスが十分にあることを確認します。

   `network subnet show -ipspace ipspace1`

   の詳細については `network subnet show`、を"ONTAPコマンド リファレンス"参照してください。

3. データへのアクセスに使用するポートに1つ以上のLIFを作成します。

   > NetAppでは、データSVMのすべてのLIFに対してサブネットオブジェクトを作成することを推奨しています。これは特にMetroCluster構成で重要です。各サブネットオブジェクトにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してONTAPがデスティネーションクラスタのフェイルオーバーターゲットを決定できます。手順については、を参照してください"サブネットを作成する"。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

     auto-revertオプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます。

   の詳細については `network interface revert`、を"ONTAPコマンド リファレンス"参照してください。

   - `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
   - オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。

- サブネットを使用してIPアドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときに、ゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
- IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。の詳細については `network route create`、を"ONTAPコマンド リファレンス"参照してください。
- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `true`。
- `-service-policy`ONTAP 9 5以降では、オプションを使用してLIFのサービスポリシーを割り当てることができます `-service-policy`。LIFにサービスポリシーを指定すると、そのポリシーを使用してLIFのデフォルトロール、フェイルオーバーポリシー、およびデータプロトコルのリストが作成されます。.5では、クラスタ間およびONTAP 9ピアサービスでのみサービスポリシーがサポートされます。ONTAP 9 .6では、複数のデータサービスおよび管理サービスのサービスポリシーを作成できます。
- `-data-protocol`FCPまたはNVMe/FCプロトコルをサポートするLIFを作成できます。IP LIFを作成する場合、このオプションは必要ありません。

4. オプション：-addressオプションでIPv6アドレスを割り当てます。

   a. コマンドを使用して `network ndp prefix show`、さまざまなインターフェイスで学習されたRAプレフィックスのリストを表示します。

      コマンドは `network ndp prefix show`、advanced権限レベルで使用できます。

      の詳細については `network ndp prefix show`、を"ONTAPコマンド リファレンス"参照してください。

   b. 形式を使用し `prefix::id`て、IPv6アドレスを手動で作成します。

      `prefix`は、さまざまなインターフェイスで学習されたプレフィックスです。

   を生成するには `id`、ランダムな64ビット16進数を選択します。

5. LIFインターフェイスの設定が正しいことを確認します。

   ```
   network interface show -vserver vs1
   ```

   ```
             Logical    Status     Network          Current   Current Is
   Vserver   Interface  Admin/Oper Address/Mask     Node      Port
   Home
   --------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
              lif1        up/up       10.0.0.128/24   node1      e0d
   true
   ```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

6. フェイルオーバーグループの設定が適切であることを確認します。

   `network interface show -failover -vserver vs1`

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	ネットワークping
IPv6アドレス	network ping6

例

次のコマンドは、LIFを作成し、パラメータと `-netmask`パラメータを使用してIPアドレスとネットワークマスク値を指定し `-address`ます。

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワークマスク値を指定したサブネット（client1_sub）から割り当てます。

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

次のコマンドでは、NVMe/FC LIFを作成してデータプロトコルを指定し `nvme-fc`ます。

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

ONTAP LIFの変更

LIFの属性は変更できます。これには、ホームノードや現在のノード、管理ステータス、IPアドレス、ネットマスク、フェイルオーバーポリシー、ファイアウォールポリシー、サービスポリシーなどがあります。LIFのアドレスファミリーをIPv4からIPv6に変更することもできます。

タスクの内容

- LIFの管理ステータスをdownに変更すると、そのLIFの管理ステータスがupに戻るまで、未処理のNFSv4ロックが維持されます。

  ロックされたファイルに他のLIFがアクセスしようとしたときにロックの競合が発生するのを防ぐには、管理ステータスをdownに設定する前に、NFSv4クライアントを別のLIFに移動する必要があります。

- FC LIFで使用されるデータプロトコルは変更できません。ただし、サービスポリシーに割り当てられているサービスを変更したり、IP LIFに割り当てられているサービスポリシーを変更したりすることはできます。

  FC LIFで使用されるデータプロトコルを変更するには、LIFを削除して再作成する必要があります。IP LIFのサービスポリシーを変更するために、更新中に短時間の停止が発生します。

- ノードを対象とした管理LIFのホームノードと現在のノードは変更できません。
- サブネットを使用してLIFのIPアドレスとネットワークマスク値を変更すると、指定したサブネットからIPアドレスが割り当てられます。LIFの以前のIPアドレスが別のサブネットから割り当てられている場合は、そのIPアドレスがそのサブネットに返されます。
- LIFのアドレスファミリーをIPv4からIPv6に変更するには、IPv6アドレスのコロン表記を使用し、パラメータに新しい値を追加する必要があります `-netmask-length`。
- 自動設定されたリンクローカルIPv6アドレスは変更できません。
- LIFを変更すると、LIFに有効なフェイルオーバーターゲットがなくなるため、警告メッセージが表示されます。

  有効なフェイルオーバーターゲットのないLIFがフェイルオーバーしようとすると、システムが停止する可能性があります。

- ONTAP 9 5以降では、LIFに関連付けられているサービスポリシーを変更できます。
- ONTAP 9 .11.1以降では、All-Flash SAN Array（ASA）プラットフォームでiSCSI LIFの自動フェイルオーバーを使用できます。

  既存のiSCSI LIF（9.11.1以降へのアップグレード前に作成されたLIF）については、フェイルオーバーポリシーをに変更できます"iSCSI LIFの自動フェイルオーバーを有効にする"。

- ONTAP は、ネットワーク タイム プロトコル (NTP) を使用してクラスタ全体の時間を同期します。LIF IP アドレスを変更した後、同期の失敗を防ぐために NTP 設定を更新する必要がある場合があります。詳細については、"NetAppナレッジベース: LIF IP の変更後に NTP 同期が失敗する" 。

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

System Manager

- ONTAP 9.12.0以降では、System Managerを使用してネットワークインターフェイス*を編集できます

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*>[編集]*を選択します ⋮ 。
3. 1つ以上のネットワークインターフェイス設定を変更します。詳細については、を参照してください "LIFの作成"。
4. 変更を保存します。

CLI

- LIFの変更にはCLIを使用してください*

手順

1. コマンドを使用して、LIFの属性を変更します `network interface modify`。

   次の例は、datalif2というLIFのIPアドレスとネットワークマスクを、サブネットclient1_subのIPアドレスとネットワークマスク値を使用して変更する方法を示しています。

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   次の例は、LIFのサービスポリシーを変更する方法を示しています。

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

2. IPアドレスに到達できることを確認します。

使用する機能	使用する方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

   の詳細については `network ping`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP LIFの移行

ポートで障害が発生した場合やメンテナンスが必要な場合は、同じノードの別のポートやクラスタ内の別のノードにLIFを移行しなければならないことがあります。LIFの移行はLIFのフェイルオーバーと似ていますが、LIFの移行は手動操作です。一方、LIFのフェイルオーバーは、LIFの現在のネットワークポートでリンク障害が発生した場合にLIFを自動的に移行する処理です。

開始する前に

- LIFのフェイルオーバーグループを設定しておく必要があります。
- デスティネーションのノードとポートが動作していて、ソースポートと同じネットワークにアクセスできる必要があります。

タスクの内容

- BGP LIFはホームポートに配置され、他のノードやポートに移行することはできません。
- ノードからNICを削除する前に、NICに属しているポートでホストされているLIFをクラスタ内の他のポートに移行する必要があります。
- クラスタLIFを移行するコマンドは、そのクラスタLIFがホストされているノードから実行する必要があります。
- ノードを対象としたLIF（ノードを対象とした管理LIF、クラスタLIF、クラスタ間LIFなど）はリモートノードに移行できません。
- NFSv4のLIFをノード間で移行した場合、そのLIFが新しいポートで使用できるようになるまでに最大45秒かかります。

  この問題を回避するには、遅延が発生しないNFSv4.1を使用します。

- iSCSI LIFは、ONTAP 9 .11.1以降を実行しているオールフラッシュSANアレイ（ASA）プラットフォームで移行できます。

  iSCSI LIFの移行は、ホームノードまたはHAパートナーのポートに限定されます。

- ONTAPバージョン9.11.1以降を実行しているオールフラッシュSANアレイ（ASA）プラットフォームでないプラットフォームでは、ノード間でiSCSI LIFを移行することはできません。

  この制限を回避するには、デスティネーションノードにiSCSI LIFを作成する必要があります。詳細はこちらをご覧ください "iSCSI LIFを作成しています"。

- RDMA経由のNFSのLIF（ネットワークインターフェイス）を移行する場合は、デスティネーションポートがRoCEに対応していることを確認する必要があります。を使用してを移行するには、.10.1以降を実行している必要があります。ONTAP 9を使用して移行するには、ONTAP 9 .12.1を実行している必要があります。System ManagerでRoCE対応のデスティネーションポートを選択したら、* RoCEポートを使用する*の横にあるチェックボックスをオンにして、移行を正常に完了する必要があります。詳細については、をご覧ください "NFS over RDMA用のLIFを設定しています"。
- ソースLIFまたはデスティネーションLIFを移行すると、VMware VAAIのコピーオフロード処理が失敗します。コピーオフロードの詳細：
  - "NFS環境"
  - "SAN環境"

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

System Manager

- System Managerを使用して、ネットワーク・インターフェイス*を移行します

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*> Migrate *を選択します ⋮ 。

   iSCSI LIFの場合、*[インターフェイスの移行]*ダイアログボックスで、HAパートナーのデスティネーションノードとポートを選択します。

   iSCSI LIFを永続的に移行する場合は、チェックボックスを選択します。iSCSI LIFは完全に移行される前にオフラインにする必要があります。また、iSCSI LIFが永続的に移行されたあとは、元に戻すことはできません。リバートオプションはありません。

3. [* Migrate （移行）] をクリックします
4. 変更を保存します。

CLI

- LIFの移行にはCLIを使用してください*

ステップ

特定のLIFを移行するかすべてのLIFを移行するかに応じて、該当する処理を実行します。

移行する項目	入力するコマンド
特定の LIF	`network interface migrate`
ノードのすべてのデータ LIF とクラスタ管理 LIF	`network interface migrate-all`
ポートに接続していないすべての LIF です	`network interface migrate-all -node <node> -port <port>`

次の例は、SVM上の `vs0`というLIFをの `node0b`ポートに `e0d`移行する方法を示してい `datalif1`ます。

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

次の例は、現在の（ローカル）ノードからすべてのデータLIFとクラスタ管理LIFを移行する方法を示しています。

```
network interface migrate-all -node local
```

関連情報

- "ネットワークインターフェイスの移行"

ONTAPノードのフェイルオーバーまたはポート移行後に**LIF**をホームポートにリバートする

別のポートにフェイルオーバーまたは移行されたLIFを、手動または自動でホームポートにリバートできます。特定のLIFのホームポートを使用できない場合、LIFは現在のポートに残り、リバートされません。

タスクの内容

- 自動リバートオプションを設定する前にLIFのホームポートをup状態にした場合、LIFはホームポートに戻りません。
- 「auto-revert」オプションの値をtrueに設定しないかぎり、LIFは自動的にリバートされません。
- LIFをホームポートにリバートするには、「auto-revert」オプションを有効にする必要があります。

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

System Manager

- System Managerを使用して、ネットワークインターフェイスをホームポートに戻します。*

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*> Revert *を選択します ⋮ 。
3. ネットワークインターフェイスをホームポートに戻すには、* Revert *を選択します。

CLI

- CLIを使用してLIFをホームポート*にリバートします

ステップ

LIFをホームポートに手動または自動でリバートします。

ホームポートへの LIF のリバートの方法	入力するコマンド
シユトウ	`network interface revert -vserver vserver_name -lif lif_name`
自動	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

の詳細については `network interface`、を"ONTAPコマンド リファレンス"参照してください。

正しく設定されていない**ONTAP LIF**をリカバリする

クラスタネットワークがスイッチにケーブル接続されているが、Cluster IPspaceに設定されているすべてのポートがCluster IPspaceに設定されている他のポートに到達できな

い場合、クラスタを作成できません。

タスクの内容

スイッチクラスタで、クラスタネットワークインターフェイス（LIF）が間違ったポートに設定されている場合、またはクラスタポートが間違ったネットワークに接続されている場合、 `cluster create`コマンドが次のエラーで失敗することがあります。

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

の詳細については `cluster create`、を"ONTAPコマンド リファレンス"参照してください。

コマンドの結果では `network port show`、クラスタLIFが設定されたポートに接続されているために、複数のポートがクラスタIPspaceに追加されたと表示されることがあります。しかし、 `network port reachability show -detail`コマンドは、どのポートが相互に接続されていないかを明らかにします。

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

クラスタLIFが設定されている他のポートに到達できないポートに設定されたクラスタLIFをリカバリするには、次の手順を実行します。

手順

1. クラスタLIFのホームポートを正しいポートにリセットします。

   ```
   network port modify -home-port
   ```

   の詳細については `network port modify`、を"ONTAPコマンド リファレンス"参照してください。

2. クラスタLIFが設定されていないポートをクラスタブロードキャストドメインから削除します。

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

   の詳細については `network port broadcast-domain remove-ports`、を"ONTAPコマンド リファレンス"参照してください。

3. クラスタを作成します。

   ```
   cluster create
   ```

結果

クラスタの作成が完了すると、正しい設定が検出され、正しいブロードキャストドメインにポートが配置されます。

関連情報

- "network port reachability showの場合"

ONTAP LIF を削除

不要になったネットワークインターフェイス（LIF）は削除できます。

開始する前に

使用中のLIFは削除できません。

手順

1. 次のコマンドを使用して、削除するLIFを「Administratively Down」にマークします。

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. コマンドを使用し `network interface delete`て、1つまたはすべてのLIFを削除します。

削除の対象	入力するコマンド
特定の LIF	`network interface delete -vserver vserver_name -lif lif_name`
すべての LIFs	`network interface delete -vserver vserver_name -lif *`

の詳細については `network interface delete`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、mgmtlif2というLIFを削除します。

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. コマンドを使用し `network interface show`て、LIFが削除されたことを確認します。

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP仮想IP（VIP）LIFの設定

一部の次世代データセンターでは、サブネット間でLIFをフェイルオーバーする必要があるレイヤ3（IP）ネットワークメカニズムが使用されています。ONTAPは、これらの次世代ネットワークのフェイルオーバー要件を満たすために、仮想IP（VIP）データLIFと関連するルーティングプロトコルであるBorder Gateway Protocol（BGP）をサポートしています。

タスクの内容

VIPデータLIFは、どのサブネットにも属さず、同じIPspace内のBGP LIFをホストするすべてのポートから到

達可能なLIFです。VIPデータLIFを使用すると、ホストは個 々 のネットワークインターフェイスに依存しなくなります。複数の物理アダプタがデータトラフィックを伝送するため、すべての負荷が単一のアダプタおよび関連するサブネットに集中することはありません。VIPデータLIFの存在は、ルーティングプロトコルであるBorder Gateway Protocol（BGP）を使用してピアルータにアドバタイズされます。

VIPデータLIFには次の利点があります。

- ブロードキャストドメインやサブネットをまたいで LIF を移動できます。各 VIP データ LIF の現在の場所が BGP を通じてルータに通知されるため、 VIP データ LIF をネットワークのどのサブネットにもフェイルオーバーできます。
- アグリゲートスループット： VIP データ LIF は、同時に複数のサブネットまたはポートに対してデータを送受信できるため、個々のポートの帯域幅を超えるアグリゲートスループットをサポートできます。

Border Gateway Protocol（BGP;ボーダーゲートウェイプロトコル）のセットアップ

VIP LIFを作成する前に、BGPを設定する必要があります。BGPは、VIP LIFの存在をピアルータに通知するためのルーティングプロトコルです。

ONTAP 9 .9.1以降では、BGPピアグループを使用したデフォルトルート自動化がオプションで提供され、設定が簡素化されます。

ONTAPには、BGPピアが同じサブネット上にある場合に、BGPピアをネクストホップルータとして使用してデフォルトルートを学習する簡単な方法があります。この機能を使用するには、属性をに `true`設定し `-use-peer-as-next-hop`ます。デフォルトでは、この属性はです `false`。

静的ルートが設定されている場合でも、自動化されたデフォルトルートよりも静的ルートが優先されます。

開始する前に

設定されたAutonomous System Number（ASN；自律システム番号）のBGP接続をBGP LIFから受け入れるようにピアルータを設定する必要があります。

> ONTAPはルータからの着信ルートアナウンスを処理しません。したがって、クラスタにルートアップデートを送信しないようにピアルータを設定する必要があります。これにより、ピアとの通信が完全に機能するようになるまでの時間が短縮され、ONTAP内の内部メモリ使用量が削減されます。

タスクの内容

BGPをセットアップするには、必要に応じてBGP設定を作成し、BGP LIFを作成し、BGPピアグループを作成します。ONTAPは、最初のBGPピアグループが特定のノードに作成されると、デフォルト値を使用してデフォルトのBGP設定を自動的に作成します。

BGP LIFは、ピアルータとのBGP TCPセッションの確立に使用されます。ピアルータの場合、BGP LIFはVIP LIFに到達するためのネクストホップです。BGP LIFのフェイルオーバーは無効になっています。BGPピアグループは、そのピアグループが使用するIPspace内のすべてのSVMのVIPルートをアドバタイズします。ピアグループで使用されるIPspaceはBGP LIFから継承されます。

セッションを保護するために、ONTAP 9ピアグループでMD5認証がサポートされるようになりました。MD5がイネーブルの場合、BGPセッションは許可されたピア間でのみ確立および処理されるため、許可されていないアクターによるセッションの中断を防ぐことができます。

コマンドと `network bgp peer-group modify`コマンドに次のフィールドが追加されまし `network bgp peer-

group create`た。

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

これらのパラメータを使用すると、セキュリティを強化するためにMD5シグニチャを使用してBGPピアグループを設定できます。MD5認証の使用には、次の要件が適用されます。

- パラメータを指定できるのは、パラメータがに設定されて `true`いる場合 `-md5-enabled`のみ `-md5-secret`です。
- MD5 BGP認証をイネーブルにする前に、IPSecをグローバルにイネーブルにする必要があります。BGP LIFにはアクティブなIPsec設定は必要ありません。を参照してください "IP Security（IPsec）のネットワーク上での暗号化の設定"。
- NetAppでは、ONTAPコントローラでMD5を設定する前に、ルータにMD5を設定することを推奨します。

ONTAP 9 .9.1以降では、次のフィールドが追加されました。

- `-asn`OR `-peer-asn` (4バイトの値)属性自体は新しいものではありませんが、現在は4バイトの整数を使用しています。
- `-med`
- `-use-peer-as-next-hop`

パス優先順位付けのためのMulti-Exit Discriminator（MED）サポートを使用して、高度なルート選択を行うことができます。MEDは、トラフィックに最適なルートを選択するようにルータに指示するBGPアップデートメッセージのオプション属性です。MEDは符号なし32ビット整数（0～4294967295）です。小さい値が推奨されます。

ONTAP 9 .8以降では、次のフィールドがコマンドに追加されてい `network bgp peer-group`ます。

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

これらのBGP属性を使用すると、BGPピアグループのASパス属性およびコミュニティ属性を設定できます。

> ONTAPは上記のBGP属性をサポートしていますが、ルータはこれらの属性を尊重する必要はありません。NetAppでは、ルータでサポートされているアトリビュートを確認し、それに応じてBGPピアグループを設定することを強く推奨します。詳細については、ルータが提供するBGPのマニュアルを参照してください。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. オプション：次のいずれかの操作を実行して、クラスタの BGP 設定を作成するか、デフォルトの BGP 設定を変更します。

a. BGP設定を作成します。

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

- `-routerid`パラメータは、ASドメイン内で一意である必要があるドット付き10進32ビット値を受け入れます。NetAppでは、一意性が保証されるノード管理IP（v4）アドレスを使用することを推奨しています `<router_id>。
- ONTAP BGPは32ビットASN番号をサポートしますが、サポートされるのは標準10進表記のみです。プライベートASNでは4259840001ではなく65000.1などのドット付きASN表記はサポートされません。

2バイトASNのサンプル：

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

4バイトASNのサンプル：

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. デフォルトのBGP設定を変更します。

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>`ASN番号を指定します。.8以降では、ONTAP 9 for BGPは2バイトの非負整数をサポートしています。これは16ビットの数値です（使用可能な値は1～65534です）。.9.1以降では、ONTAP 9 for BGPは4バイトの非負整数（1～4294967295）をサポートしています。デフォルトのASNは65501です。ASN 23456は、4バイトのASN機能を通知しないピアとのONTAPセッション確立用に予約されています。
- `<hold_time>`保持時間を秒単位で指定します。デフォルト値は180sです。

ONTAPでサポートされるグローバル、 <hold_time>、、およびは `<router_id>`1つだけです。これは、 `<asn_number>`複数のIPspaceに対してBGPを設定する場合でも同様です。BGPとすべてのIPルーティング情報は、1つのIPspace内で完全に分離されます。IPspaceは、Virtual Routing and Forwarding（VRF；仮想ルーティング/転送）インスタンスに相当します。

3. システムSVM用のBGP LIFを作成します。

デフォルトIPspaceの場合、SVM名はクラスタ名です。追加のIPspaceの場合、SVM名はIPspace名と同じになります。

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

BGP LIFのサービスポリシー、または「management-bgp」サービスを含む任意のカスタムサービスポリシーを使用できます `default-route-announce`。

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. リモートピアルータとのBGPセッションを確立するために使用するBGPピアグループを作成し、ピアルータにアドバタイズされるVIPルート情報を設定します。

   例 1 ：自動デフォルトルートのないピアグループを作成する

   この場合、管理者はBGPピアへのスタティックルートを作成する必要があります。

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

   例 2 ：自動デフォルトルートを使用してピアグループを作成する

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

例3：MD5を有効にしてピアグループを作成する

a. IPSecを有効にします。

```
security ipsec config modify -is-enabled true
```

b. MD5をイネーブルにしてBGPピアグループを作成します。

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

16進キーを使用した例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657420
```

文字列を使用した例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

BGPピアグループを作成したあと、コマンドを実行すると、仮想イーサネットポート（v0a..v0z、v1a...で始まるポート）が表示され `network port show` ます。このインターフェイスのMTUは常に1500で報告されます。トラフィックに実際に使用されるMTUは、トラフィックが送信されるタイミングで決定される物理ポート（BGP LIF）から取得されます。の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

仮想IP（VIP）データLIFを作成する

VIPデータLIFの存在は、ルーティングプロトコルであるBorder Gateway Protocol（BGP）を使用してピアルータにアドバタイズされます。

開始する前に

- BGPピアグループをセットアップし、LIFを作成するSVMのBGPセッションをアクティブにしておく必要があります。

- SVMの発信VIPトラフィック用に、BGPルータまたはBGP LIFのサブネット内のその他のルータへの静的ルートを作成する必要があります。
- 発信VIPトラフィックが使用可能なすべてのルートを使用できるように、マルチパスルーティングをオンにする必要があります。

  マルチパスルーティングがイネーブルになっていない場合、すべての発信VIPトラフィックは1つのインターフェイスから送信されます。

手順

1. VIPデータLIFを作成します。

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   コマンドでホームポートを指定しない場合は、VIPポートが自動的に選択され `network interface create`ます。

   デフォルトでは、VIPデータLIFは、システムによってIPspaceごとに作成される「vip」という名前のブロードキャストドメインに属します。VIPブロードキャストドメインは変更できません。

   VIPデータLIFは、IPspaceのBGP LIFをホストしているすべてのポートで同時に到達できます。ローカルノードにVIPのSVMに対するアクティブなBGPセッションがない場合、VIPデータLIFは、そのSVMに対してBGPセッションが確立されているノードの次のVIPポートにフェイルオーバーします。

2. VIPデータLIFのSVMに対してBGPセッションのステータスがupになっていることを確認します。

```
network bgp vserver-status show

Node        Vserver  bgp status
        ----------  -------- ---------
        node1       vs1      up
```

   あるノードのSVMのBGPステータスがの場合、 `down`VIPデータLIFは、そのSVMのBGPステータスがupになっている別のノードにフェイルオーバーします。すべてのノードでBGPステータスが設定されている場合は `down`、VIPデータLIFをどこでもホストできず、LIFステータスがdownになります。

BGPの管理用コマンド

5以降では、コマンドを使用してONTAPでONTAP 9 `network bgp`セッションを管理します。

BGP設定を管理します。

状況	使用するコマンド
BGP設定を作成する	`network bgp config create`

BGP設定を変更する	`network bgp config modify`
BGP設定を削除する	`network bgp config delete`
BGP設定を表示する	`network bgp config show`
VIP LIFのSVMに対するBGPステータスを表示する	`network bgp vserver-status show`

BGPのデフォルト値の管理

状況	使用するコマンド
BGPのデフォルト値を変更する	`network bgp defaults modify`
BGPのデフォルト値を表示する	`network bgp defaults show`

BGPピアグループを管理します。

状況	使用するコマンド
BGPピアグループを作成する	`network bgp peer-group create`
BGPピアグループを変更する	`network bgp peer-group modify`
BGPピア グループを削除する	`network bgp peer-group delete`
BGPピア グループの情報を表示する	`network bgp peer-group show`
BGPピア グループの名前を変更する	`network bgp peer-group rename`

MD5を使用した**BGP**ピアグループの管理

ONTAP 9 .16.1以降では、既存のピアグループでMD5認証をイネーブルまたはディセーブルにできます。

既存のBGPピアグループでMD5をイネーブルまたはディセーブルにすると、BGP接続が終了し、MD5設定の変更を適用するために再作成されます。

状況	使用するコマンド
既存のBGPピアグループでMD5をイネーブルにする	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
既存のBGPピアグループでMD5をディセーブルにする	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

関連情報

- "ONTAPコマンド リファレンス"
- "ネットワークBGP"
- "ネットワークインターフェイス"

- "security ipsec config modifyと入力します"

ネットワーク負荷の分散

DNSロードバランシングを使用したONTAPネットワークトラフィックの最適化

負荷が適切に割り当てられたLIFでクライアント要求を処理するようにクラスタを設定できます。その結果、LIFとポートの利用率がバランスよくなるため、クラスタのパフォーマンスが向上します。

DNSロードバランシングを使用すると、負荷が適切なデータLIFを選択し、使用可能なすべてのポート（物理、インターフェイスグループ、VLAN）にユーザネットワークのトラフィックを分散させることができます。

DNSロードバランシングでは、LIFはSVMのロードバランシングゾーンに関連付けられます。サイト規模のDNSサーバは、すべてのDNS要求を転送し、ネットワークトラフィックとポートリソースの可用性（CPU使用率、スループット、開いている接続など）に基づいて最も負荷の低いLIFを返すように設定されています。DNSロードバランシングには次の利点があります。

- 新しいクライアント接続は、使用可能なリソース全体に分散されます。
- 特定のSVMをマウントするときに使用するLIFが手動操作なしで決定されます。
- DNSロードバランシングは、NFSv3、NFSv4、NFSv4.1、SMB 2.0、SMB 2.1、SMB 3.0、S3をサポートしています。

ONTAPネットワークのDNSロードバランシングの詳細

クライアントは、 LIF に関連付けられた IP アドレス、または複数の IP アドレスに関連付けられたホスト名を指定することにより、 SVM をマウントします。デフォルトでは、すべての LIF のワークロードのバランスが取れるように、サイト規模の DNS サーバによってラウンドロビン方式で LIF が選択されます。

ラウンドロビン方式のロードバランシングでは、 LIF のいくつかが過負荷になることがあります。そのため、 SVM でホスト名の解決を取り扱う DNS のロードバランシングゾーンを使用するオプションがあります。DNS ロードバランシングゾーンを使用すると、新しいクライアント接続が使用可能なリソース間でバランスよく配分されるため、クラスタのパフォーマンスが向上します。

DNS ロードバランシングゾーンは、クラスタ内の DNS サーバであり、すべての LIF の負荷を動的に評価して、負荷を適切に割り当てる LIF を返します。ロードバランシングゾーンでは、 DNS が負荷に基づいてそれぞれの LIF に重み（メトリック）を割り当てます。

すべての LIF に、ポートの負荷とホームノードの CPU 利用率に基づいて重みが割り当てられます。DNS クエリでは、負荷が低いポートの LIF から優先的に返されます。重みは手動で割り当てることもできます。

ONTAPネットワーク用のDNSロードバランシングゾーンを作成する

DNSロードバランシングゾーンを作成すると、負荷（LIFにマウントされているクライアント数）に基づいてLIFを動的に選択できます。ロードバランシングゾーンはデータLIFの作成時に作成できます。

開始する前に

サイト規模のDNSサーバ上に、設定したLIFにロードバランシングゾーンに対するすべての要求を転送するDNSフォワーダを設定する必要があります。

その"NetAppナレッジベース: Cluster-Mode で DNS ロードバランシングを設定する方法"条件付き転送を使用した DNS 負荷分散の構成に関する詳細情報が含まれています。

タスクの内容

- どのデータLIFも、DNSロードバランシングゾーン名のDNSクエリに応答できます。
- DNSロードバランシングゾーンの名前はクラスタ内で一意である必要があり、ゾーン名は次の要件を満たしている必要があります。
  - 最大文字数は256文字です。
  - ピリオドを少なくとも1つ含める必要があります。
  - 最初と最後の文字をピリオドなどの特殊文字にすることはできません。
  - 文字間にスペースを使用することはできません。
  - DNS名の各ラベルの最大文字数は63文字です。

    ラベルは、ピリオドの前後のテキストです。たとえば、storage.company.comという名前のDNSゾーンは3つのラベルで構成されています。

ステップ

`network interface create`コマンドでオプションを指定し `dns-zone`て、DNSロードバランシングゾーンを作成します。の詳細については `network interface create`、をlink:https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html["ONTAPコマンド リファレンス"^]参照してください。

ロードバランシングゾーンがすでに存在する場合は、LIFがロードバランシングゾーンに追加されます。

次の例は、LIFの作成時にstorage.company.comという名前のDNSロードバランシングゾーンを作成する方法を示してい `lif1`ます。

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

ロードバランシングゾーンに対するONTAP LIFの追加または削除

仮想マシン（SVM）のDNSロードバランシングゾーンに対してLIFを追加または削除できます。また、すべてのLIFをロードバランシングゾーンから同時に削除することもできます。

開始する前に

- ロードバランシングゾーンのLIFはすべて同じSVMに属している必要があります。
- 1つのLIFが属することができるDNSロードバランシングゾーンは1つだけです。
- LIFが別 々 のサブネットに属している場合は、各サブネットのフェイルオーバーグループが設定されている必要があります。

タスクの内容

管理ステータスがdownのLIFは、一時的にDNSロードバランシングゾーンから削除されます。LIFの管理ステータスがupに戻ると、LIFは自動的にDNSロードバランシングゾーンに追加されます。

ステップ

ロードバランシングゾーンに対してLIFを追加または削除します。

状況	入力するコマンド
LIFを追加する	`network interface modify -vserver vserver_name -lif lif_name -dns-zone zone_name`例： `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`
1 つの LIF を削除する	`network interface modify -vserver vserver_name -lif lif_name -dns-zone none`例： `network interface modify -vserver vs1 -lif data1 -dns-zone none`
すべての LIF を削除します	`network interface modify -vserver vserver_name -lif * -dns-zone none` 例： `network interface modify -vserver vs0 -lif * -dns-zone none`ロードバランシングゾーンからSVMのすべてのLIFを削除することで、そのゾーンからSVMを削除できます。

関連情報

- "network interface modify"

ONTAPネットワーク用のDNSサービスの設定

NFSまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定する必要があります。通常、DNSネーム サーバは、NFSまたはSMBサーバが参加するドメインのActive Directory統合DNSサーバです。

タスクの内容

Active Directory統合DNSサーバには、ドメインLDAPサーバとドメインコントローラサーバのサービスロケーションレコード（SRV）が格納されます。SVMがActive Directory LDAPサーバおよびドメインコントローラを見つけられない場合は、NFSまたはSMBサーバのセットアップに失敗します。

SVMは、ホストに関する情報を検索する際に、hostsネームサービスns-switchデータベースを使用して、使用するネームサービスとその順序を決定します。hostsデータベースでサポートされる2つのネームサービスは、filesとdnsです。

SMBサーバを作成する前に、DNSがソースの1つであることを確認する必要があります。

mgwdプロセスおよびsecdプロセスのDNSネームサービスの統計を表示するには、統計UIを使用します。

手順

1. hostsネームサービスデータベースの現在の設定を確認します。この例では、hostsネームサービスデータベースでデフォルトの設定が使用されています。

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. 必要に応じて、次の操作を実行します。

   a. DNSネーム サービスを希望の順番でhostsネーム サービス データベースに追加するか、ソースの順番を変更します。

      この例では、DNSおよびローカル ファイルをこの順番で使用するようにhostsデータベースを設定しています。

      `vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files`

   b. ネーム サービスの設定が正しいことを確認します。

      `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Name Service Source Order: dns, files
   ```

3. DNSサービスを設定します。

   `vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51`

   vserver services name-service dns createコマンドによって設定が自動検証され、ONTAPがネーム サーバに接続できない場合はエラー メッセージが報告されます。

4. DNSの設定が正しいことと、サービスが有効になっていることを確認します。

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. ネーム サーバのステータスを検証します。

   ```
   vserver services name-service dns check -vserver vs1
   ```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

SVMでの動的**DNS**の設定

Active Directory統合DNSサーバをDNSにあるNFSまたはSMBサーバのDNSレコードに動的に登録する場合は、SVMで動的DNS（DDNS）を設定する必要があります。

開始する前に

SVMでDNSネームサービスが設定されている必要があります。セキュアなDDNSを使用する場合は、Active Directory統合DNSネームサーバを使用し、SVM用にNFSサーバまたはSMBサーバまたはActive Directoryアカウントを作成しておく必要があります。

タスクの内容

完全修飾ドメイン名（FQDN）は一意である必要があります。

完全修飾ドメイン名（FQDN）は一意である必要があります。

- NFSの場合、コマンドで `vserver services name-service dns dynamic-update`に指定した値 `-vserver-fqdn`がLIFに登録されたFQDNになります。
- SMBの場合、CIFSサーバのNetBIOS名およびCIFSサーバの完全修飾ドメイン名として指定した値が、LIFの登録FQDNになります。これはONTAPでは設定できません。次のシナリオでは、LIF FQDNは「CIFS_VS1.EXAMPLE.COM":」です。

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

DDNS更新に関するRFCルールに準拠していないSVM FQDNの設定エラーを回避するには、RFC準拠のFQDN名を使用してください。詳細については、を参照してください "RFC 1123"。

手順

1. SVMでDDNSを設定します。

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   カスタマイズしたFQDNの一部としてアスタリスクを使用することはできません。たとえば、`*.netapp.com`は無効です。

2. DDNSの設定が正しいことを確認します。

   ```
   vserver services name-service dns dynamic-update show
   ```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

ONTAPネットワークの動的DNSサービスの設定

Active Directory統合DNSサーバをDNSにあるNFSまたはSMBサーバのDNSレコードに動的に登録する場合は、SVMで動的DNS（DDNS）を設定する必要があります。

開始する前に

SVMでDNSネームサービスが設定されている必要があります。セキュアなDDNSを使用する場合は、Active Directory統合DNSネームサーバを使用し、SVM用にNFSサーバまたはSMBサーバまたはActive Directoryアカウントを作成しておく必要があります。

タスクの内容

一意の FQDN を指定する必要があります。

DDNS更新に関するRFCルールに準拠していないSVM FQDNの設定エラーを回避するには、RFC準拠のFQDN名を使用してください。

手順

1. SVMでDDNSを設定します。

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   カスタマイズしたFQDNの一部としてアスタリスクを使用することはできません。たとえば、`*.netapp.com`は無効です。

2. DDNSの設定が正しいことを確認します。

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

ホストメイカイケツ

ONTAPネットワークのホスト名解決について

ONTAPは、クライアントにアクセスを提供したりサービスにアクセスしたりするために、ホスト名を数値のIPアドレスに変換できなければなりません。Storage Virtual Machine（SVM）でローカルまたは外部のネームサービスを使用してホスト情報を解決するように設定する必要があります。ONTAPでは、ホスト名を解決するために外部DNSサーバまたはローカルのhostsファイルを設定できます。

外部DNSサーバを使用する場合は、新規または変更されたDNS情報をストレージシステムからDNSサーバに自動的に送信する動的DNS（DDNS）を設定できます。動的DNS更新を使用しない場合、新しいシステムがオンラインになったとき、または既存のDNS情報が変更されたときに、識別されたDNSサーバにDNS情報（DNS名とIPアドレス）を手動で追加する必要があります。このプロセスには時間がかかり、エラーが発生し

やすくなります。ディザスタリカバリ時に手動設定を行うと、長時間のダウンタイムが発生する可能性があります。

ONTAPネットワークのホスト名解決に使用するDNSの設定

ホスト情報を取得するには、DNSを使用してローカルまたはリモートのソースにアクセスします。これらのソースの一方または両方にアクセスするようにDNSを設定する必要があります。

ONTAPがクライアントに適切なアクセスを許可するには、ホスト情報を検索できる必要があります。ネームサービスを設定して、ONTAPがホスト情報を取得するためにローカルまたは外部のDNSサービスにアクセスできるようにする必要があります。

ONTAPでは、UNIXシステムのファイルに相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf`。

外部DNSサーバを使用してホスト名解決用にSVMとデータLIFを設定する

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。

開始する前に

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。 `vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。

タスクの内容

SVMでの動的DNSの設定の詳細については、を参照してください動的DNSサービスの設定。

手順

1. SVMでDNSを有効にします。

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> コマンドは `vserver services name-service dns create`設定の自動検証を実行し、ONTAPがネームサーバに接続できない場合はエラーメッセージを報告します。

2. コマンドを使用して、ネームサーバのステータスを検証し `vserver services name-service dns check`ます。

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

DNSに関連するサービスポリシーの詳細については、を参照してください"ONTAP 9 .6以降のLIFとサービスポリシー"。

ホスト名解決のためのネームサービススイッチテーブルの設定

ONTAPがホスト情報を取得するためにローカルまたは外部のネームサービスにアクセスできるようにするには、ネームサービススイッチテーブルを正しく設定する必要があります。

開始する前に

環境内のホストマッピングに使用するネームサービスを決めておく必要があります。

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. ネームサービススイッチテーブルに想定されるエントリが適切な順序で格納されていることを確認します。

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

例

次の例は、SVM vs1のネームサービススイッチテーブル内のエントリを、ホスト名を解決するためにまずローカルのhostsファイルを使用し、次に外部DNSサーバを使用するように変更します。

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

ONTAP hostsテーブルを管理するONTAPコマンド

クラスタ管理者は、管理Storage Virtual Machine（SVM）のhostsテーブルのホスト名エントリを追加、変更、削除、および表示できます。SVM管理者は、割り当てられたSVMのホスト名エントリのみを設定できます。

ローカルホスト名エントリの管理用コマンド

コマンドを使用して、DNSホストテーブルエントリを作成、変更、または削除できます `vserver services name-service dns hosts`。

DNSホスト名エントリを作成または変更する場合は、複数のエイリアスアドレスをカンマで区切って指定できます。

状況	使用するコマンド
DNS ホスト名エントリを作成します	`vserver services name-service dns hosts create`
DNS ホスト名エントリを変更する	`vserver services name-service dns hosts modify`
DNS ホスト名エントリを削除する	`vserver services name-service dns hosts delete`

コマンドの詳細については `vserver services name-service dns hosts` 、を参照して "ONTAPコマンド リファレンス"ください。

ネットワークのセキュリティを確保

すべての**SSL**接続に**FIPS**を使用した**ONTAP**ネットワークセキュリティの設定

ONTAPは、すべてのSSL接続について、連邦情報処理標準（FIPS）140-2に準拠しています。ONTAPでは、SSL FIPSモードをオンまたはオフにしたり、SSLプロトコルをグローバルに設定したり、RC4などの弱い暗号を無効にしたりできます。

デフォルトでは、ONTAPのSSLはFIPS準拠を無効にし、次のTLSプロトコルを有効にして設定されます。

- TLSv1.3（ONTAP 9.11.1以降）
- TLSv1.2

以前のONTAPリリースでは、次のTLSプロトコルがデフォルトで有効になっていました。

- TLSv1.1（ONTAP 9.12.1以降ではデフォルトで無効）
- TLSv1（ONTAP 9.8以降ではデフォルトで無効）

SSL FIPSモードが有効な場合、ONTAPからONTAPの外部のクライアントまたはサーバコンポーネントへのSSL通信では、SSL用のFIPS準拠の暗号が使用されます。

管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにする場合は、SSL FIPSモードを有効にする前に、ホストキーのアルゴリズムがサポートされていることを確認する必要があります。

*注：ONTAP 9.11.1以降では、ホストキーアルゴリズムのサポートが変更されています。

ONTAP リリース	サポートされているキータイプ	サポートされていないキータイプです
9.11.1以降	ECDSA - sha2 - nistp256	rsa-sha2-512+ rsa-sha2-256+ ssh-ed25519 + ssh-dss+ssh-rsa
9.10.1以前	ECDSA - sha2 -nistp256 + ssh-ed25519	SSH-DSS + ssh-rsa

FIPSを有効にする前に、サポートされているキーアルゴリズムがない既存のSSH公開鍵アカウントをサポートされているキータイプで再設定する必要があります。そうしないと、管理者認証が失敗します。

詳細については、を参照してください "SSH公開鍵アカウントの有効化"。

およびSSL FIPSモードの設定の詳細については、を"ONTAPコマンド リファレンス"参照し `security config modify`てください。

FIPSを有効にする

システムのインストールまたはアップグレードの直後に、すべてのセキュアなユーザがセキュリティ設定を調整することをお勧めします。SSL FIPSモードが有効な場合、ONTAPからONTAPの外部のクライアントまたはサーバコンポーネントへのSSL通信では、SSL用のFIPS準拠の暗号が使用されます。

FIPSが有効な場合、RSAキーの長さが4096の証明書をインストールまたは作成することはできません。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. FIPSを有効にします。

   ```
   security config modify -interface SSL -is-fips-enabled true
   ```

3. 続行するかどうかを尋ねられたら、 `y`
4. ONTAP 9.9.1 以降では、再起動は必要ありません。 ONTAP 9.8 以前を実行している場合は、クラスタ内の各ノードを 1 つずつ手動で再起動します。

例

ONTAP 9 .9.1以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

FIPSの無効化

古いシステム構成を実行していて、ONTAPを下位互換性のある方法で設定したい場合は、FIPSが無効になっている場合にのみSSLv3を有効にできます。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. FIPSを無効にするには、

   ```
   security config modify -interface SSL -is-fips-enabled false
   ```

3. 続行するかどうかを尋ねられたら、と入力し `y`ます。
4. ONTAP 9.9.1 以降では、再起動は必要ありません。ONTAP 9.8以前を実行している場合は、クラスタ内の各ノードを手動でリブートします。

例

ONTAP 9 .9.1以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -interface SSL -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

の詳細については `security config status show`、を"ONTAPコマンド リファレンス"参照してください。

FIPS準拠ステータスの表示

クラスタ全体で現在のセキュリティ設定が実行されているかどうかを確認できます。

手順

1. クラスタ内の各ノードを1つずつリブートします。

   すべてのクラスタノードを同時にリブートしないでください。クラスタ内のすべてのアプリケーションで新しいセキュリティ設定が実行されるようにするには、リブートが必要です。また、FIPSのオン/オフモード、プロトコル、および暗号に対するすべての変更を行うには、リブートが必要です。

2. 現在の準拠ステータスを表示します。

   `security config show`

   ```
   security config show

             Cluster                                                 Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                                !EXP:!eNULL
   ```

   の詳細については `security config show`、を"ONTAPコマンド リファレンス"参照してください。

IPSec転送中暗号化の設定

ONTAPネットワークでIPセキュリティを使用するための準備

ONTAP 9 .8以降では、IPセキュリティ（IPsec）を使用してネットワークトラフィックを保護するオプションが用意されています。IPSecは、ONTAPで使用できる複数の転送中データ暗号化または転送中データ暗号化オプションの1つです。本番環境でIPSecを使用する前に、IPSecを設定する準備をしておく必要があります。

ONTAPでのIPセキュリティの実装

IPsecは、IETFによって維持されているインターネット標準です。IPレベルでネットワークエンドポイント間を流れるトラフィックに対して、データの暗号化と整合性、および認証を提供します。

ONTAPでは、ONTAPとさまざまなクライアント（NFS、SMB、iSCSIプロトコルを含む）の間のすべてのIPトラフィックがIPsecによって保護されます。プライバシーとデータの整合性に加えて、ネットワークトラフィックはリプレイ攻撃や中間者攻撃などのいくつかの攻撃から保護されます。ONTAPでは、IPsecトランスポートモードの実装が使用されます。Internet Key Exchange（IKE;インターネットキーエクスチェンジ）プロトコルバージョン2を利用して、IPv4またはIPv6を使用してONTAPとクライアント間でキーマテリアルをネゴシエートします。

クラスタでIPSec機能を有効にすると、ネットワークでは、ONTAPセキュリティポリシーデータベース（SPD）にさまざまなトラフィック特性に一致するエントリが1つ以上必要になります。これらのエントリは、データの処理と送信に必要な特定の保護の詳細（暗号スイート、認証方式など）にマッピングされます。各クライアントには、対応するSPDエントリも必要です。

トラフィックの種類によっては、別の転送中データ暗号化オプションを使用することをお勧めします。たとえば、NetApp SnapMirrorおよびクラスタピアリングトラフィックの暗号化には、一般に、IPsecではなくTransport Layer Security（TLS）プロトコルが推奨されます。これは、ほとんどの状況でTLSの方がパフォーマンスが向上するためです。

関連情報

- "インターネット技術タスクフォース"
- "RFC 4301：『Security Architecture for the Internet Protocol』"

ONTAP IPsec実装の進化

IPsecはONTAP 9.8で初めて導入されました。以下に説明するように、この実装はその後のONTAPリリースでも進化し続けています。

ONTAP 9.17.1

IPsecハードウェアオフロードのサポートが拡張されました"リンクアグリゲーショングループ" 。"耐量子事前共有鍵（PPK）" IPsec 事前共有キー (PSK) 認証がサポートされています。

ONTAP 9 .16.1

暗号化や整合性チェックなどの暗号化処理のいくつかは、サポートされているNICカードにオフロードできます。詳細については、を参照してください IPSecハードウェアオフロード機能 。

ONTAP 9 12.1

IPSecフロントエンド・ホスト・プロトコルは、MetroCluster IPおよびMetroClusterファブリック接続構成でサポートされます。MetroClusterクラスタで提供されるIPSecのサポートはフロントエンドホストトラフィッ

クに限定され、MetroClusterクラスタ間LIFではサポートされません。

ONTAP 9 10.1

PSK に加えて証明書も IPsec 認証に使用できます。ONTAP 9.10.1より前のバージョンでは、認証でサポートされるのはPSKのみでした。

ONTAP 9 .9.1

IPsecで使用される暗号化アルゴリズムはFIPS 140-2に準拠しています。これらのアルゴリズムは、ONTAPのNetApp暗号モジュールによって処理され、FIPS 140-2の検証が行われます。

ONTAP 9.8

IPsecのサポートは、最初はトランスポートモードの実装に基づいて利用可能になります。

IPSecハードウェアオフロード機能

ONTAP 9.16.1以降を使用している場合は、暗号化や整合性チェックなど、計算負荷の高い特定の処理を、ストレージノードに取り付けられたネットワークインターフェイスコントローラ（NIC）カードにオフロードすることができます。NICカードにオフロードされた処理のスループットは約5%以下です。これにより、IPsecで保護されるネットワークトラフィックのパフォーマンスとスループットが大幅に向上します。

要件と推奨事項

IPsecハードウェアオフロード機能を使用する前に、いくつかの要件を考慮する必要があります。

サポートされるイーサネットカード

サポートされているイーサネットカードのみをインストールして使用してください。ONTAPONTAP以降では、以下のイーサネットカードがサポートされています。

- X50131A（2p、40G/100G/200G/400Gイーサネットコントローラ）
- X60132A（4p、10G / 25Gイーサネットコントローラ）

ONTAP 9.17.1 では、次のイーサネット カードのサポートが追加されました。

- X50135A (2p、40G/100G イーサネット コントローラー)
- X60135A (2p、40G/100G イーサネット コントローラ)

X50131A および X50135A カードは、次のプラットフォームでサポートされています。

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K用
- AFF A90用
- AFF A70用

X60132A および X60135A カードは、次のプラットフォームでサポートされています。

- ASA A50

- ASA A30
- ASA A20
- AFF A50用
- AFF A30用
- AFF A20用

参照"NetApp Hardware Universe"サポートされているプラットフォームとカードの詳細については、こちらをご覧ください。

クラスタスコープ

IPSecハードウェアオフロード機能は、クラスタに対してグローバルに設定されます。たとえば、コマンドは`security ipsec config`クラスタ内のすべてのノードに適用されます。

一貫した構成

サポートされているNICカードがクラスタ内のすべてのノードに取り付けられている必要があります。サポートされているNICカードが一部のノードでしか使用できない場合、オフロードに対応したNICで一部のLIFがホストされていないと、フェイルオーバー後にパフォーマンスが大幅に低下することがあります。

アンチリプレイを無効にする

ONTAP（デフォルト設定）およびIPsecクライアントでは、IPsecアンチリプレイ保護をディセーブルにする必要があります。ディセーブルにしない場合、フラグメンテーションおよびマルチパス（冗長ルート）はサポートされません。

ONTAP IPsecの設定がデフォルトから変更され、アンチリプレイ保護がイネーブルになっている場合は、次のコマンドを使用してディセーブルにします。

```
security ipsec config modify -replay-window 0
```

IPsecアンチリプレイ保護がクライアントでディセーブルになっていることを確認する必要があります。アンチリプレイ保護をディセーブルにするには、クライアントのIPSecマニュアルを参照してください。

制限事項

IPsecハードウェアオフロード機能を使用する前に、いくつかの制限事項を考慮する必要があります。

IPv6

IPsec ハードウェア オフロード機能では IPv6 はサポートされていません。IPv6は、IPsecソフトウェア実装でのみサポートされます。

拡張シーケンス番号

IPSec拡張シーケンス番号は、ハードウェアオフロード機能ではサポートされていません。通常の32ビットシーケンス番号のみが使用されます。

リンクアグリゲーション

ONTAP 9.17.1以降では、IPsecハードウェアオフロード機能を"リンク アグリゲーション グループ" 。

9.17.1より前のバージョンでは、IPsecハードウェアオフロード機能はリンクアグリゲーションをサポートし

ていません。この機能は、 `network port ifgrp` ONTAP CLI でのコマンド。

ONTAP CLIでの設定のサポート

ONTAP 9 .16.1では、次に説明するように、3つの既存のCLIコマンドが更新され、IPSecハードウェアオフロード機能がサポートされています。詳細については、も参照してください"ONTAPでのIPセキュリティの設定"。

ONTAPコマンド	更新
`security ipsec config show`	ブーリアンパラメータは `Offload Enabled`、現在のNICオフロードステータスを示します。
`security ipsec config modify`	パラメータを `is-offload-enabled`使用して、NICオフロード機能を有効または無効にできます。
`security ipsec config show-ipsecsa`	インバウンドおよびアウトバウンドトラフィックをバイトおよびパケット単位で表示するために、4つの新しいカウンタが追加されました。

ONTAP REST APIでの設定のサポート

ONTAP 9 .16.1では、次に説明するように、2つの既存のREST APIエンドポイントが更新され、IPsecハードウェアオフロード機能がサポートされます。

RESTエンドポイント	更新
`/api/security/ipsec`	パラメータ `offload_enabled`が追加され、PATCHメソッドで使用できるようになりました。
`/api/security/ipsec/security_association`	オフロード機能で処理された総バイト数とパケット数を追跡するために、2つの新しいカウンタ値が追加されました。

を含むONTAP REST APIの詳細については、ONTAP自動化に関するドキュメントを参照し "ONTAP REST APIの新機能"てください。の詳細については、ONTAP自動化に関するドキュメントも参照して "IPSecエンドポイント"ください。

関連情報

- "セキュリティ IPsec"

ONTAPネットワークのIPセキュリティの設定

ONTAPクラスタで転送中のIPSec暗号化を設定してアクティブにするには、いくつかのタスクを実行する必要があります。

IPSecを設定する前に、を確認してください"IPセキュリティを使用する準備"。たとえば、ONTAP 9 .16.1以降で使用可能なIPsecハードウェアオフロード機能を使用するかどうかを決定する必要がある場合があります。

クラスタでIPSecを有効にする

クラスタでIPSecを有効にすると、転送中もデータが継続的に暗号化されてセキュアになるようにすることができます。

手順

1. IPsecがすでに有効になっているかどうかを確認します。

   ```
   security ipsec config show
   ```

   結果にが含まれている場合は `IPsec Enabled: false`、次の手順に進みます。

2. IPSecを有効にします。

   ```
   security ipsec config modify -is-enabled true
   ```

   IPSecハードウェアオフロード機能は、ブーリアンパラメータを使用してイネーブルにできます `is-offload-enabled`。

3. 検出コマンドを再度実行します。

   ```
   security ipsec config show
   ```

   結果にが含まれるようになりまし `IPsec Enabled: true`た。

証明書認証を使用した**IPSec**ポリシーの作成の準備

認証に事前共有キー（PSK）のみを使用し、証明書認証を使用しない場合は、この手順を省略できます。

認証に証明書を使用するIPsecポリシーを作成する前に、次の前提条件を満たしていることを確認する必要があります。

- ONTAPとクライアントの両方がエンド エンティティ（ONTAPまたはクライアント）の証明書を検証できるように、両方に相手側のCA証明書がインストールされている。
- ポリシーの対象になるONTAP LIFの証明書がインストールされている。

> ⓘ 証明書はONTAP LIF間で共有できます。証明書とLIFが1対1で対応している必要はありません。

手順

1. 相互認証で使用したすべてのCA証明書（ONTAP側CAとクライアント側CAの両方を含む）をONTAP証明書管理にインストールします（ONTAPの自己署名ルートCAの場合など）。

   サンプルコマンド
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. インストールされているCAが認証時にIPsec CA検索パス内にあることを確認するには、コマンドを使用して、IPsecモジュールにONTAP証明書管理CAを追加し `security ipsec ca-certificate add`ます。

   サンプルコマンド
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. ONTAP LIFで使用する証明書を作成してインストールします。この証明書の発行者CAがONTAPにインス

トールされ、IPsecに追加されている必要があります。

サンプルコマンド

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

ONTAPの証明書の詳細については、ONTAP 9のドキュメントのsecurity certificateコマンドを参照してください。

セキュリティ ポリシー データベース（**SPD**）の定義

IPsecでトラフィックをネットワーク上で転送するためにはSPDエントリが必要です。これは、認証にPSKと証明書のどちらを使用する場合にも当てはまります。

手順

1. コマンドを使用し `security ipsec policy create`て次の処理を行います
   a. ONTAP転送に参加するIPアドレスまたはIPアドレスのサブネットを選択します。
   b. ONTAP IPアドレスに接続するクライアントIPアドレスを選択します。

      クライアントは、事前共有キー（PSK）を使用してInternet Key Exchangeバージョン2（IKEv2）をサポートしている必要があります。

   c. 必要に応じて、トラフィックを保護するための上位層プロトコル（UDP、TCP、ICMPなど）、ローカルポート番号、リモートポート番号などの詳細なトラフィックパラメータを選択します。対応するパラメータは以下のとおりです。 `protocols` 、 `local-ports`そして `remote-ports`それぞれ。

      ONTAP IPアドレスとクライアントIPアドレス間のすべてのトラフィックを保護するには、この手順を省略します。すべてのトラフィックを保護することがデフォルトです。

   d. 目的の認証方式のパラメータにPSKまたは公開キーインフラストラクチャ（PKI）を入力します `auth-method`。
      i. PSKを入力する場合は、パラメータを指定し、<enter>キーを押して事前共有キーの入力と確認を求めるプロンプトを表示します。

         `local-identity`ホストとクライアントの両方でstrongSwanを使用し、ホストまたはクライアントに対してワイルドカードポリシーが選択されていない場合、パラメータと `remote-identity`パラメータはオプションです。

      ii. PKIを入力する場合は、、 `local-identity`、 `remote-identity`パラメータも入力する必要があり`cert-name`ます。リモート側の証明書IDが不明な場合、または複数のクライアントIDが予想される場合は、特別なIDを入力し `ANYTHING`ます。
   e. ONTAP 9.17.1以降では、オプションで量子暗号事前共有キー（PPK）IDを `ppk-identity`パラメータ。PPKは、将来の量子コンピュータ攻撃に対するセキュリティをさらに強化します。PPKIDを入力すると、PPKシークレットの入力を求められます。PPKはPSK認証でのみサポートされています。

詳細はこちら `security ipsec policy create`の中で"ONTAPコマンド リファレンス" 。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAPとクライアントの両方が一致するIPsecポリシーを設定し、認証クレデンシャル（PSKまたは証明書）が両側に配置されるまで、IPトラフィックはクライアントとサーバの間を流れません。

IPsec IDの使用

事前共有キー認証方式では、ホストとクライアントの両方でstrongSwanを使用しており、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、ローカルIDとリモートIDは任意です。

PKI / 証明書を使用する認証方式では、ローカルとリモートの両方のIDが必須です。IDはONTAPとクライアントそれぞれの証明書でどのIDが認定されているかを示すもので、検証プロセスで使用されます。リモートIDが不明な場合、または多数の異なるIDである可能性がある場合は、特別なIDを使用し `ANYTHING`ます。

タスクの内容

ONTAP内では、SPDエントリを変更するか、SPDポリシーの作成時にIDを指定します。SPDには、IPアドレスまたは文字列形式のID名を指定できます。

手順

1. 既存のSPD ID設定を変更するには、次のコマンドを使用します。

```
security ipsec policy modify
```

コマンド例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPSecの複数クライアント設定

IPsecを利用する必要があるクライアントの数が少ない場合は、クライアントごとに1つのSPDエントリを使用すれば十分です。ただし、数百、数千のクライアントがIPsecを利用する必要がある場合は、NetApp IPsecの複数クライアント構成を使用することを推奨します。

タスクの内容

ONTAPでは、IPSecを有効にした状態で、1つのSVM IPアドレスに複数のクライアントを多数のネットワーク経由で接続できます。これには、次のいずれかの方法を使用します。

- * サブネット構成 *

  特定のサブネット（192.168.134.0/24など）のすべてのクライアントが単一のSPDポリシーエントリを使

用して単一のSVM IPアドレスに接続できるようにするには、をサブネット形式で指定する必要があります `remote-ip-subnets`。また、フィールドに正しいクライアント側IDを指定する必要があり`remote-identity`ます。

> サブネット設定で単一のポリシーエントリを使用する場合、そのサブネット内のIPsecクライアントは、IPsec IDと事前共有キー（PSK）を共有します。ただし、これは証明書認証には当てはまりません。証明書を使用する場合は、各クライアントはそれぞれ固有の証明書か共有の証明書のいずれかを認証に使用できます。ONTAPのIPsecは、証明書の有効性をローカルの信頼ストアにインストールされているCAに基づいてチェックします。証明書失効リスト（CRL）のチェックもサポートされています。

- * すべてのクライアント設定を許可 *

  ソースIPアドレスに関係なくすべてのクライアントがSVMのIPsec対応IPアドレスに接続できるようにするには `0.0.0.0/0`、フィールドにワイルドカードを指定し `remote-ip-subnets`ます。

  また、フィールドに正しいクライアント側IDを指定する必要があり `remote-identity`ます。証明書認証の場合は、と入力できます `ANYTHING`。

  また、ワイルドカードを使用する場合は `0.0.0.0/0`、使用する特定のローカルまたはリモートポート番号を設定する必要があります。たとえば、 `NFS port 2049`です。

  手順

  a. 複数のクライアントに対してIPsecを設定するには、次のいずれかのコマンドを使用します。

     i. サブネット設定*を使用して複数のIPsecクライアントをサポートする場合：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     コマンド例

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. [すべてのクライアントの設定を許可する]*を使用して複数のIPsecクライアントをサポートする場合は、次の手順を実行します。

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

  コマンド例

  ```
  security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
  IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
  -identity ontap_side_identity -remote-identity client_side_identity
  ```

IPSec統計を表示します。

ネゴシエーションを使用すると、ONTAP SVMのIPアドレスとクライアントのIPアドレスの間に、IKEセキュリティアソシエーション（SA）と呼ばれるセキュリティチャネルを確立できます。IPsec SAは、実際のデータ暗号化および復号化作業を行うために、両方のエンドポイントにインストールされます。statisticsコマンドを使用して、IPsec SAとIKE SAの両方のステータスを確認できます。

IPSecハードウェアオフロード機能を使用している場合は、コマンドでいくつかの新しいカウンタが表示され `security ipsec config show-ipsecsa`ます。

コマンド例

IKE SAサンプルコマンド：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

ipsec saコマンドおよび出力例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
             Policy Local           Remote
Vserver      Name   Address         Address         Initator-SPI     State
------------ ------ --------------- --------------- ----------------
------------
vs1          test34
                    192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

ipsec saコマンドおよび出力例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
             Policy  Local           Remote          Inbound  Outbound
Vserver      Name    Address         Address         SPI      SPI
State
------------ ------- --------------- --------------- -------- --------
---------
vs1          test34
                     192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

関連情報

- "セキュリティ証明書のインストール"
- "セキュリティ IPsec"

ONTAPネットワーク内のLIFのファイアウォールポリシーを設定する

ファイアウォールを設定すると、クラスタのセキュリティが強化され、ストレージシステムへの不正アクセスを防止できます。デフォルトでは、オンボードファイアウォールは、データLIF、管理LIF、およびクラスタ間LIFに対して特定のIPサービスセットへのリモートアクセスを許可するように設定されています。

ONTAP 9 .10.1以降：

- ファイアウォールポリシーは廃止され、LIFのサービスポリシーに置き換えられました。以前は、オンボードファイアウォールはファイアウォールポリシーを使用して管理されていました。これにはLIFサービスポリシーを使用します。
- ファイアウォールポリシーはすべて空で、基盤となるファイアウォールのポートは開かれません。代わりに、LIFサービスポリシーを使用してすべてのポートを開く必要があります。
- 9.10.1以降にアップグレードしたあとも、ファイアウォールポリシーからLIFのサービスポリシーに移行するための対処は必要ありません。以前のONTAPリリースで使用していたファイアウォールポリシーと整合性のあるLIFのサービスポリシーが自動的に作成されます。カスタムファイアウォールポリシーを作成および管理するスクリプトやその他のツールを使用する場合は、それらのスクリプトをアップグレードしてカスタムサービスポリシーを作成する必要があります。

詳細については、を参照してください"ONTAP 9 .6以降のLIFとサービスポリシー"。

ファイアウォールポリシーを使用して、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、SNMPなどの管理サービスプロトコルへのアクセスを制御できます。NFSやSMBなどのデータプロトコルにファイアウォールポリシーを設定することはできません。

ファイアウォールサービスとポリシーは次の方法で管理できます。

- ファイアウォールサービスの有効化と無効化
- 現在のファイアウォールサービス設定の表示
- ポリシー名とネットワークサービスを指定して新しいファイアウォールポリシーを作成する
- 論理インターフェイスへのファイアウォールポリシーの適用
- 既存のポリシーとまったく同じ新しいファイアウォールポリシーを作成する

  この機能は、同じSVM内で同様の特性を持つポリシーを作成する場合や、別のSVMにポリシーをコピーする場合に使用できます。

- ファイアウォールポリシーに関する情報の表示
- ファイアウォールポリシーで使用されるIPアドレスとネットマスクの変更
- LIFで使用されていないファイアウォールポリシーを削除する

ファイアウォールポリシーとLIF

LIFのファイアウォールポリシーは、各LIFを介したクラスタへのアクセスを制限するために使用されます。デフォルトのファイアウォールポリシーが各タイプのLIFを介したシステムアクセスに与える影響と、ファイアウォールポリシーをカスタマイズしてLIFのセキュリティを増減する方法を理解しておく必要があります。

コマンドまたは `network interface modify`コマンドを使用してLIFを設定する場合、 `network

`interface create`パラメータに指定した値 `-firewall-policy`によって、LIFへのアクセスが許可されるサービスプロトコルとIPアドレスが決まります。の詳細については `network interface`、を"ONTAPコマンド リファレンス"参照してください。

多くの場合、デフォルトのファイアウォールポリシーの値をそのまま使用できます。また、特定のIPアドレスや管理サービスプロトコルへのアクセスを制限しなければならない場合もあります。使用可能な管理サービスプロトコルには、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、およびSNMPがあります。

すべてのクラスタLIFのファイアウォールポリシーはデフォルトで設定さ`""`れており、変更することはできません。

次の表に、LIFの作成時にロール（ONTAP 9 .5以前）またはサービスポリシー（ONTAP 9 .6以降）に応じて各LIFに割り当てられるデフォルトのファイアウォールポリシーを示します。

ファイアウォールポリシー	デフォルトのサービスプロトコル	デフォルトのアクセス	適用先のLIF
管理	dns、http、https、ndmp、ndmps、ntp、snmp、ssh	任意のアドレス（0.0.0.0/0 ）	クラスタ管理 LIF 、 SVM 管理 LIF 、ノード管理 LIF
管理- NFS	dns、http、https、ndmp、ndmps、ntp、portmap、snmp、ssh	任意のアドレス（0.0.0.0/0 ）	SVM 管理アクセスもサポートするデータ LIF
クラスタ間	HTTPS、NDMP、ndmps	任意のアドレス（0.0.0.0/0 ）	すべてのクラスタ間LIF
データ	DNS 、 NDMP 、 ndmps 、 portmap	任意のアドレス（0.0.0.0/0 ）	すべてのデータLIF

portmapサービスの設定

portmapサービスは、RPCサービスをリッスンするポートにマッピングします。

portmapサービスはONTAP 9 .3以前では常にアクセス可能であり、ONTAP 9 .4ではONTAP 9 .6を使用して設定可能になり、ONTAP 9 .7から自動的に管理されるようになりました。

- ONTAP 9 .3以前では、サードパーティ製のファイアウォールではなく組み込みのONTAPファイアウォールを使用するネットワーク構成では、ポート111でportmapサービス（rpcbind）に常にアクセスできました。
- ONTAP 9 .4~lif.6 ONTAP 9では、ファイアウォールポリシーを変更して、portmapサービスへのアクセスを許可するかどうかをLIFごとに制御できます。
- ONTAP 9 .7以降では、portmapファイアウォールサービスは廃止されています。代わりに、NFSサービスをサポートするすべてのLIFに対してportmapポートが自動的に開きます。
- ポートマップサービスは、 ONTAP 9.4 ～ ONTAP 9.6* のファイアウォールで設定可能です

このトピックの残りの部分では、ONTAP 9 .4～ONTAP 9 .6リリースのportmapファイアウォールサービスを設定する方法について説明します。

構成によっては、特定のタイプのLIF（通常は管理LIFとクラスタ間LIF）でサービスへのアクセスを禁止することができます。状況によっては、データLIFへのアクセスを禁止することもできます。

想定される動作

ONTAP 9.4～ONTAP 9.6の動作は、アップグレード時にシームレスに移行できるように設計されています。portmapサービスにすでに特定のタイプのLIFからアクセスしている場合、それらのタイプのLIFからは引き続きサービスにアクセスできます。ONTAP 9.3以前と同様に、ファイアウォール内でアクセスを許可するサービスをLIFのタイプ別のファイアウォール ポリシーで指定できます。

この動作を有効にするには、クラスタ内のすべてのノードでONTAP 9.4～ONTAP 9.6が実行されている必要があります。影響するのはインバウンド トラフィックのみです。

新しいルールは次のとおりです。

- リリース9.4～9.6にアップグレードすると、既存のすべてのファイアウォール ポリシー（デフォルトまたはカスタム）にportmapサービスが追加されます。
- 新しいクラスタやIPspaceを作成した場合、portmapサービスはデフォルトのデータ ポリシーにのみ追加され、デフォルトの管理ポリシーまたはクラスタ間ポリシーには追加されません。
- 必要に応じて、デフォルトまたはカスタムのポリシーにportmapサービスを追加したり削除したりできます。

portmapサービスを追加または削除する方法

SVMまたはクラスタのファイアウォール ポリシーにportmapサービスを追加する（ファイアウォール内でのアクセスを許可する）には、次のように入力します。

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

SVMまたはクラスタのファイアウォール ポリシーからportmapサービスを削除する（ファイアウォール内でのアクセスを禁止する）には、次のように入力します。

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

network interface modifyコマンドを使用して、既存のLIFにファイアウォールポリシーを適用できます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ファイアウォールポリシーを作成して**LIF**に割り当てる

LIFの作成時に、デフォルトのファイアウォールポリシーが各LIFに割り当てられます。多くの場合、ファイアウォールのデフォルト設定をそのまま使用でき、変更する必要はありません。ただし、LIFにアクセスできるネットワーク サービスやIPアドレスを変更したい場合は、カスタム ファイアウォール ポリシーを作成してLIFに割り当てます。

タスクの内容

- `intercluster`、、 `cluster`、またはの `mgmt`名前 `data`でファイアウォールポリシーを作成することはできません `policy`。

  これらの値は、システム定義のファイアウォールポリシー用に予約されています。

- クラスタLIFのファイアウォールポリシーを設定または変更することはできません。

クラスタLIFのファイアウォールポリシーは、すべてのサービスタイプで0.0.0.0/0に設定されます。

- ポリシーからサービスを削除する必要がある場合は、既存のファイアウォールポリシーを削除して新しいポリシーを作成する必要があります。
- クラスタでIPv6が有効になっている場合は、IPv6アドレスを使用してファイアウォールポリシーを作成できます。

  IPv6を有効にすると、 `data`、 `intercluster`および `mgmt`ファイアウォールポリシーの有効なアドレスのリストに::/0というIPv6ワイルドカードが含まれます。

- System Managerを使用してクラスタ全体のデータ保護機能を設定する場合は、許可されるアドレスのリストにクラスタ間LIFのIPアドレスを含め、クラスタ間LIFと会社所有のファイアウォールの両方でHTTPSサービスを許可する必要があります。

  デフォルトでは、ファイアウォールポリシーは `intercluster`すべてのIPアドレス（IPv6の場合は0.0.0.0/0、または：：：/0）からのアクセスを許可し、HTTPS、NDMP、およびNDMPSサービスを有効にします。このデフォルトポリシーを変更する場合、またはインタークラスタLIF用に独自のファイアウォールポリシーを作成する場合は、許可されるリストに各インタークラスタLIFのIPアドレスを追加し、HTTPSサービスを有効にする必要があります。

- ONTAP 9 .6以降では、HTTPSおよびSSHファイアウォールサービスはサポートされていません。

  ONTAP 9 .6では `management-https` `management-ssh`、HTTPSおよびSSH管理アクセスにLIFサービスとLIFサービスを使用できます。

手順

1. 特定のSVMのLIFで使用できるファイアウォールポリシーを作成します。

   ```
   system services firewall policy create -vserver vserver_name -policy
   policy_name -service network_service -allow-list ip_address/mask
   ```

   このコマンドを複数回使用して、ファイアウォールポリシーに複数のネットワークサービスと各サービスで許可されるIPアドレスのリストを追加できます。

2. コマンドを使用して、ポリシーが正しく追加されたことを確認します `system services firewall policy show`。
3. ファイアウォールポリシーをLIFに適用します。

   ```
   network interface modify -vserver vserver_name -lif lif_name -firewall-policy
   policy_name
   ```

4. コマンドを使用して、ポリシーがLIFに正しく追加されたことを確認します `network interface show -fields firewall-policy`。

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ファイアウォールポリシーを作成して**LIF**に割り当てる例

次のコマンドは、10.10サブネットのIPアドレスからのHTTPおよびHTTPSプロトコルによるアクセスを許可するdata_httpというファイアウォールポリシーを作成し、SVM vs1のdata1というLIFに適用してから、クラスタのすべてのファイアウォールポリシーを表示します。

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

ファイアウォールサービスとポリシーを管理するためのONTAPコマンド

ファイアウォールサービスを管理するにはコマンド、ファイアウォールポリシーを管理する `network interface modify`にはコマンド、 `system services firewall policy`LIFのファイアウォール設定を管理するにはコマンドを使用し `system services firewall`ます。

ONTAP 9 .10.1以降：

- ファイアウォールポリシーは廃止され、LIFのサービスポリシーに置き換えられました。以前は、オンボードファイアウォールはファイアウォールポリシーを使用して管理されていました。これにはLIFサービスポリシーを使用します。
- ファイアウォールポリシーはすべて空で、基盤となるファイアウォールのポートは開かれません。代わりに、LIFサービスポリシーを使用してすべてのポートを開く必要があります。
- 9.10.1以降にアップグレードしたあとも、ファイアウォールポリシーからLIFのサービスポリシーに移行するための対処は必要ありません。以前のONTAPリリースで使用していたファイアウォールポリシーと整合性のあるLIFのサービスポリシーが自動的に作成されます。カスタムファイアウォールポリシーを作成および管理するスクリプトやその他のツールを使用する場合は、それらのスクリプトをアップグレードしてカスタムサービスポリシーを作成する必要があります。

詳細については、を参照してください"ONTAP 9 .6以降のLIFとサービスポリシー"。

状況	使用するコマンド
ファイアウォールサービスを有効または無効にする	`system services firewall modify`
ファイアウォールサービスの現在の設定を表示する	`system services firewall show`
ファイアウォールポリシーを作成するか、既存のファイアウォールポリシーにサービスを追加する	`system services firewall policy create`
ファイアウォールポリシーをLIFに適用する	`network interface modify -lif lifname -firewall-policy`
ファイアウォールポリシーに関連付けられているIPアドレスとネットマスクを変更する	`system services firewall policy modify`
ファイアウォールポリシーに関する情報を表示する	`system services firewall policy show`
既存のポリシーとまったく同じ新しいファイアウォールポリシーを作成する	`system services firewall policy clone`
LIFで使用されていないファイアウォールポリシーを削除する	`system services firewall policy delete`

関連情報

- "システムサービスファイアウォール"

- "network interface modify"

QoSマーキング（クラスタ管理者のみ）

ONTAPネットワークQuality of Service（QoS；サービス品質）の詳細

ネットワークサービス品質（QoS）マーキングを使用すると、ネットワークの状態に基づいてさまざまなトラフィックタイプに優先順位を付け、ネットワークリソースを効果的に使用できます。IPspaceあたりのサポートされるトラフィックタイプに応じて、送信IPパケットのDifferentiated Services Code Point（DSCP；DiffServコードポイント）値を設定できます。

UC準拠のためのDSCPマーキング

デフォルトまたはユーザが指定したDSCPコードを使用して、特定のプロトコルの送信IPパケット トラフィックでDifferentiated Services Code Point（DSCP）マーキングを有効にすることができます。DSCPマーキングは、ネットワーク トラフィックを分類して管理するためのメカニズムであり、Unified Capabilities（UC）準拠のコンポーネントです。

DSCP マーキング（ _ QoS マーキング _ または _ サービスマーキングの品質）は、 IPspace 、プロトコル、DSCP の値を指定することで有効になります。DSCPマーキングを適用できるプロトコルは、NFS、SMB 、iSCSI、SnapMirror、NDMP、FTP、HTTP/HTTPS、SSH、Telnet、およびSNMPです。

特定のプロトコルに対してDSCPマーキングをイネーブルにするときにDSCP値を指定しない場合は、デフォルトが使用されます。

- データプロトコル/トラフィックのデフォルト値は0x0A（10）です。
- 制御プロトコル/トラフィックのデフォルト値は0x30（48）です。

ONTAPネットワークのQoSマーキング値を変更します。

IPspace ごとに、さまざまなプロトコルのサービス品質（ QoS ）マーキング値を変更できます。

開始する前に

クラスタ内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。

ステップ

コマンドを使用して、QoSマーキング値を変更します `network qos-marking modify`。

- パラメータは `-ipspace`、QoSマーキングエントリを変更するIPspaceを指定します。
- パラメータは `-protocol`、QoSマーキングエントリを変更するプロトコルを指定します。
- パラメータは `-dscp`、Differentiated Services Code Point（DSCP）値を指定します。指定できる値の範囲は、 0~63 です。
- パラメータは `-is-enabled`、パラメータで指定したIPspace内の指定したプロトコルのQoSマーキングを有効または無効にする場合に使用し `–ipspace`ます。

次のコマンドは、デフォルトの IPspace の NFS プロトコルに対して QoS マーキングを有効にします。

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

次のコマンドは、デフォルトの IPspace の NFS プロトコルに対して DSCP 値を 20 に設定します。

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

プロトコルの詳細と有効な値については、を"ONTAPコマンド リファレンス"参照し `network qos-marking modify`てください。

ONTAPネットワークのQoSマーキング値の表示

IPspace ごとに、さまざまなプロトコルの QoS マーキング値を表示できます。

ステップ

コマンドを使用して、QoSマーキング値を表示します `network qos-marking show`。

次のコマンドは、デフォルトの IPspace のすべてのプロトコルの QoS マーキングを表示します。

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

の詳細については `network qos-marking show`、を"ONTAPコマンド リファレンス"参照してください。

SNMPの管理（クラスタ管理者のみ）

ONTAPネットワーク上のSNMPの詳細

クラスタのSVMを監視するようにSNMPを設定すると、問題を発生前に回避したり、発生時に対応したりすることができます。SNMPを管理するには、SNMPユーザを設定し、すべてのSNMPイベントのSNMPトラップの送信先（管理ワークステーション）を設定する必要があります。データLIFでは、SNMPはデフォルトで無効になっています。

データSVMに、読み取り専用SNMPユーザを作成して管理できます。データLIFは、SVMでSNMP要求を受信するように設定する必要があります。

SNMPネットワーク管理ワークステーションまたはマネージャは、SVM SNMPエージェントに情報を照会できます。SNMPエージェントは情報を収集し、SNMPマネージャに転送します。SNMPエージェントはまた、特定のイベントの発生時にトラップ通知を生成します。SVM上のSNMPエージェントの権限は読み取り専用権限であるため、設定操作や、トラップに応答して対処するために使用することはできません。ONTAPはSNMPバージョンv1、v2c、およびv3と互換性のあるSNMPエージェントを備えています。SNMPv3は、パスフレーズと暗号化を使用して高度なセキュリティを提供します。

ONTAPシステムでのSNMPサポートの詳細については、を参照してください "TR-4220 ：『 SNMP Support in Data ONTAP 』"。

MIBの概要

管理情報ベース（MIB）は、SNMPのオブジェクトとトラップが記述されたテキスト ファイルです。

MIBは、ストレージ システムの管理データの構造を表し、オブジェクト識別子（OID）を含む階層状のネームスペースを使用します。各OIDは、SNMPを使用して読み取り可能な変数を識別します。

MIBは構成ファイルではなく、ONTAPはこれらのファイルを読み取らないため、SNMP機能はMIBによる影響を受けません。ONTAPには次のMIBファイルが用意されています。

- NetAppカスタムMIB(`netapp.mib`)

ONTAPは、IPv4とIPv6の両方のデータを表示するIPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）、およびICMP（RFC 2466）MIBをサポートしています。

ONTAPでは、ファイル内のオブジェクト識別子（OID）とオブジェクトの簡略名の簡単な相互参照も提供されています `traps.dat`。

> ONTAP の MIB および「 traps.dat 」ファイルの最新バージョンは、NetApp Support Siteから入手できます。ただし、サポートサイトにあるファイルのバージョンが、お使いのONTAPバージョンのSNMP機能に必ずしも対応しているとは限りません。これらのファイルは、最新バージョンのONTAPのSNMP機能を評価するのに役立ちます。

SNMPトラツフ

SNMPトラップは、SNMPエージェントからSNMPマネージャに非同期通知として送信されたシステム監視情報をキャプチャします。

SNMPトラップには、標準、ビルトイン、およびユーザ定義の3種類があります。ONTAPでは、ユーザ定義トラップはサポートされていません。

トラップを使用して、MIBで定義されている動作しきい値または障害を定期的にチェックできます。しきい値に達するか障害が検出されると、SNMPエージェントはトラップホストにイベントを警告するメッセージ（トラップ）を送信します。

ONTAPでは、SNMPv1トラップとSNMPv3トラップがサポートされています。ONTAPでは、SNMPv2cトラップおよびINFORMはサポートされていません。

標準**SNMP**トラップ

これらのトラップはRFC 1215で定義されています。ONTAPでサポートされているSNMPトラップは、coldStart、warmStart、linkDown、linkUp、およびauthenticationFailureの5つです。

authenticationFailureトラップはデフォルトでディセーブルになっています。トラップを有効にするには、コマンドを使用する必要があり `system snmp authtrap` ます。の詳細については `system snmp authtrap`、を"ONTAPコマンド リファレンス"参照してください。

ビルトイン**SNMP**トラップ

ビルトイントラップはONTAPで事前定義されており、イベントが発生するとトラップホストリストのネットワーク管理ステーションに自動的に送信されます。diskFailedShutdown、cpuTooBusy、volumeNearlyFullなどのトラップは、カスタムMIBで定義されています。

各ビルトイントラップは、一意のトラップコードによって識別されます。

ONTAPネットワーク用のSNMPコミュニティの作成

SNMPv1およびSNMPv2cを使用する場合に、管理ステーションとStorage Virtual Machine（SVM）間の認証メカニズムとして機能するSNMPコミュニティを作成できます。

データSVMにSNMPコミュニティを作成することで、データLIFでや `snmpget`などのコマンドを実行でき `snmpwalk`ます。

タスクの内容

- ONTAPの新規インストールでは、SNMPv1とSNMPv2cはデフォルトで無効になっています。

  SNMPv1とSNMPv2cは、SNMPコミュニティを作成すると有効になります。

- ONTAPでは、読み取り専用コミュニティがサポートされます。
- デフォルトでは、データLIFに割り当てられている「data」ファイアウォールポリシーでは、SNMPサービスがに設定されて `deny`います。

  データSVMのSNMPユーザを作成するときに、新しいファイアウォールポリシーを作成してSNMPサービスをに設定する必要があります `allow`。

ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- 管理 SVM とデータ SVM の両方に、 SNMPv1 ユーザと SNMPv2c ユーザの SNMP コミュニティを作成できます。
- SVMはSNMP標準の一部ではないため、データLIFでのクエリにはNetAppのルートOID（1.3.6.1.4.1.789）を含める必要があります（例：） `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

手順

1. コマンドを使用して、SNMPコミュニティを作成し `system snmp community add`ます。次のコマンドは、管理 SVM cluster-1 に SNMP コミュニティを作成する方法を示しています。

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

次のコマンドは、データ SVM vs1 に SNMP コミュニティを作成する方法を示しています。

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. system snmp community showコマンドを使用して、コミュニティが作成されたことを確認します。

次のコマンドは、SNMPv1およびSNMPv2c用に作成された2つのコミュニティを表示します。

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. コマンドを使用して、「data」ファイアウォールポリシーでSNMPがサービスとして許可されているかどうかを確認します `system services firewall policy` show。

次のコマンドは、デフォルトの「data」ファイアウォールポリシーではsnmpサービスが許可されていないことを示しています（snmpサービスは「mgmt」ファイアウォールポリシーでのみ許可されています）。

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. コマンドを使用して、サービス `system services firewall policy create`によるアクセスを許可する新しいファイアウォールポリシーを作成し `snmp`ます。

   次のコマンドは、「data1」という名前の新しいデータファイアウォールポリシーを作成し、 `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. コマンドで-firewall-policyパラメータを指定して、ファイアウォールポリシーをデータLIFに適用し `network interface modify`ます。

次のコマンドは、新しい「data1」ファイアウォールポリシーをLIF「datalif1」に割り当てます。

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPクラスタでのSNMPv3ユーザの設定

SNMPv3は、SNMPv1やSNMPv2cに比べてセキュアなプロトコルです。SNMPv3を使用するには、SNMPマネージャからSNMPユーティリティを実行するようにSNMPv3ユーザを設定する必要があります。

ステップ

使用 `security login create` SNMPv3 ユーザーを作成するコマンド。

次の情報を入力するように求められます。

- エンジン ID ：デフォルトで、推奨値はローカルエンジン ID です
- 認証プロトコル
- 認証パスワード
- プライバシー プロトコル
- プライバシー プロトコルのパスワード

結果

SNMPv3ユーザは、ユーザ名とパスワードを使用してSNMPマネージャからログインし、SNMPユーティリティコマンドを実行できます。

SNMPv3セキュリティパラメータ

SNMPv3には認証機能が含まれています。この機能を選択すると、コマンドを呼び出すときに、ユーザの名前、認証プロトコル、認証キー、および必要なセキュリティレベルの入力が必要になります。

次の表に、SNMPv3セキュリティパラメータを示します。

パラメータ	コマンドラインオプション	説明
エンジン ID	-e engineID	SNMP エージェントのエンジン ID 。デフォルト値はlocal engineIDです（推奨）。
securityName の略	-u 名	ユーザ名は 32 文字以内にする必要があります。
authProtocol の略	• a ｛ none	md5

sha	SHA-256 }	認証タイプには、 none 、 md5 、 SHA 、または SHA-256 を指定できます。
authKey	• パスフレーズ	8 文字以上の長さのパスフレーズ
セキュリティレベル	-l ｛ authNoPriv	AuthPriv
noAuthNoPriv }	セキュリティレベルには、「 Authentication 、 No Privacy 」、「 Authentication 、 Privacy 」、「 No Authentication 、 No Authentication 」のいずれかを指定できます。 プライバシーなし。	privProtocol の略
-x ｛ none	des	aes128 }
プライバシープロトコルには、 none 、 des 、または aes128 を指定できます	プライベートパスワード	-X パスワード

さまざまなセキュリティレベルの例

次の例は、さまざまなセキュリティレベルで作成したSNMPv3ユーザが、SNMPクライアント側のコマンド（など）を使用してクラスタオブジェクトを照会する方法を示してい `snmpwalk`ます。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

認証プロトコルがSHAの場合は、5.3.1以降を使用する必要があります `snmpwalk`。

セキュリティレベル：**authPriv**

authPrivセキュリティレベルのSNMPv3ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPSモード

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalkテスト

このSNMPv3ユーザがsnmpwalkコマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティレベル：**authNoPriv**

authNoPrivセキュリティレベルのSNMPv3ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPSモード

FIPSでは、プライバシープロトコルに* none *を選択することはできません。そのため、authNoPriv SNMPv3ユーザをFIPSモードで設定することはできません。

snmpwalkテスト

このSNMPv3ユーザがsnmpwalkコマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティレベル：**noAuthNoPriv**

noAuthNoPrivセキュリティレベルのSNMPv3ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPSモード

FIPSでは、プライバシープロトコルに* none *を選択することはできません。

snmpwalkテスト

このSNMPv3ユーザがsnmpwalkコマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークでSNMPのトラップホストを設定する

クラスタで SNMP トラップが生成されたときに通知（ SNMP トラップ PDU ）を受信するトラップホスト（ SNMP マネージャ）を設定できます。SNMP トラップホストのホスト名または IP アドレス（ IPv4 または IPv6 ）を指定できます。

開始する前に

- クラスタでSNMPとSNMPトラップが有効になっている必要があります。

> SNMPおよびSNMPトラップはデフォルトで有効になっています。

- クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。
- IPv6 アドレスを使用して SNMP トラップホストを設定するには、クラスタで IPv6 を有効にする必要があります。
- トラップホストの作成時に、事前定義されたユーザベースのセキュリティモデル（USM）の認証とプライバシーのクレデンシャルを指定しておく必要があります。

ステップ

SNMPトラップホストを追加します。

```
system snmp traphost add
```

> トラップを送信できるのは、少なくとも 1 つの SNMP 管理ステーションがトラップホストとして指定されているときのみです。

次のコマンドは、 yyy.example.com という新しい SNMPv3 トラップホストを既知の USM ユーザとともに追加します。

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

次のコマンドは、トラップホストの IPv6 アドレスを指定して、そのホストを追加します。

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

ONTAPクラスタでのSNMPポーリングの確認

SNMP を設定したら、クラスタをポーリングできることを確認する必要があります。

タスクの内容

クラスタをポーリングするには、などのサードパーティのコマンドを使用する必要があり `snmpwalk`ます。

手順

1. SNMP コマンドを送信して、別のクラスタからクラスタをポーリングします。

   SNMPv1を実行しているシステムでは、CLIコマンドを使用し `snmpwalk -v version -c community_stringip_address_or_host_name system`てMIB（管理情報ベース）の内容を検出します。

   この例では、ポーリングするクラスタ管理 LIF の IP アドレスは 10.11.12.123 です。要求された MIB 情報が表示されます。

   ```
   C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

   SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
              Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
   SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
   19:47:24.48
   SNMPv1-MIB::sysContact.0 = STRING:
   SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
   SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
   SNMPv1-MIB::sysServices.0 = INTEGER: 72
   ```

   SNMPv2cを実行しているシステムでは、CLIコマンドを使用し `snmpwalk -v version -c community_stringip_address_or_host_name system`てMIB（管理情報ベース）の内容を検出します。

   この例では、ポーリングするクラスタ管理 LIF の IP アドレスは 10.11.12.123 です。要求された MIB 情報が表示されます。

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

SNMPv3を実行しているシステムでは、CLIコマンドを使用し `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system`てMIB（管理情報ベース）の内容を検出します。

この例では、ポーリングするクラスタ管理 LIF の IP アドレスは 10.11.12.123 です。要求された MIB 情報が表示されます。

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

SNMP、トラップ、およびトラップホストを管理するためのONTAPコマンド

SNMP、トラップ、およびトラップホストを管理するには、コマンドを使用し `system snmp`ます。SVMのSNMPユーザを管理するには、コマンドを使用し `security`ます。SNMPトラップに関連するイベントを管理するには、コマンドを使用し `event`ます。

SNMPの設定用コマンド

状況	使用するコマンド

クラスタでSNMPを有効にする	`options -option-name snmp.enable -option-value on` 管理（mgmt）ファイアウォールポリシーでSNMPサービスが許可されている必要があります。SNMPが許可されているかどうかを確認するには、system services firewall policy showコマンドを使用します。
クラスタでSNMPを無効にする	`options -option-name snmp.enable -option-value off`

SNMP v1、**v2c**、および**v3**ユーザを管理するコマンド

状況	使用するコマンド
SNMPユーザの設定	`security login create`
SNMP ユーザを表示します	`security snmpusers and security login show -application snmp`
SNMP ユーザを削除する	`security login delete`
SNMPユーザのログイン方法のアクセス制御ロール名を変更する	`security login modify`

連絡先と場所の情報を提供するコマンド

状況	使用するコマンド
クラスタの連絡先の詳細を表示または変更する	`system snmp contact`
クラスタの場所の詳細を表示または変更する	`system snmp location`

SNMPコミュニティの管理用コマンド

状況	使用するコマンド
1 つの SVM 、またはクラスタのすべての SVM に読み取り専用（ ro ）コミュニティを追加する	`system snmp community add`
1 つまたはすべてのコミュニティを削除します	`system snmp community delete`
すべてのコミュニティのリストを表示します。	`system snmp community show`

SVMはSNMP標準の一部ではないため、データLIFでのクエリにはNetAppのルートOID（1.3.6.1.4.1.789）を

含める必要があります。たとえば、のように指定します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`

SNMPオプション値を表示するコマンド

状況	使用するコマンド
クラスタの連絡先、連絡先の場所、クラスタがトラップを送信するように設定されているかどうか、トラップホストのリスト、コミュニティのリスト、アクセス制御の種類など、すべてのSNMPオプションの現在の値を表示する	`system snmp show`

SNMPトラップおよびトラップホストの管理用コマンド

状況	使用するコマンド
クラスタから送信されるSNMPトラップを有効にする	`system snmp init -init 1`
クラスタからのSNMPトラップの送信を無効にする	`system snmp init -init 0`
クラスタ内の特定のイベントに関するSNMP通知を受信するトラップホストを追加する	`system snmp traphost add`
トラップホストを削除する	`system snmp traphost delete`
トラップホストのリストを表示します。	`system snmp traphost show`

SNMPトラップに関連するイベントの管理用コマンド

状況	使用するコマンド
SNMP トラップ（ビルトイン）が生成されたイベントを表示します	`event route show` SNMP関連のイベントのみを表示するには、パラメータを使用し `-snmp-support true`ます。 パラメータを使用して `instance -messagename <message>`、イベントが発生した理由と対処方法の詳細を表示します。 個 々 のSNMPトラップイベントを特定の送信先トラップホストにルーティングすることはできません。すべてのSNMPトラップイベントがすべての送信先トラップホストに送信されます。
SNMP トラップ履歴レコードのリストを表示します。 SNMP トラップに送信されたイベント通知です	`event snmphistory show`

SNMP トラップ履歴レコードを削除します	`event snmphistory delete`

関連情報

- "システムSNMP"
- "security snmpusersを指定します"
- "セキュリティ"
- "イベント"
- "セキュリティログイン"

SVMのルーティングを管理します。

ONTAPネットワークでのSVMルーティングの詳細

SVMのルーティング テーブルは、SVMがデスティネーションとの通信に使用するネットワーク パスを決めるものです。ネットワークの問題を未然に防ぐためには、ルーティング テーブルの仕組みを理解しておくことが重要です。

ルーティング ルールは次のとおりです。

- ONTAPは、最も限定的かつ使用可能なルートでトラフィックをルーティングします。
- より限定的なルートがない場合、最後の手段としてデフォルト ゲートウェイ ルート（0ビットのネットマスク）でトラフィックがルーティングされます。

デスティネーション、ネットマスク、メトリックが同じでルートが複数ある場合、リブート後またはアップグレード後に同じルートが使用される保証はありません。複数のデフォルト ルートを設定している場合は、この点が特に問題となります。

SVMにはデフォルト ルートを1つだけ設定することを推奨します。システム停止を回避するには、より限定的なルートでは到達できないネットワーク アドレスにもデフォルト ルートが到達できることを確認する必要があります。詳細については、"NetAppナレッジベース: SU134 - クラスタ化されたONTAPでのルーティング構成が正しくないため、ネットワーク アクセスが中断される可能性があります"

ONTAPネットワークの静的ルートを作成する

Storage Virtual Machine（SVM）内で静的ルートを作成して、LIFが発信トラフィックをネットワークでどのように使用するかを制御できます。

SVMに関連付けられたルートエントリを作成すると、そのルートが、ゲートウェイと同じサブネットにあり、指定したSVMに所有されているすべてのLIFで使用されます。

ステップ

コマンドを使用し `network route create`てルートを作成します。

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

の詳細については `network route create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークのマルチパスルーティングを有効にする

複数のルートが1つの宛先に対して同じメトリックを持つ場合、発信トラフィック用に選択されるルートは1つだけです。これにより、発信トラフィックの送信に他のルートが使用されなくなります。マルチパスルーティングをイネーブルにすると、使用可能なすべてのルートをメトリックに応じてロードバランシングできます。ECMPルーティングでは、同じメトリックの使用可能なルート間でロードバランシングが行われます。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. マルチパスルーティングを有効にします。

   ```
   network options multipath-routing modify -is-enabled true
   ```

   クラスタ内のすべてのノードでマルチパスルーティングが有効になっている。

   ```
   network options multipath-routing modify -is-enabled true
   ```

   の詳細については `network options multipath-routing modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークから静的ルートを削除する

不要な静的ルートをStorage Virtual Machine（SVM）から削除できます。

ステップ

コマンドを使用し `network route delete`て、静的ルートを削除します。

次の例は、SVM vs0に関連付けられている、ゲートウェイ10.63.0.1、デスティネーションIPアドレス0.0.0.0/0の静的ルートを削除します。

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

の詳細については `network route delete`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPルーティング情報の表示

クラスタの各 SVM のルーティング設定に関する情報を表示することができます。この情報は、クライアントアプリケーションまたはサービスとクラスタ内のノード上の LIF との接続に関連するルーティングの問題を診断するのに役立ちます。

手順

1. コマンドを使用し `network route show`て、1つ以上のSVM内のルートを表示します。次の例は、 vs0 という SVM に設定されているルートを表示しています。

```
network route show
  (network route show)
Vserver              Destination     Gateway         Metric
-------------------- --------------- --------------- ------
vs0
                     0.0.0.0/0       172.17.178.1    20
```

2. コマンドを使用し `network route show-lifs`て、1つ以上のSVM内のルートとLIFの関連付けを表示します。

   次の例は、 vs0 という SVM が所有しているルートと LIF の関連付けを表示しています。

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   および `network route show-lifs`の詳細については `network route show`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドを使用して `network route active-entry show`、1つ以上のノード、SVM、サブネットに設定されているルート、または指定したデスティネーションに一致するルートを表示します。

   次の例は、特定の SVM に設定されているすべてのルートを表示しています。

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
```

```
---------------------  -------------------  ---------  ------  -----
127.0.0.1              127.0.0.1            lo             10  UHS
127.0.10.1             127.0.20.1           losk           10  UHS
127.0.20.1             127.0.20.1           losk           10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination            Gateway              Interface   Metric  Flags
---------------------  -------------------  ---------  ------  -----
default                fd20:8b1e:b255:814e::1
                                            e0d            20  UGS
fd20:8b1e:b255:814e::/64
                       link#4               e0d             0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination            Gateway              Interface   Metric  Flags
---------------------  -------------------  ---------  ------  -----
127.0.0.1              127.0.0.1            lo             10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination            Gateway              Interface   Metric  Flags
---------------------  -------------------  ---------  ------  -----
127.0.10.1             127.0.20.1           losk           10  UHS
127.0.20.1             127.0.20.1           losk           10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination            Gateway              Interface   Metric  Flags
---------------------  -------------------  ---------  ------  -----
default                fd20:8b1e:b255:814e::1
                                            e0d            20  UGS
fd20:8b1e:b255:814e::/64
                       link#4               e0d             0  UC
fd20:8b1e:b255:814e::1 link#4               e0d             0  UHL
11 entries were displayed.
```

の詳細については `network route active-entry show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークのルーティングテーブルから動的ルートを削除する

IPv4 と IPv6 の ICMP リダイレクトを受信すると、動的ルートがルーティングテーブルに追加されます。デフォルトでは、ダイナミックルートは300秒後に削除されます。動的ルートを維持する時間を変更する場合は、タイムアウト値を変更できます。

タスクの内容

0~65 、 535 秒のタイムアウト値を設定できます。値を 0 に設定すると、ルートは無期限になります。動的ルートを削除すると、無効なルートの永続性が原因で接続が切断されるのを防ぐことができます。

手順

1. 現在のタイムアウト値を表示します。
   - IPv4の場合：

     ```
     network tuning icmp show
     ```

   - IPv6の場合：

     ```
     network tuning icmp6 show
     ```

2. タイムアウト値を変更します。
   - IPv4の場合：

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - IPv6の場合：

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. タイムアウト値が正しく変更されたことを確認します。
   - IPv4の場合：

     ```
     network tuning icmp show
     ```

   - IPv6の場合：

     ```
     network tuning icmp6 show
     ```

の詳細については `network tuning icmp`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワーク情報

ONTAPネットワーク情報の表示

CLIを使用して、ポート、LIF、ルート、フェイルオーバールール、フェイルオーバーグループ、ファイアウォールルール、DNS、NIS、および接続に関する情報を表示できます。ONTAP 9 .8以降では、ネットワークについてSystem Managerに表示されるデータもダウンロードできます。

この情報は、ネットワーク設定の再設定時やクラスタのトラブルシューティング時に役立ちます。

クラスタ管理者は、ネットワーク情報をすべて表示できます。SVM管理者は、割り当てられているSVMに関する情報のみを表示できます。

System Managerの_リスト表示_に情報を表示するときに*[ダウンロード]*をクリックすると、表示されているオブジェクトのリストがダウンロードされます。

- このリストは、カンマ区切り値（ CSV ）形式でダウンロードされます。
- 表示されている列のデータのみがダウンロードされます。
- CSV ファイル名は、オブジェクト名とタイムスタンプでフォーマットされます。

ONTAPのネットワークポート情報の表示

クラスタ内の特定のポート、またはすべてのノードのすべてのポートに関する情報を表示できます。

タスクの内容

次の情報が表示されます。

- ノード名
- ポート名
- IPspaceメイ
- ブロードキャストドメイン名
- リンクステータス（upまたはdown）
- MTUの設定
- ポート速度の設定と動作ステータス（1ギガビットまたは10ギガビット/秒）
- 自動ネゴシエーション設定（trueまたはfalse）
- 二重モードと動作ステータス（halfまたはfull）
- ポートのインターフェイスグループ（該当する場合）
- ポートのVLANタグ情報（該当する場合）

- ポートのヘルスステータス（healthまたはdegraded）
- ポートがデグレードとマークされた理由

該当するデータがないフィールドの値はと表示されます（アクティブでないポートの二重モードの動作中や速度は表示されません）。 –

ステップ

コマンドを使用して、ネットワークポートの情報を表示します `network port show`。

各ポートの詳細情報を表示するには、パラメータを指定します。特定の情報を表示 `-instance`するには、パラメータを使用してフィールド名を指定し `-fields`ます。

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP VLAN情報の表示

クラスタ内の特定の VLAN またはすべての VLAN の情報を表示できます。

タスクの内容

パラメータを指定すると、各VLANの詳細情報を表示できます `-instance`。特定の情報を表示するには、パ

ラメータを使用してフィールド名を指定し `-fields`ます。

ステップ

コマンドを使用して、VLANに関する情報を表示します `network port vlan show`。次のコマンドは、クラスタ内のすべてのVLANに関する情報を表示します。

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

の詳細については `network port vlan show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPインターフェイスグループ情報の表示

インターフェイスグループに関する情報を表示して、その設定を確認できます。

タスクの内容

次の情報が表示されます。

- インターフェイスグループが配置されているノード
- インターフェイスグループに含まれているネットワークポートのリスト
- インターフェイスグループの名前
- 分散機能（ MAC 、 IP 、ポート、またはシーケンシャル）
- インターフェイスグループの Media Access Control （ MAC ；メディアアクセス制御）アドレス
- ポートのアクティビティステータス。集約されたポートがアクティブであるかどうか（すべてのポートがアクティブであるかどうか）、アクティブであるポートがないかどうか（一部のポートがアクティブであるかどうか）、アクティブでないかどうかを示します

ステップ

コマンドを使用して、インターフェイスグループに関する情報を表示します `network port ifgrp show`。

各ノードの詳細情報を表示するには、パラメータを指定し `-instance`ます。特定の情報を表示するには、パラ

メータを使用してフィールド名を指定し `-fields`ます。

次のコマンドは、クラスタ内のすべてのインターフェイスグループに関する情報を表示します。

```
network port ifgrp show
          Port     Distribution                    Active
Node      IfGrp    Function     MAC Address        Ports   Ports
--------- -------- ------------ -----------------  ------- --------
cluster-1-01
          a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
          a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
          a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
          a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

次のコマンドは、 1 つのノードのインターフェイスグループの詳細情報を表示します。

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

の詳細については `network port ifgrp show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP LIF情報の表示

LIF に関する詳細情報を表示して、その設定を確認できます。

この情報は、IPアドレスが重複していないか、ネットワーク ポートが正しいサブネットに属しているかなど、LIFの基本的な問題を診断するのにも便利です。Storage Virtual Machine（SVM）管理者は、SVMに関連付けられているLIFの情報だけを表示できます。

タスクの内容

次の情報が表示されます。

- LIF に関連付けられている IP アドレス

- LIF の管理ステータス
- LIFの動作ステータス

  データ LIF の動作ステータスは、そのデータ LIF が関連付けられている SVM のステータスによって決まります。SVM が停止すると、 LIF の動作ステータスが down に変わります。SVM が再び起動すると、動作ステータスは up に変わります

- LIF が配置されているノードとポート

該当するデータがないフィールド（ステータスの詳しい情報がない場合など）については、と表示されます - 。

ステップ

コマンドを使用して、LIFの情報を表示します `network interface show`。

各 LIF の詳しい情報を表示するには、 -instance パラメータを指定します。特定の情報を表示するには、 -fields パラメータを使用してフィールド名を指定します。

次のコマンドは、クラスタ内のすべての LIF に関する一般的な情報を表示します。

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

次のコマンドは、 1 つの LIF に関する詳細情報を表示します。

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
             Administrative Status: up
                  Failover Policy: local-only
                  Firewall Policy: data
                      Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPネットワークのルーティング情報の表示

SVM内のルートに関する情報を表示できます。

ステップ

表示するルーティング情報のタイプに応じて、該当するコマンドを入力します。

表示する情報	入力するコマンド
SVM の静的ルート	`network route show`

SVM の各ルートの LIF	`network route show-lifs`

パラメータを指定すると、各ルートの詳細情報を表示できます `-instance`。次のコマンドは、cluster-1のSVM内の静的ルートを表示します。

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

次のコマンドは、cluster-1のすべてのSVM内の静的ルートと論理インターフェイス（LIF）の関連付けを表示します。

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

および `network route show-lifs` の詳細については `network route show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP DNSホストテーブルエントリの表示

DNS hosts テーブルエントリは、ホスト名と IP アドレスのマッピングです。クラスタ内のすべての SVM のホスト名およびエイリアス名と IP アドレスのマッピングを表示することができます。

ステップ

vserver services name-service dns hosts showコマンドを使用して、すべてのSVMのホスト名エントリを表示します。

次の例は、ホストテーブルエントリを表示します。

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。

ONTAP DNSドメイン設定情報の表示

クラスタ内の1つ以上のStorage Virtual Machine（SVM）のDNSドメイン設定を表示して、正しく設定されているかどうかを確認できます。

ステップ

コマンドを使用して、DNSドメイン設定を表示します `vserver services name-service dns show`。

次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

```
vserver services name-service dns show
                                                    Name
Vserver         State     Domains                   Servers
--------------- --------- ------------------------- -------------
cluster-1        enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs1             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs2             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs3             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
```

次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
         Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

ONTAPフェイルオーバーグループの情報を表示します。

フェイルオーバーグループに関する情報を表示することができます。これには、各フェイルオーバーグループ内のノードとポートのリスト、フェイルオーバーの有効 / 無効、各 LIF に適用されているフェイルオーバーポリシーの種類が含まれます。

手順

1. コマンドを使用して、各フェイルオーバーグループのターゲットポートを表示します `network interface failover-groups show`。

   次のコマンドは、2ノードクラスタのすべてのフェイルオーバーグループに関する情報を表示します。

   ```
   network interface failover-groups show
                                 Failover
   Vserver          Group        Targets
   ---------------- ------------ --------------------------------
   Cluster
                    Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
   vs1
                    Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
   ```

   の詳細については `network interface failover-groups show`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用して、特定のフェイルオーバーグループのターゲットポートとブロードキャストドメインを表示します `network interface failover-groups show`。

   次のコマンドは、 SVM vs4 の data12 というフェイルオーバーグループに関する詳しい情報を表示します。

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. コマンドを使用して、すべてのLIFで使用されているフェイルオーバー設定を表示します `network interface show`。

   次のコマンドは、各 LIF で使用されているフェイルオーバーポリシーとフェイルオーバーグループを表示します。

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy         failover-group
--------  -------------------  ----------------------  --------------
Cluster   cluster1-01_clus_1  local-only              Cluster
Cluster   cluster1-01_clus_2  local-only              Cluster
Cluster   cluster1-02_clus_1  local-only              Cluster
Cluster   cluster1-02_clus_2  local-only              Cluster
cluster1  cluster_mgmt        broadcast-domain-wide   Default
cluster1  cluster1-01_mgmt1   local-only              Default
cluster1  cluster1-02_mgmt1   local-only              Default
vs1       data1               disabled                Default
vs3       data2               system-defined          group2
```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP LIFのフェイルオーバーターゲットの表示

LIF のフェイルオーバーポリシーとフェイルオーバーグループが正しく設定されているかどうかを確認しなければならない場合があります。フェイルオーバールールを間違って設定しないように、 1 つまたはすべての LIF のフェイルオーバーターゲットを表示できます。

タスクの内容

LIF のフェイルオーバーターゲットを表示すると、次のことを確認できます。

- LIF に正しいフェイルオーバーグループとフェイルオーバーポリシーが設定されているかどうか
- 表示されたフェイルオーバーターゲットのポートが LIF に適しているかどうか

- データ LIF のフェイルオーバーターゲットが管理ポート（ e0M ）でないかどうか

ステップ

コマンドのオプションを `network interface show`使用して、LIFのフェイルオーバーターゲットを表示します `failover。

次のコマンドは、 2 ノードクラスタのすべての LIF のフェイルオーバーターゲットに関する情報を表示します。行は `Failover Targets`、特定のLIFにおけるノードとポートの組み合わせの（優先順位の高い）リストを示しています。

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------- --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ロードバランシングゾーンのONTAP LIFを表示する

ロードバランシングゾーンに属するすべてのLIFを表示することで、そのゾーンが正しく設定されているかどうかを確認できます。特定のLIFのロードバランシングゾーン、またはすべてのLIFのロードバランシングゾーンを表示することもできます。

ステップ

次のいずれかのコマンドを使用して、必要なLIFとロードバランシングの詳細を表示します。

表示する内容	入力するコマンド
特定のロードバランシングゾーンに属する LIF	`network interface show -dns-zone zone_name` `zone_name`ロードバランシングゾーンの名前を指定します。
特定の LIF のロードバランシングゾーン	`network interface show -lif lif_name -fields dns-zone`
すべての LIF のロードバランシングゾーン	`network interface show -fields dns-zone`

LIFのロードバランシングゾーンを表示する例

次のコマンドは、SVM vs0のstorage.company.comというロードバランシングゾーンに属するすべてのLIFの詳細を表示します。

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

次のコマンドは、data3というLIFのDNSゾーンの詳細を表示します。

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

次のコマンドは、クラスタ内のすべてのLIFとそれに対応するDNSゾーンのリストを表示します。

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPクラスタ接続の表示

クラスタ内のすべてのアクティブな接続を表示したり、クライアント、論理インターフェイス、プロトコル、またはサービス別にノードのアクティブな接続数を表示したりできます。クラスタ内のリスンしている接続をすべて表示することもできます。

クライアント別のアクティブな接続を表示する（クラスタ管理者のみ）

クライアント別にアクティブな接続を表示して、特定のクライアントが使用しているノードを確認したり、ノードあたりのクライアント数に不均衡がないかどうかを確認したりできます。

タスクの内容

クライアント別のアクティブな接続数の情報は、次のような場合に役立ちます。

- ビジー状態や過負荷のノードを見つける。
- 特定のクライアントからのボリュームへのアクセスが低速になっている理由を確認する。

  クライアントがアクセスしているノードに関する詳細を表示し、ボリュームが配置されているノードと比較できます。ボリュームへのアクセスにクラスタ ネットワークのトラバースが必要な場合、オーバーサブスクライブされたリモート ノードにあるボリュームへのリモート アクセスにより、クライアントのパフォーマンスが低下することがあります。

- データ アクセスにすべてのノードが均等に使用されていることを確認する。
- 接続数が想定よりも多いクライアントを探す。
- 特定のクライアントがノードに接続しているかどうかを確認する。

ステップ

コマンドを使用して、ノードのアクティブな接続数をクライアント別に表示します `network connections active show-clients`。

の詳細については `network connections active show-clients`、を"ONTAPコマンド リファレンス"参照してください。

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253               1
        vs0             192.0.2.252               2
        Cluster         192.10.2.124              5
node1   vs0             192.0.2.250               1
        vs0             192.0.2.252               3
        Cluster         192.10.2.123              4
node2   vs1             customer.example.com      1
        vs1             192.0.2.245               3
        Cluster         192.10.2.122              4
node3   vs1             customer.example.org      1
        vs1             customer.example.net      3
        Cluster         192.10.2.121              4
```

プロトコル別のアクティブな接続を表示する（クラスタ管理者のみ）

ノードのアクティブな接続数をプロトコル（TCPまたはUDP）別に表示して、クラスタ内のプロトコルの使用状況を比較できます。

タスクの内容

プロトコル別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 接続が切断されているUDPクライアントを探す。

  ノードの接続数が制限に近づいたときに最初に接続が切断されるのはUDPクライアントです。

- 他のプロトコルが使用されていないことを確認する。

ステップ

コマンドを使用して、ノードのアクティブな接続数をプロトコル別に表示します `network connections active show-protocols`。

の詳細については `network connections active show-protocols`、を"ONTAPコマンド リファレンス"参照してください。

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

サービス別のアクティブな接続を表示します（クラスタ管理者のみ）。

クラスタ内の各ノードのアクティブな接続数をサービスタイプ（NFS、SMB、マウントなど）別に表示できます。これは、クラスタ内のサービスの使用状況を比較するのに役立ちます。これは、ノードのプライマリワークロードを特定するのに役立ちます。

タスクの内容

サービス別のアクティブな接続数の情報は、次のような場合に役立ちます。

- すべてのノードが適切なサービス用に使用されていること、そのサービスのロード バランシングが機能していることを確認する。
- 他のサービスが使用されていないことを確認する。コマンドを使用して、ノードのアクティブな接続数をサービス別に表示します `network connections active show-services`。

の詳細については `network connections active show-services`、を"ONTAPコマンド リファレンス"参照してください。

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

ノードおよび**SVM**の**LIF**別にアクティブな接続を表示する

ノードおよびStorage Virtual Machine（SVM）別のLIFのアクティブな接続数を表示して、クラスタ内のLIF間で接続数の不均衡がないかどうかを確認できます。

タスクの内容

LIF別のアクティブな接続数は、次のような場合に役立ちます。

- 各LIFの接続数を比較して過負荷のLIFを特定する。
- すべてのデータLIFに対してDNSロードバランシングが機能していることを確認する。
- さまざまなSVMへの接続数を比較して、最もよく使用されているSVMを特定する。

ステップ

コマンドを使用して、SVMとノードのアクティブな接続数をLIF別に表示します `network connections active show-lifs`。

の詳細については `network connections active show-lifs`、を"ONTAPコマンド リファレンス"参照してください。

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

クラスタ内のアクティブな接続を表示します。

クラスタ内のアクティブな接続に関する情報を表示して、個 々 の接続で使用されているLIF、ポート、リモートホスト、サービス、Storage Virtual Machine（SVM）、およびプロトコルを確認できます。

タスクの内容

クラスタ内のアクティブな接続の情報は、次のような場合に役立ちます。

- 個々のクライアントで正しいノードの正しいプロトコルやサービスを使用していることを確認する。
- クライアントで特定の組み合わせのノード、プロトコル、およびサービスを使用してデータにアクセスできない場合に、同様のクライアントを探して設定やパケット トレースを比較する。

ステップ

コマンドを使用して、クラスタ内のアクティブな接続数を表示します `network connections active show`。

の詳細については `network connections active show`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、ノードnode1のアクティブな接続の情報を表示します。

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

次のコマンドは、SVM vs1のアクティブな接続の情報を表示します。

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

クラスタ内のリスンしている接続を表示する

クラスタ内のリスンしている接続に関する情報を表示して、特定のプロトコルおよびサービスの接続を受け入れているLIFとポートを確認できます。

タスクの内容

クラスタ内のリスンしている接続の表示は、次のような場合に役立ちます。

- 特定のLIFへのクライアント接続が必ず失敗する場合に、そのLIFを適切なプロトコルまたはサービスでリスンしていることを確認する。
- あるノードのボリュームのデータに別のノードのLIFを介してリモート アクセスできない場合に、それぞれのクラスタLIFでUDP / rclopcpリスナーが開いていることを確認する。
- 同じクラスタの2つのノード間でのSnapMirror転送に失敗した場合に、それぞれのクラスタLIFでUDP / rclopcpリスナーが開いていることを確認する。
- 異なるクラスタの2つのノード間でのSnapMirror転送に失敗した場合に、それぞれのクラスタ間LIFでTCP / ctlopcpリスナーが開いていることを確認する。

ステップ

コマンドを使用して、ノードごとにリスンしている接続を表示します `network connections listening`

show。

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

の詳細については `network connections listening show`、を"ONTAPコマンド リファレンス"参照してください。

ネットワークの問題を診断するためのONTAPコマンド

ネットワークの問題を診断するには、や `tcpdump`などのコマンドを使用し `ping`, `traceroute`, `ndp`,`ます。や `traceroute6`などのコマンドを使用して、IPv6の問題を診断することもできます `ping6`。

状況	入力するコマンド
ノードがネットワーク上の他のホストに到達できるかどうかをテストする	`network ping`
ノードがIPv6ネットワーク上の他のホストに到達できるかどうかをテストする	`network ping6`
IPv4パケットがネットワーク ノードまでたどったルートをトレースする	`network traceroute`
IPv6パケットがネットワーク ノードまでたどったルートをトレースする	`network traceroute6`
近隣探索プロトコル（NDP）を管理する	`network ndp`
指定したネットワーク インターフェイスまたはすべてのネットワーク インターフェイスで送受信されたパケットの統計情報を表示する	`run -node` *`node_name`* `ifstat`注：このコマンドはノードシェルから使用できます。

クラスタ内の各ノードおよびポートから検出された隣接デバイスに関する情報（リモートデバイスのタイプやデバイスプラットフォームなど）を表示する	`network device-discovery show`
ノードのCDP隣接デバイスを表示する（ONTAPはCDPv1通知のみをサポート）	`run -node node_name cdpd show-neighbors`注：このコマンドはノードシェルから使用できます。
ネットワークで送受信されたパケットをトレースする	`network tcpdump start -node node-name -port port_name`注：このコマンドはノードシェルから使用できます。
クラスタ間ノードまたはクラスタ内ノード間のレイテンシとスループットを測定	`network test -path -source-node source_nodename local -destination-cluster destination_clustername -destination-node destination_nodename -session -type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer`詳細については、を参照して"パフォーマンス管理"ください。

関連情報

- "ONTAPコマンド リファレンス"
- "ネットワークping"
- "ネットワークtraceroute"
- "network device-discovery show"
- "ネットワークNDP"

近接探索プロトコルによるネットワーク接続の表示

近接探索プロトコルを使用した**ONTAP**ネットワーク接続の表示

データセンターでは、近接探索プロトコルを使用して、物理システムまたは仮想システムのペアとそれらのネットワークインターフェイス間のネットワーク接続を表示できます。ONTAP では、 2 つの近接探索プロトコルとして、 Cisco Discovery Protocol （ CDP ）と Link Layer Discovery Protocol （ LLDP ）がサポートされます。

近接探索プロトコルを使用すると、ネットワーク内の直接接続されたプロトコル対応デバイスを自動的に検出し、その情報を表示できます。各デバイスは、ID、機能、および接続情報をアドバタイズします。この情報はイーサネットフレームでマルチキャストMACアドレスに送信され、隣接するすべてのプロトコル対応デバイスで受信されます。

2つのデバイスをネイバーにするには、各デバイスでプロトコルが有効になっており、正しく設定されている必要があります。検出プロトコルの機能は、直接接続されたネットワークに限定されます。ネイバーには、スイッチ、ルータ、ブリッジなどのプロトコル対応デバイスを含めることができます。ONTAPでは、2つの近接探索プロトコルがサポートされており、個別に使用することも一緒に使用することもできます

- シスコ検出プロトコル（ CDP ） *

CDPは、Cisco Systemsが開発した独自のリンク層プロトコルです。クラスタポートのONTAPではデフォルトで有効になりますが、データポートに対しては明示的に有効にする必要があります。

- リンク層検出プロトコル（ LLDP ） *

LLDPは、標準ドキュメントIEEE 802.1ABで指定されているベンダーに依存しないプロトコルです。すべてのポートに対して明示的にイネーブルにする必要があります。

CDPを使用したONTAPネットワーク接続の検出

CDPを使用したネットワーク接続の検出は、導入に関する考慮事項の確認、データ ポートでのCDPの有効化、近隣デバイスの表示、CDPの設定値の調整（必要な場合）で構成されます。クラスタ ポートでは、CDPはデフォルトで有効になります。

近隣デバイスに関する情報を表示するには、スイッチとルーターでもCDPを有効にする必要があります。

ONTAP リリース	説明
9.10.1以前	CDPは、クラスタスイッチヘルスモニタでも使用され、クラスタネットワークスイッチと管理ネットワークスイッチを自動的に検出します。
9.11.1以降	CDPは、クラスタ、ストレージ、および管理ネットワークスイッチを自動的に検出するためにクラスタスイッチヘルスモニタでも使用されます。

関連情報

"システム管理"

CDPを使用する場合の考慮事項

デフォルトでは、CDP対応デバイスはCDPv2通知を送信します。CDP対応デバイスは、CDPv1通知を受信した場合にのみCDPv1通知を送信します。ONTAPはCDPv1のみをサポートします。そのため、ONTAPノードがCDPv1通知を送信すると、CDP対応の隣接デバイスがCDPv1通知を返します。

ノードでCDPを有効にする前に、次の点を考慮してください。

- CDPはすべてのポートでサポートされます。
- CDP通知はup状態のポートから送受信されます。
- CDP通知を送受信するには、送信デバイスと受信デバイスの両方でCDPを有効にする必要があります。
- CDP通知は一定の間隔で送信され、送信間隔を設定できます。
- LIFのIPアドレスが変更されると、ノードは更新された情報を次のCDP通知で送信します。
- ONTAP 9.10.1以前：
  - CDPはクラスタ ポートで常に有効になります。
  - 非クラスタ ポートでは、CDPはデフォルトで無効になります。
- ONTAP 9.11.1以降：
  - CDPはクラスタ ポートとストレージ ポートで常に有効になります。
  - 非クラスタ ポートと非ストレージ ポートでは、CDPはデフォルトで無効になります。

ノードでLIFが変更された場合、スイッチなどの受信デバイス側でCDP情報が更新されないことがあります。このような問題が発生した場合は、ノードのネットワーク インターフェイスをいったんdown状態にしてから、up状態に設定してください。

- CDP通知で送信されるのはIPv4アドレスのみです。
- VLANが設定されている物理ネットワーク ポートの場合、VLANに設定されているすべてのLIFが通知されます。
- インターフェイス グループの一部となっている物理ポートの場合、そのインターフェイス グループに設定されているすべてのIPアドレスが、各物理ポートで通知されます。
- VLANをホストするインターフェイス グループの場合、インターフェイス グループおよびVLANに設定されているすべてのLIFが各ネットワーク ポートで通知されます。
- CDPパケットの最大サイズは1500バイトであるため、LIFが多数設定されたポートでは、隣接するスイッチで報告されるIPアドレスの一部しかありません。

CDPの有効化または無効化

CDP対応の近隣デバイスを検出して通知を送信するには、クラスタの各ノードでCDPが有効になっている必要があります。

ONTAP 9.10.1以前では、CDPはデフォルトでノードのすべてのクラスタ ポートで有効に、非クラスタ ポートで無効になります。

ONTAP 9.11.1以降では、CDPはデフォルトでノードのすべてのクラスタ ポートとストレージ ポートで有効に、非クラスタ ポートと非ストレージ ポートで無効になります。

タスクの内容

オプションは `cdpd.enable`、ノードのポートでCDPを有効にするか無効にするかを制御します。

- ONTAP 9 .10.1以前の場合、onを指定すると、非クラスタポートでCDPが有効になります。
- ONTAP 9 .11.1以降では、onを指定すると、クラスタ以外のポートとストレージ以外のポートでCDPが有効になります。
- ONTAP 9 .10.1以前の場合、offを指定すると非クラスタポートのCDPが無効になります。クラスタポートのCDPを無効にすることはできません。
- ONTAP 9 .11.1以降では、offを指定すると、非クラスタポートとストレージポートでCDPが無効になります。クラスタポートではCDPを無効にすることはできません。

CDP対応デバイスに接続されているポートでCDPを無効にすると、ネットワークトラフィックが最適化されない場合があります。

手順

1. クラスタ内の1つまたはすべてのノードの、現在のCDP設定を表示します。

CDP 設定を表示する対象	入力するコマンド
ノード	`run - node <node_name> options cdpd.enable`
クラスタ内のすべてのノード	`options cdpd.enable`

2. クラスタ内の1つまたはすべてのノードで、すべてのポートのCDPを有効または無効に設定します。

CDPを有効または無効にする対象	入力するコマンド
ノード	`run -node node_name options cdpd.enable {on or off}`
クラスタ内のすべてのノード	`options cdpd.enable {on or off}`

CDP近隣情報の表示

クラスタのノードのポートにCDP対応デバイスが接続されている場合は、そのポートの隣接デバイスに関する情報を表示できます。ネイバー情報を表示するには、コマンドを使用し `network device-discovery show -protocol cdp`ます。の詳細については `network device-discovery show`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

ONTAP 9 .10.1以前では、CDPはクラスタポートで常に有効になっているため、これらのポートのCDP隣接情報が常に表示されます。非クラスタポートの隣接情報を表示するには、非クラスタポートでCDPを有効にする必要があります。

ONTAP 9 .11.1以降では、クラスタポートとストレージポートのCDPは常に有効になっているため、それらのポートのCDP隣接情報が常に表示されます。非クラスタポートおよび非ストレージポートのネイバー情報を表示するには、これらのポートでCDPを有効にする必要があります。

ステップ

クラスタ内のノードのポートに接続されているすべてのCDP対応デバイスの情報を表示します。

```
network device-discovery show -node node -protocol cdp
```

次のコマンドは、ノードsti2650-212のポートに接続されている近隣デバイスの情報を表示します。

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

このコマンドの出力には、指定したノードの各ポートに接続されているCiscoデバイスが一覧表示されます。

CDPメッセージの保持時間の設定

保持時間は、CDP通知がCDP対応の近隣デバイスのキャッシュに格納される時間です。保持時間は各CDPv1パケットで通知され、ノードがCDPv1パケットを受信するたびに更新されます。

- このオプションの値は `cdpd.holdtime`、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの保持時間の値は180秒ですが、10~255秒の範囲の値を入力できます。
- 保持期限が切れる前にIPアドレスが削除された場合、CDP情報は保持期限が切れるまでキャッシュされます。

手順

1. クラスタ内の1つまたはすべてのノードのCDPの現在の保持時間を表示します。

保持時間を表示する対象	入力するコマンド
ノード	`run -node node_name options cdpd.holdtime`
クラスタ内のすべてのノード	`options cdpd.holdtime`

2. クラスタ内の1つまたはすべてのノードのすべてのポートでCDP保持時間を設定します。

保持時間を設定する対象	入力するコマンド
ノード	`run -node node_name options cdpd.holdtime holdtime`
クラスタ内のすべてのノード	`options cdpd.holdtime holdtime`

CDP通知の送信間隔を設定する

CDP通知は、一定の間隔でCDP近隣機器に送信されます。ネットワーク トラフィックの量やネットワーク トポロジの変化に応じて、CDP通知の送信間隔を調節することができます。

- このオプションの値は `cdpd.interval`、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの間隔は60秒ですが、5~900秒の値を入力できます。

手順

1. クラスタ内の1つまたはすべてのノードについて、CDP通知の現在の送信間隔を表示します。

送信間隔を表示する対象	入力するコマンド
ノード	`run -node node_name options cdpd.interval`
クラスタ内のすべてのノード	`options cdpd.interval`

2. クラスタ内の1つまたはすべてのノードのすべてのポートについて、CDP通知の送信間隔を設定します。

送信間隔を設定する対象	入力するコマンド
ノード	`run -node node_name options cdpd.interval interval`
クラスタ内のすべてのノード	`options cdpd.interval interval`

CDP統計情報の表示と消去

ネットワーク接続で発生する可能性のある問題を見つけるために、各ノードのクラスタ ポートと非クラスタ ポートのCDP統計情報を確認できます。CDP統計情報は、前回消去されたときからの累積値です。

タスクの内容

ONTAP 9 .10.1以前では、CDPはポートに対して常にイネーブルになっているため、これらのポートのトラフィックについては常にCDP統計情報が表示されます。ポートの統計情報を表示するには、CDPをポートでイネーブルにする必要があります。

ONTAP 9 .11.1以降では、クラスタポートとストレージポートのCDPは常に有効になっているため、これらのポートのトラフィックのCDP統計は常に表示されます。非クラスタポートまたは非ストレージポートの統計を表示するには、非クラスタポートまたは非ストレージポートでCDPを有効にする必要があります。

ステップ

ノードのすべてのポートに関する現在のCDP統計情報を表示、または消去します。

状況	入力するコマンド
CDP統計情報を表示	`run -node node_name cdpd show-stats`
CDP統計情報を消去	`run -node node_name cdpd zero-stats`

統計情報の表示と消去の例

次のコマンドは、消去する前のCDP統計情報の例を示します。前回統計情報が消去されてから、送信および受信したパケットの総数が出力されています。

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

次のコマンドは、CDP統計情報を消去します。

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:              0   | Csum Errors:         0   | Unsupported Vers:      0
 Invalid length:       0   | Malformed:           0   | Mem alloc fails:       0
 Missing TLVs:         0   | Cache overflow:      0   | Other errors:          0

TRANSMIT
 Packets:              0   | Xmit fails:          0   | No hostname:           0
 Packet truncated:     0   | Mem alloc fails:     0   | Other errors:          0

OTHER
 Init failures:        0
```

統計情報を消去すると、次にCDP通知が送信または受信された時点から情報が累積されていきます。

CDPがサポートされないイーサネット スイッチへの接続

一部のベンダー スイッチではCDPがサポートされません。参照"NetAppナレッジベース: ONTAPデバイス検出でスイッチではなくノードが表示される"詳細についてはこちらをご覧ください。

この問題を解決するには、次の2つの方法があります。

- CDPを無効にし、LLDPを有効にします（サポートされている場合）。詳細については、を参照してください "LLDPを使用したネットワーク接続の検出" 。
- CDPアドバタイズメントをドロップするように、スイッチにMACアドレスパケットフィルタを設定します。

LLDPを使用したONTAPネットワーク接続の検出

LLDPを使用したネットワーク接続の検出は、導入に関する考慮事項の確認、すべてのポートでのLLDPの有効化、隣接デバイスの表示、LLDPの設定値の調整（必要な場合）で構成されます。

ネイバーデバイスに関する情報を表示するには、スイッチおよびルータでもLLDPをイネーブルにする必要があります。

ONTAPは現在、次のType-Length-Value構造体（TLV）を報告します。

- シャーシID
- ポートID
- Time-To-Live（TTL）
- システム名

  システム名TLVは、CNAデバイスでは送信されません。

X1143アダプタやUTA2オンボード ポートなどの特定の統合ネットワーク アダプタ（CNA）にはLLDPのオフロード サポートが含まれています。

- LLDPのオフロードは、Data Center Bridging（DCB）に使用されます。
- 表示される情報がクラスタとスイッチの間で異なる場合があります。

  スイッチで表示されるシャーシIDとポートIDのデータは、CNAポートとCNA以外のポートで異なる場合があります。

例：

- CNA以外のポートの場合：
  - シャーシIDは、ノード上のいずれかのポートの固定MACアドレスです。
  - port IDは、ノード上のそれぞれのポートのポート名です。
- CNAポートの場合：
  - シャーシIDとポートIDは、ノード上の各ポートのMACアドレスです。

ただし、これらのタイプのポートについては、クラスタで表示されるデータに一貫性があります。

LLDP仕様では、SNMP MIBを介した収集された情報へのアクセスが定義されています。ただし、ONTAPは現在LLDP MIBをサポートしていません。

LLDPの有効化または無効化

LLDP対応の近隣デバイスを検出して通知を送信するには、クラスタの各ノードでLLDPが有効になっている必要があります。ONTAP 9.7以降では、ノードのすべてのポートでLLDPがデフォルトで有効になります。

タスクの内容

LLDP .10.1以前の場合ONTAP 9は、 `lldp.enable`オプションでノードのポートでLLDPを有効にするか無効にするかを制御します。

- `on`すべてのポートでLLDPをイネーブルにします。
- `off`すべてのポートでLLDPをディセーブルにします。

LLDP.11.1以降の場合、ONTAP 9オプションは、 `lldp.enable`ノードの非クラスタポートおよびストレージポートでLLDPを有効にするか無効にするかを制御します。

- `on`すべての非クラスタポートおよびストレージポートでLLDPをイネーブルにします。
- `off`すべての非クラスタポートおよびストレージポートでLLDPを無効にします。

手順

1. クラスタ内の1つまたはすべてのノードの現在のLLDP設定を表示します。
   - シングルノード： `run -node node_name options lldp.enable`
   - すべてのノード：オプション `lldp.enable`
2. クラスタ内の1つまたはすべてのノードのすべてのポートでLLDPを有効または無効にします。

LLDPを有効または無効にする対象	入力するコマンド
ノード	`run -node node_name options lldp.enable {on
off}`	クラスタ内のすべてのノード
`options lldp.enable {on	off}`

- シングルノード：

```
run -node node_name options lldp.enable {on|off}
```

- すべてのノード：

```
options lldp.enable {on|off}
```

LLDP近隣情報の表示

クラスタのノードのポートにLLDP対応デバイスが接続されている場合は、そのポートの近隣デバイスの情報を表示することができます。近隣情報を表示するには、network device-discovery showコマンドを使用します。

ステップ

1. クラスタ内のノードのポートに接続されているすべてのLLDP準拠デバイスの情報を表示します。

```
network device-discovery show -node node -protocol lldp
```

次のコマンドは、ノードcluster-1_01のポートに接続されているネイバーの情報を表示します。出力には、指定したノードの各ポートに接続されているLLDP対応デバイスが表示されます。この `-protocol`オプションを省略すると、CDP対応デバイスも出力に表示されます。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

LLDP通知の送信間隔を調整する

LLDP通知は、一定の間隔でLLDPネイバーに送信されます。ネットワークトラフィックやネットワークトポロジの変化に応じて、LLDP通知の送信間隔を増減できます。

タスクの内容

IEEEが推奨するデフォルトの間隔は30秒ですが、5～300秒の値を入力できます。

手順

1. クラスタ内の1つまたはすべてのノードについて、LLDP通知の現在の間隔を表示します。
   - シングルノード：

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - すべてのノード：

     ```
     options lldp.xmit.interval
     ```

2. クラスタ内の1つまたはすべてのノードのすべてのポートについて、LLDP通知の送信間隔を調整します。
   - シングルノード：

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - すべてのノード：

     ```
     options lldp.xmit.interval <interval>
     ```

LLDP通知のTime-To-Live値を調整する

Time-To-Live（TTL）は、LLDP通知がLLDP準拠の隣接デバイスのキャッシュに格納される期間です。TTLは各LLDPパケットでアドバタイズされ、ノードがLLDPパケットを受信するたびに更新されます。TTLは発信LLDPフレームで変更できます。

タスクの内容

- TTLは計算された値(`lldp.xmit.interval`（送信間隔の積）と保持乗数(`lldp.xmit.hold`）に1を足したものです。
- デフォルトの保持乗数の値は4ですが、1～100の範囲の値を入力できます。
- したがって、IEEEが推奨するデフォルトのTTLは121秒ですが、送信間隔と保持乗数の値を調整することで、発信フレームの値を6秒から30001秒に指定できます。
- TTLが期限切れになる前にIPアドレスが削除された場合、LLDP情報はTTLが期限切れになるまでキャッシュされます。

手順

1. クラスタ内の1つまたはすべてのノードの現在の保持の乗数を表示します。
   - シングルノード：

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - すべてのノード：

     ```
     options lldp.xmit.hold
     ```

2. クラスタ内の1つまたはすべてのノードのすべてのポートで、保持の乗数を調整します。
   - シングルノード：

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - すべてのノード：

     ```
     options lldp.xmit.hold <hold_value>
     ```

LLDP統計の表示またはクリア

各ノードのクラスタポートと非クラスタポートのLLDP統計を表示して、ネットワーク接続の潜在的な問題を検出できます。LLDP統計情報は、最後に消去された時点からの累積値です。

タスクの内容

LLDP.10.1以前の場合、ONTAP 9はクラスタポートで常に有効になっているため、これらのポートのトラフィックについては常にLLDP統計が表示されます。非クラスタポートの統計を表示するには、非クラスタポートでLLDPを有効にする必要があります。

LLDPはクラスタポートとストレージポートで常に有効になるため、LLDP統計はそれらのポートのトラフィックについて常に表示されますONTAP 9。非クラスタポートおよびストレージポートの統計情報を表示するには、非クラスタポートおよびストレージポートでLLDPを有効にする必要があります。

ステップ

ノードのすべてのポートの現在のLLDP統計を表示または消去します。

状況	入力するコマンド
LLDP統計を表示します	`run -node node_name lldp stats`
LLDP統計情報をクリアします	`run -node node_name lldp stats -z`

統計情報の表示と消去の例

次のコマンドは、クリア前のLLDP統計情報を表示します。出力には、統計情報が最後に消去されてから送受信されたパケットの合計数が表示されます。

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

次のコマンドは、LLDP統計情報をクリアします。

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

統計情報を消去すると、次のLLDPアドバタイズメントが送信または受信されたあとに統計情報が蓄積され始めます。

NASストレージの管理

System Managerを使用したNASプロトコルの管理

ONTAP System Managerを使用したNAS管理について学ぶ

このセクションのトピックでは、ONTAP 9 .7以降のリリースでSystem Managerを使用してNAS環境を構成および管理する方法について説明します。

従来のSystem Manager（ONTAP 9 .7以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- "NFSセツテイノカイヨウ"
- "SMBセツテイノカイヨウ"

System Managerでサポートされるワークフロー

- NASファイルサービスに使用するクラスタの初期設定。
- 変化するストレージニーズに対応する追加のボリュームプロビジョニング。
- 業界標準の認証およびセキュリティ機能の設定とメンテナンス。

System Managerを使用すると、NASサービスをコンポーネント レベルで管理できます。

- プロトコル – NFS、SMB、または両方（NASのマルチプロトコル）
- ネーム サービス – DNS、LDAP、NIS
- ネーム サービス スイッチ
- KerberosとTLSのセキュリティ
- エクスポートと共有
- qtree
- ユーザおよびグループのネーム マッピング

ONTAP System Manager を使用して VMware データストア用の NFS ストレージをプロビジョニングする

Virtual Storage Console for VMware vSphere（VSC）を使用してESXiホスト用のONTAPベースのストレージシステムにNFSボリュームをプロビジョニングする前に、System Manager for ONTAP 9 .7以降を使用してNFSを有効にしてください。

System Managerでを作成したら"NFS 対応の Storage VM"、VSCを使用してNFSボリュームをプロビジョニングし、データストアを管理します。

VSC 7.0以降では、VSCがに組み込まれて "ONTAP Tools for VMware vSphere 仮想アプライアンス"おり、VSC、vStorage APIs for Storage Awareness（VASA）Provider、およびStorage Replication Adapter（SRA）for VMware vSphereの機能が含まれています。

で "NetAppのInteroperability Matrix"、現在使用しているONTAPリリースとVSCリリースの互換性を確認してください。

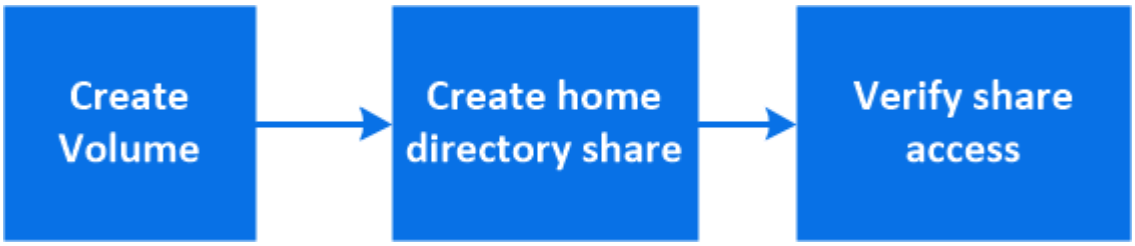
System Manager Classic（ONTAP 9.7以前のリリース）を使用してESXiホストからデータストアへのNFSアクセスを設定するには、を参照してください。 "VSCを使用したESXi向けのNFS設定の概要"

詳細については、およびVSCリリースのドキュメントを参照してください "TR-4597 ：『 VMware vSphere for ONTAP 』"。

ONTAP System Manager を使用してホームディレクトリ用の NAS ストレージをプロビジョニングする

SMBプロトコルを使用して、ホームディレクトリ用のストレージを提供するボリュームを作成します。

この手順では、にホームディレクトリ用の新しいボリュームを作成し"SMB対応の既存のStorage VM"ます。ボリュームの設定時にシステムのデフォルトを受け入れることも、カスタム設定を指定することもできます。



FlexVolを作成することも、高パフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。参照"FlexGroup ボリュームを作成します"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

手順

1. SMBが有効なStorage VMに新しいボリュームを追加します。
   a. [ストレージ]>[ボリューム]を選択し、[追加]*をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      SMBプロトコルが設定されているStorage VMのみが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

      - この時点で * Save * をクリックすると、 System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。
      - さらに * その他のオプション * をクリックしてボリュームの設定をカスタマイズし、許可、サービス品質、データ保護などのサービスを有効にすることができます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。
2. [ワークフローでステップ 2 、ステップ 2] [* ストレージ] > [共有] をクリックし、 [* 追加] をクリックして、 [* ホームディレクトリ *] を選択します。
3. Windowsクライアントで次の手順を実行して、共有にアクセスできることを確認します。
   a. エクスプローラで、次の形式で共有にドライブをマッピングします。

```
\\<SMB_Server_Name>\<Share_Name>
```

変数（%w、%d、または%u）を使用して共有名を作成した場合は、解決された名前でアクセスをテストしてください。

b. 新しく作成したドライブで、テストファイルを作成して削除します。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

  - QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
  - 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
  - ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

    このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻り、[step2]ホームディレクトリのプロビジョニングを完了します。

ONTAP System Manager で NFS を使用して Linux サーバー用の NAS ストレージをプロビジョニングする

ONTAP System Manager（9.7以降）でNFSプロトコルを使用して、Linuxサーバ用のストレージを提供するボリュームを作成します。

この手順では、に新しいボリュームを作成し"NFS対応の既存のStorage VM"ます。ボリュームの設定時にシステムのデフォルトを受け入れることも、カスタム設定を指定することもできます。

FlexVolを作成することも、高パフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。参照"FlexGroup ボリュームを作成します"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

ONTAP NFSプロトコルの機能の範囲の詳細については、を参照して"NFSプロトコルのONTAPファイルアクセスについて学ぶ"ください。

手順

1. NFS対応Storage VMに新しいボリュームを追加してください。
   a. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      NFSプロトコルが設定されているStorage VMだけが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

      - この時点で * Save * をクリックすると、 System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。

        デフォルトのエクスポートポリシーでは、すべてのユーザにフルアクセスが許可されます。

      - さらに * その他のオプション * をクリックしてボリュームの設定をカスタマイズし、許可、サービス品質、データ保護などのサービスを有効にすることができます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。
2. [step2-complete-prov, Step 2 in the workflow]] Linuxクライアントで、次の手順を実行してアクセスを確認します。
   a. Storage VMのネットワークインターフェイスを使用してボリュームを作成してマウントします。
   b. 新しくマウントしたボリュームで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

   アクセスの検証が完了したら、マウントボリュームに対して必要なUNIXの所有権と権限を設定できます"ボリュームのエクスポートポリシーを使用してクライアントアクセスを制限します"。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

- QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
- 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

  このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻り、[step2-complete-prov]NFSを使用するLinuxサーバのプロビジョニングを完了します。

ONTAPで実行するその他の方法

実行するタスク	参照先
System Managerクラシック（ONTAP 9 .7以前）	"NFSセツテイノカイヨウ"
ONTAPコマンドラインインターフェイス（CLI）	"ONTAP CLIを使用したNFS設定の詳細"

ONTAP System Manager でエクスポート ポリシーを使用してアクセスを管理する

エクスポートポリシーを使用して、LinuxクライアントからNFSサーバへのアクセスを有効にします。

この手順では、のエクスポートポリシーを作成または変更し"NFS対応の既存のStorage VM"ます。

手順

1. System Manager で、 * Storage * > * Volumes * をクリックします。
2. NFS 対応ボリュームをクリックし、 * 詳細 * をクリックします。
3. [* エクスポートポリシーの編集 *] をクリックし、 [* 既存のポリシーの選択 *] または [* 新しいポリシーの追加 *] をクリックします。

ONTAP System Manager で SMB を使用して Windows サーバー用の NAS ストレージをプロビジョニングする

ONTAP 9 .7以降で利用可能なSystem Managerを使用して、SMBプロトコルを使用して、Windowsサーバ用のストレージを提供するボリュームを作成します。

この手順では、に新しいボリュームを作成し"SMB対応の既存のStorage VM"、ボリュームのルート（/）ディレクトリの共有を作成します。ボリュームの設定時にシステムのデフォルトを受け入れることも、カスタム設定を指定することもできます。SMBの初期設定後、追加の共有を作成してそのプロパティを変更することもできます。

FlexVolを作成することも、高パフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。参照"FlexGroup ボリュームを作成します"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

ONTAP SMBプロトコルの機能の範囲の詳細については、を参照して"参照概要"ください。

開始する前に

- ONTAP 9.13.1以降では、新しいボリュームに対して容量分析とアクティビティ追跡をデフォルトで有効にすることができます。System Managerでは、クラスタレベルまたはStorage VMレベルでデフォルト設定を管理できます。詳細については、を参照してください "ファイルシステム分析を有効にする"。

手順

1. SMBが有効なStorage VMに新しいボリュームを追加します。
   a. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      SMBプロトコルが設定されているStorage VMのみが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

      - この時点で*[保存]*を選択した場合、System Managerはデフォルトのシステム設定を使用してFlexVolボリュームを作成および追加します。
      - [その他のオプション]*を選択すると、ボリュームの構成をカスタマイズして、許可、サービス品質（QoS）、データ保護などのサービスを有効にすることができます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。
2. [step2-sat-prov-win, Step 2 in the workflow]]共有がアクセス可能であることを確認するためにWindowsクライアントに切り替えます。
   a. エクスプローラで、次の形式で共有にドライブをマッピングします。
      `\\_SMB_Server_Name__Share_Name_`
   b. 新しく作成したドライブで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

アクセスを確認した後、共有 ACL を使用してクライアント アクセスを制限し、マップされたドライブに必要なセキュリティ プロパティを設定できます。詳細については、を参照してください "シェアを作成する" 。

共有を追加または変更する

SMBの初期設定後に共有を追加できます。共有は、選択したデフォルト値とプロパティを使用して作成されます。これらは後で変更できます。

共有を設定するときは、次の共有プロパティを設定できます。

- アクセス権限
- 共有プロパティ
  - Hyper-V over SMBおよびSQL Server over SMBデータを含む共有の継続的可用性を有効にする（ONTAP 9 10.1以降）。関連項目：
    - "Hyper-V over SMBノケイソクテキカヨウセイヲヒエタキヨウユウノヨウケン"
    - "SQLServeroverSMBテノケイソクテキカヨウセイヲヒエタキヨウユウ"
  - この共有へのアクセス時にSMB 3.0でデータを暗号化します。

初期設定後に、次のプロパティを変更することもできます。

- シンボリックリンク
  - シンボリックリンクとワイドリンクを有効または無効にする
- 共有プロパティ
  - クライアントにスナップショットディレクトリへのアクセスを許可します。
  - oplockを有効にして、クライアントがファイルをロックし、コンテンツをローカルにキャッシュできるようにします（デフォルト）。
  - ユーザのアクセス権限に基づいて共有リソースを表示するには、Access-Based Enumeration（ABE；アクセスベースの列挙）を有効にします。

手順

1. SMB 対応ボリュームに新しい共有を追加するには、 [ストレージ] 、 [共有] の順にクリックし、 [追加] をクリックして [共有 **] を選択します。
2. 既存の共有を変更するには、**[ストレージ]>[共有]**をクリックし、をクリックし ⋮ て[*編集]を選択します。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

  - QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。

- 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

  このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻り、[step2-compl-prov-win]SMBを使用したWindowsサーバのプロビジョニングを完了します。

ONTAPで実行するその他の方法

実行するタスク	参照先
System Managerクラシック（ONTAP 9 .7以前）	"SMBセツテイノカイヨウ"
ONTAPコマンドラインインターフェイス	"CLIヲシヨウシタSMBセツテイノカイヨウ"

ONTAP System Manager で NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングします。

NFSまたはSMBプロトコルを使用して、クライアントにストレージを提供するボリュームを作成します。

この手順では、に新しいボリュームを作成し"既存の Storage VM で NFS プロトコルと SMB プロトコルの両方が有効になっています"ます。

NFSプロトコルは、一般にLinux環境で使用されます。SMBプロトコルは、一般にWindows環境で使用されます。ただし、NFSとSMBはどちらもLinuxとWindowsのどちらでも使用できます。

FlexVolを作成することも、高パフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。見る"FlexGroup ボリュームを作成します"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

手順

1. NFSとSMBの両方が有効になっているStorage VMに新しいボリュームを追加してください。

   a. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* 追加] をクリックします。

   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      NFSプロトコルとSMBプロトコルの両方が設定されているStorage VMのみが表示されます。NFS プロトコルと SMB プロトコルが設定された Storage VM が 1 つしかない場合、「 * Storage VM * 」フィールドは表示されません。

   c. をクリックし、[NFS経由でエクスポート]*を選択します。

      デフォルトの設定では、すべてのユーザにフルアクセスが許可されます。あとでエクスポートポリシーにルールを追加できます。

   d. [* SMB / CIFS で共有] を選択します。

      共有が作成され、デフォルトのアクセス制御リスト（ ACL ）が「 Everyone 」グループに「 Full Control 」に設定されます。あとでACLに制限を追加できます。

   e. この時点で * Save * をクリックすると、 System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。

   また、許可、QoS、データ保護など、必要な追加サービスを引き続き有効にすることもできます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。

2. [step2-sed-prov-nfs-smb、ワークフローの手順2] Linuxクライアントで、エクスポートがアクセス可能であることを確認します。

   a. Storage VMのネットワークインターフェイスを使用してボリュームを作成してマウントします。

   b. 新しくマウントしたボリュームで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

3. Windowsクライアントで次の手順を実行して、共有にアクセスできることを確認します。

   a. エクスプローラで、次の形式で共有にドライブをマッピングします。
      `\\_SMB_Server_Name__Share_Name_`

   b. 新しく作成したドライブで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

   アクセスの検証が完了したら"ボリュームのエクスポートポリシーでクライアントアクセスを制限、共有ACLでクライアントアクセスを制限"、エクスポートおよび共有ボリュームに所有権と権限を設定できます。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

  - QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
  - 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
  - ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

    このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻って、[step2-compl-prov-nfs-smb]WindowsサーバおよびLinuxサーバのマルチプロトコルプロビジョニングを完了します。

ONTAPで実行するその他の方法

実行するタスク	参照するコンテンツ
System Managerクラシック（ONTAP 9 .7以前）	"SMB と NFS のマルチプロトコル構成の概要"
ONTAPコマンドラインインターフェイス	• "CLIヲシヨウシタSMBセツテイノカイヨウ" • "ONTAP CLIを使用したNFS設定の詳細" • "セキュリティスタイルとその効果について学ぶ" • "マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別"

ONTAP System Manager を使用して Kerberos でクライアント アクセスを保護する

Kerberosを有効にしてNASクライアントのストレージアクセスを保護します。

この手順では、またはに対して有効になっている既存のStorage VMでKerberosを設定し"NFS""SMB"ます。

作業を開始する前に、ストレージシステムでDNS、NTP、およびを設定しておく必要があり"LDAP"ます。

手順

1. ONTAPコマンドラインで、Storage VMのルートボリュームのUNIX権限を設定します。

   a. Storage VMのルートボリュームに対する関連する権限を表示します `volume show -volume root_vol_name-fields user,group,unix-permissions`。の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

      Storage VMのルートボリュームを次のように設定しておく必要があります。

名前	設定
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	755

   a. これらの値が表示されない場合は、コマンドを使用し `volume modify`て更新します。の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

2. Storage VMのルートボリュームのユーザ権限を設定します。

   a. ローカルUNIXユーザを表示します。 `vserver services name-service unix-user show -vserver vserver_name`の詳細については `vserver services name-service unix-user show`、を"ONTAPコマンド リファレンス"参照してください。

      Storage VMに次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザ**ID**	プライマリグループ**ID**
NFS	500	0
root	0	0

+

   ◦ 注： NFS クライアントユーザの SPN に対する Kerberos-UNIX ネームマッピングがある場合は、 nfs ユーザは必要ありません。手順 5 を参照してください。

      a. これらの値が表示されない場合は、コマンドを使用し `vserver services name-service unix-user modify`て更新します。の詳細については `vserver services name-service unix-user modify`、を"ONTAPコマンド リファレンス"参照してください。

3. Storage VMのルートボリュームのグループ権限を設定します。

   a. ローカルUNIXグループを表示します。 `vserver services name-service unix-group show -vserver vserver_name`の詳細については `vserver services name-service unix-group show`、を"ONTAPコマンド リファレンス"参照してください。

Storage VMに次のUNIXグループを設定しておく必要があります。

グループ名	グループID
デーモン	1
root	0

a. これらの値が表示されない場合は、コマンドを使用し `vserver services name-service unix-group modify`て更新します。の詳細については `vserver services name-service unix-group modify`、を"ONTAPコマンド リファレンス"参照してください。

4. System Managerに切り替えてKerberosを設定
5. System Manager で、 * Storage > Storage VM* をクリックし、 Storage VM を選択します。
6. [* 設定 *] をクリックします。
7. [Kerberos]をクリックします →
8. Kerberos Realm の下の * Add * をクリックし、次のセクションを完了します。
   - Kerberos Realmの追加

     KDCベンダーに応じて設定の詳細を入力します。
   - Realmへのネットワークインターフェイスの追加

     [* 追加] をクリックし、ネットワーク・インターフェイスを選択します。
9. 必要に応じて、Kerberosプリンシパル名からローカルユーザ名へのマッピングを追加します。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. をクリックし、[ネームマッピング]*の下をクリックします →。
   c. [KerberosからUNIX]*で、正規表現を使用してパターンと置換を追加します。

ONTAP System Managerを使用してネームサービスによるクライアントアクセスを提供する

ONTAPによるNASクライアントの認証にLDAPまたはNISを使用したホスト、ユーザ、グループ、またはネットグループ情報の検索を有効にします。

この手順では、またはが有効になっている既存のStorage VMのLDAP設定またはNIS設定を作成または変更し"NFS""SMB"ます。

LDAP設定の場合は、環境で必要なLDAP設定の詳細を確認し、デフォルトのONTAP LDAPスキーマを使用する必要があります。

手順

1. 必要なサービスを設定します。 * Storage > Storage VM* をクリックします。
2. Storage VMを選択し、*[設定]*をクリックし、[LDAP]または[NIS]のをクリックし ⚙ ます。
3. ネームサービススイッチに変更を反映します。[ネームサービススイッチ]の下にあるをクリックします。 ✎

ONTAP System Managerでディレクトリとファイルを管理する

System Managerのボリューム表示を展開して、ディレクトリとファイルを表示および削除します。

ONTAP 9 .9.1以降では、低レイテンシの非同期ディレクトリ削除機能によってディレクトリが削除されます。

ONTAP 9 .9.1以降でのファイルシステムの表示の詳細については、を参照してください"ファイルシステム分析の概要"。

ステップ

1. Storage > Volumes （ストレージ）を選択します。ボリュームを展開して内容を表示します。

ONTAP System Managerを使用してホスト固有のユーザーとグループを管理する

10.1以降では、ホストまたは**ONTAP 9**ホストに固有のユーザとグループを**System Manager**で管理できます。

次の手順を実行できます。

ウィンドウ	UNIX
• Windowsのユーザとグループの表示 • [add-edit-delete-Windows] • [manage-windows-users]	• UNIXユーザおよびグループの表示 • [add-edit-delete-UNIX] • [manage-unix-users]

Windowsのユーザとグループの表示

System Managerでは、Windowsのユーザとグループのリストを表示できます。

手順

1. System Manager で、 * Storage > Storage VM* をクリックします。
2. Storage VM を選択し、 * Settings * タブを選択します。
3. [* Host Users and Groups* （ホストユーザーとグループ * ）] 領域までスクロールします。

   「 * Windows * 」セクションには、選択した Storage VM に関連付けられている各グループのユーザ数の概要が表示されます。

4. Windows *セクションでをクリックします → 。
5. [グループ]*タブをクリックし、グループ名の横にあるをクリックすると、 ⌄ そのグループの詳細が表示されます。
6. グループ内のユーザーを表示するには、グループを選択し、 * ユーザー * タブをクリックします。

Windowsグループの追加、編集、削除

System Managerでは、Windowsグループを追加、編集、または削除して管理できます。

手順

1. System Managerで、Windowsグループのリストを表示します。を参照してください Windowsのユーザとグループの表示。
2. [* グループ *] タブでは、次のタスクを使用してグループを管理できます。

実行する処理	実行する手順
グループを追加します	1. をクリックします。 + Add 2. グループ情報を入力します。 3. 権限を指定します。 4. グループメンバーを指定します（ローカルユーザ、ドメインユーザ、またはドメイングループを追加します）。
グループを編集します	1. グループ名の横にあるをクリックし ⋮、*[編集]*をクリックします。 2. グループ情報を変更します。
グループを削除します	1. 削除するグループの横にあるチェックボックスをオンにします。 2. をクリックします。 Delete *注：*グループ名の横にあるをクリックし、*削除*をクリックして、1つのグループを削除することもできます ⋮ 。

Windowsユーザの管理

System Managerでは、Windowsユーザの追加、編集、削除、有効化、無効化を行うことができます。Windowsユーザのパスワードを変更することもできます。

手順

1. System Managerで、グループのユーザのリストを表示します。を参照してください Windowsのユーザとグループの表示。
2. [**Users**] タブでは、次のタスクを実行してユーザを管理できます。

実行する処理	実行する手順
ユーザを追加します	1. をクリックします。 + Add 2. ユーザ情報を入力します。
ユーザを編集します	1. ユーザ名の横にあるをクリックし ⋮、*[編集]*をクリックします。 2. ユーザ情報を変更します。

ユーザを削除します	1. 削除するユーザの横にあるチェックボックスをオンにします。 2. をクリックします。 Delete *注：*ユーザー名の横にあるをクリックし、*削除*をクリックして、1人のユーザーを削除することもできます 。
ユーザパスワードを変更します	1. ユーザ名の横にあるをクリックし 、*[パスワードの変更]*をクリックします。 2. 新しいパスワードを入力し、確認のためにもう一度入力します。
ユーザを有効にします	1. 有効にする無効になっている各ユーザの横にあるチェックボックスをオンにします。 2. をクリックします Enable
ユーザを無効にします	1. 無効にする有効な各ユーザの横にあるチェックボックスをオンにします。 2. をクリックします Disable

UNIXユーザおよびグループの表示

System Managerでは、UNIXユーザおよびグループのリストを表示できます。

手順

1. System Manager で、 * Storage > Storage VM* をクリックします。
2. Storage VM を選択し、 * Settings * タブを選択します。
3. [* Host Users and Groups* （ホストユーザーとグループ * ）] 領域までスクロールします。

   「 * unix * 」セクションには、選択した Storage VM に関連付けられた各グループのユーザ数の概要が表示されます。

4. [UNIX]セクションでをクリックします 。
5. [* グループ *] タブをクリックすると、そのグループの詳細が表示されます。
6. グループ内のユーザーを表示するには、グループを選択し、 * ユーザー * タブをクリックします。

UNIXグループを追加、編集、または削除する

System Managerでは、UNIXグループを追加、編集、または削除して管理できます。

手順

1. System Managerで、UNIXグループのリストを表示します。を参照してください UNIXユーザおよびグループの表示。

2. [* グループ *] タブでは、次のタスクを使用してグループを管理できます。

実行する処理	実行する手順
グループを追加します	1. をクリックします。 + Add 2. グループ情報を入力します。 3. （任意）関連付けられているユーザを指定します。
グループを編集します	1. グループを選択します。 2. をクリックします。 Edit 3. グループ情報を変更します。 4. （オプション）ユーザを追加または削除します。
グループを削除します	1. 削除するグループを選択します。 2. をクリックします。 Delete

UNIXユーザを管理します。

System Managerでは、Windowsユーザを追加、編集、削除して管理できます。

手順

1. System Managerで、グループのユーザのリストを表示します。を参照してください UNIXユーザおよびグループの表示。
2. [**Users**] タブでは、次のタスクを実行してユーザを管理できます。

実行する処理	実行する手順
ユーザを追加します	1. をクリックします。 + Add 2. ユーザ情報を入力します。
ユーザを編集します	1. 編集するユーザを選択します。 2. をクリックします。 Edit 3. ユーザ情報を変更します。
ユーザを削除します	1. 削除するユーザを選択します。 2. をクリックします。 Delete

ONTAP System ManagerでNFSアクティブクライアントを監視する

ONTAP 9 8以降では、クラスタでNFSのライセンスが有効な場合に、アクティブなNFSクライアント接続がSystem Managerに表示されます。

これにより、どのNFSクライアントがStorage VMにアクティブに接続しているか、どのNFSクライアントがアイドル状態であるか、どのNFSクライアントが切断されているかを簡単に確認できます。

NFS クライアントの各 IP アドレスについて、 * nfs clients * display show に * Time of last access * Network interface IP address * nfs connection version * Storage VM name と表示されます

また、過去 48 時間にアクティブだった NFS クライアントのリストが * Storage > Volumes * の表示にも表示され、 NFS クライアントの数は * Dashboard * 表示にも表示されます。

ステップ

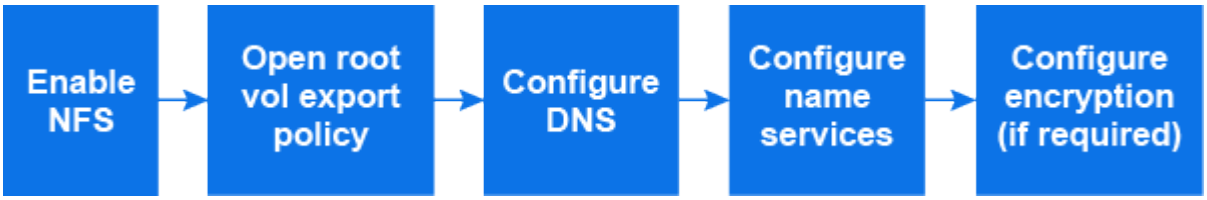
1. NFS クライアントアクティビティを表示します。 [*Hosts] > [NFS Clients] をクリックします。

NASストレージの有効化

ONTAP System Managerで**NFS**を使用して**Linux**サーバー用の**NAS**ストレージを有効にする

Storage VMを作成または変更して、Linuxクライアントにデータを提供するためのNFSサーバを有効にします。

次の手順を使用して、NFSプロトコル用に新規または既存のStorage VMを有効にします。



開始する前に

環境で必要なネットワークサービス、認証サービス、またはセキュリティサービスの設定の詳細をメモしておいてください。

手順

1. Storage VMでNFSを有効にします。
   - 新しいStorage VMの場合：**[ストレージ]>[Storage VM]***をクリックし、[追加]をクリックして**Storage VM**名を入力し、[SMB / CIFS、NFS、S3]タブで[NFSの有効化]*を選択します。
     i. デフォルトの言語を確認します。
     ii. ネットワークインターフェイスを追加
     iii. Storage VM管理者アカウント情報の更新（オプション）
   - 既存のStorage VMの場合：**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[NFS]*の下をクリックし ⚙ ます。
2. Storage VMルートボリュームのエクスポートポリシーを開きます。
   a. [ストレージ]>[ボリューム]をクリックし、**Storage VM**のルートボリューム（デフォルトでは**_volume-name__root**）を選択して、[エクスポートポリシー]*に表示されるポリシーをクリックします。
   b. [追加]*をクリックしてルールを追加します。
      - クライアント仕様= `0.0.0.0/0`

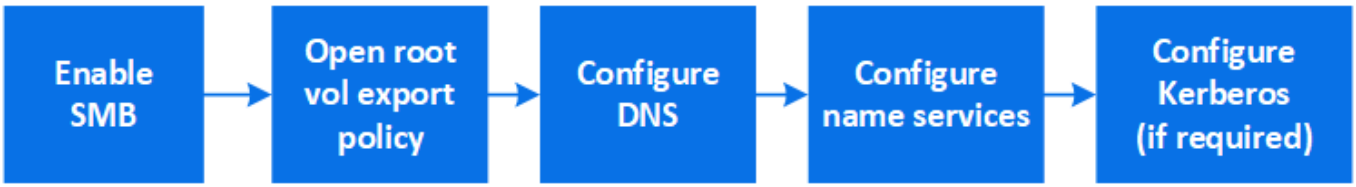
- アクセスプロトコル= NFS
- アクセスの詳細 = UNIX読み取り専用

3. ホスト名解決に使用するDNSを設定します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[DNS]*の下をクリックし ます。
4. ネームサービスを必要に応じて設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックし、[LDAP]または[NIS]をクリックします 。
   b. [ネームサービススイッチ]タイル内をクリックし て変更を反映します。
5. 必要に応じてKerberosを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
   b. [Kerberos]タイル内をクリックし 、*[追加]*をクリックします。

ONTAP System Managerで**SMB**を使用して**Windows**サーバの**NAS**ストレージを有効にする

Windowsクライアントにデータを提供するためのSMBサーバを有効にするために、Storage VMを作成または変更します。

この手順では、新規または既存のStorage VMでSMBプロトコルを有効にします。環境で必要なネットワークサービス、認証サービス、またはセキュリティサービスについて、設定の詳細が提供されていることを前提としています。



手順

1. Storage VMでSMBを有効にします。
   a. 新しいStorage VMの場合：* Storage > Storage VM*をクリックし、* Add をクリックして**Storage VM**名を入力し、 SMB / CIFS、NFS、S3 タブで SMB / CIFSの有効化*を選択します。
      - 次の情報を入力します。
        - 管理者の名前とパスワード
        - サーバ名
        - Active Directoryドメイン
      - 組織単位を確定します。
      - DNS値を確定します。
      - デフォルトの言語を確認します。
      - ネットワークインターフェイスを追加
      - Storage VM管理者アカウント情報の更新（オプション）
   b. 既存のStorage VMの場合：**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]

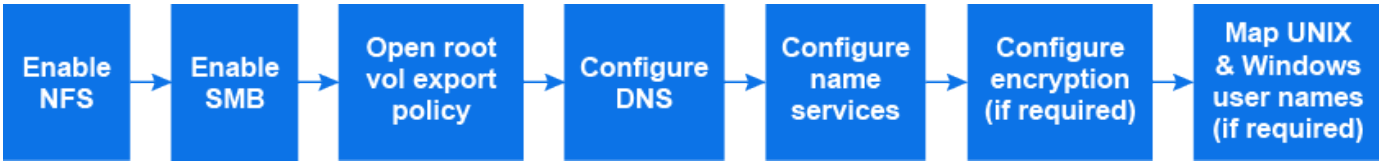
をクリックし、[SMB]*の下をクリックし ます。

2. Storage VMルートボリュームのエクスポートポリシーを開きます。
   a. [ストレージ]>[ボリューム]をクリックし、**Storage VM**のルートボリューム（デフォルトでは**_volume-name_root_**）を選択し、[エクスポートポリシー]*に表示されるポリシーをクリックします。
   b. [追加]*をクリックしてルールを追加します。
      - クライアント仕様= `0.0.0.0/0`
      - アクセスプロトコル = SMB
      - アクセスの詳細= NTFS読み取り専用
3. ホスト名解決に使用するDNSを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]をクリックし、[DNS]*の下をクリックします 。
   b. DNSサーバに切り替えてSMBサーバをマッピングします。
      - フォワードルックアップ（A -アドレスレコード）とリバースルックアップ（PTR -ポインタレコード）のエントリを作成して、SMBサーバ名をデータネットワークインターフェイスのIPアドレスにマッピングします。
      - NetBIOSエイリアスを使用する場合は、エイリアスの正規名（CNAMEリソースレコード）ルックアップエントリを作成して、各エイリアスをSMBサーバのデータネットワークインターフェイスのIPアドレスにマッピングします。
4. ネームサービスを必要に応じて設定
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]をクリックし、[LDAP]または[NIS]*の下をクリックします 。
   b. ネームサービススイッチファイルに変更を反映します。*[ネームサービススイッチ]*の下にあるをクリックします 。
5. 必要に応じてKerberosを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
   b. でをクリックし、[追加]*をクリックし ます。

ONTAP System Manager で **NFS** と **SMB** の両方を使用して **Windows** と **Linux** の両方で **NAS** ストレージを有効にする

Storage VMを作成または変更して、NFSサーバとSMBサーバがLinuxクライアントとWindowsクライアントにデータを提供できるようにします。

この手順を使用して、新規または既存のStorage VMがNFSプロトコルとSMBプロトコルの両方を提供できるようにします。



開始する前に

環境で必要なネットワークサービス、認証サービス、またはセキュリティサービスの設定の詳細をメモしてお

いてください。

手順

1. Storage VMでNFSとSMBを有効にします。
   a. 新しいStorage VMの場合：* Storage > Storage VM*をクリックし、* Add をクリックして**Storage VM**名を入力し、 SMB / CIFS、NFS、S3 タブで SMB / CIFSの有効化*と* NFSの有効化*を選択します。
   b. 次の情報を入力します。
      - 管理者の名前とパスワード
      - サーバ名
      - Active Directoryドメイン
   c. 組織単位を確定します。
   d. DNS値を確定します。
   e. デフォルトの言語を確認します。
   f. ネットワークインターフェイスを追加
   g. Storage VM管理者アカウント情報の更新（オプション）
   h. 既存のStorage VMの場合：* Storage > Storage VM*をクリックし、Storage VMを選択して* Settings *をクリックします。NFSまたはSMBがまだ有効になっていない場合は、次のサブ手順を実行します。
      - [NFS]*の下にあるをクリックします 。
      - [SMB]*でをクリックします 。
2. Storage VMルートボリュームのエクスポートポリシーを開きます。
   a. [ストレージ]>[ボリューム]をクリックし、**Storage VM**のルートボリューム（デフォルトでは**_volume-name_root_**）を選択し、[エクスポートポリシー]*に表示されるポリシーをクリックします。
   b. [追加]*をクリックしてルールを追加します。
      - クライアント仕様= `0.0.0.0/0`
      - アクセスプロトコル= NFS
      - アクセスの詳細 = NFS読み取り専用
3. ホスト名解決に使用するDNSを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]をクリックし、[DNS]*の下をクリックします 。
   b. DNSの設定が完了したら、DNSサーバに切り替えてSMBサーバをマッピングします。
      - フォワードルックアップ（A -アドレスレコード）とリバースルックアップ（PTR -ポインタレコード）のエントリを作成して、SMBサーバ名をデータネットワークインターフェイスのIPアドレスにマッピングします。
      - NetBIOSエイリアスを使用する場合は、エイリアスの正規名（CNAMEリソースレコード）ルックアップエントリを作成して、各エイリアスをSMBサーバのデータネットワークインターフェイスのIPアドレスにマッピングします。
4. ネームサービスを必要に応じて設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックし、[LDAP]または[NIS]をクリックし ます。

b. ネームサービススイッチファイルに変更を反映します。*[ネームサービススイッチ]*の下にあるをクリックします 。

5. 必要に応じてKerberosを設定します。

a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。

b. [Kerberos]タイル内をクリックし 、*[追加]*をクリックします。

6. 必要に応じてUNIXとWindowsのユーザ名をマッピングします。**[**ネームマッピング**]***でをクリックし、[追加]*をクリックし ます。

この処理は、WindowsとUNIXのユーザアカウントが暗黙的にマッピングされない場合にのみ実行します。小文字のWindowsユーザ名がUNIXユーザ名と一致している場合は、この処理を実行します。ユーザ名は、LDAP、NIS、またはローカルユーザを使用してマッピングできます。一致しないユーザセットが2つある場合は、ネームマッピングを設定する必要があります。

CLIを使用したNFSの設定

ONTAP CLIを使用したNFS設定の詳細

ONTAP 9 CLIコマンドを使用して、新規または既存のStorage Virtual Machine（SVM）の新しいボリュームまたはqtreeに格納されているファイルへのNFSクライアントアクセスを設定できます。

次の手順は、ボリュームまたはqtreeへのアクセスを設定する場合に使用します。

- ONTAPで現在サポートされている次のいずれかのバージョンを使用する必要がある：NFSv3、NFSv4、NFSv4.1、NFSv4.2、またはpNFSを含むNFSv4.1。
- System Managerや自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

  System Managerを使用してNASマルチプロトコルアクセスを設定する方法については、を参照してください"NFSとSMBの両方を使用したWindowsとLinux用のNASストレージのプロビジョニング"。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

  コマンド構文の詳細については、を"ONTAPコマンド リファレンス"参照してください。

- 新しいボリュームはUNIXファイル権限を使用して保護されます。
- SVM管理者Privilegesではなく、クラスタ管理者Privilegesが必要です。

ONTAP NFSプロトコルの機能の範囲の詳細については、を参照して"NFSプロトコルのONTAPファイルアクセスについて学ぶ"ください。

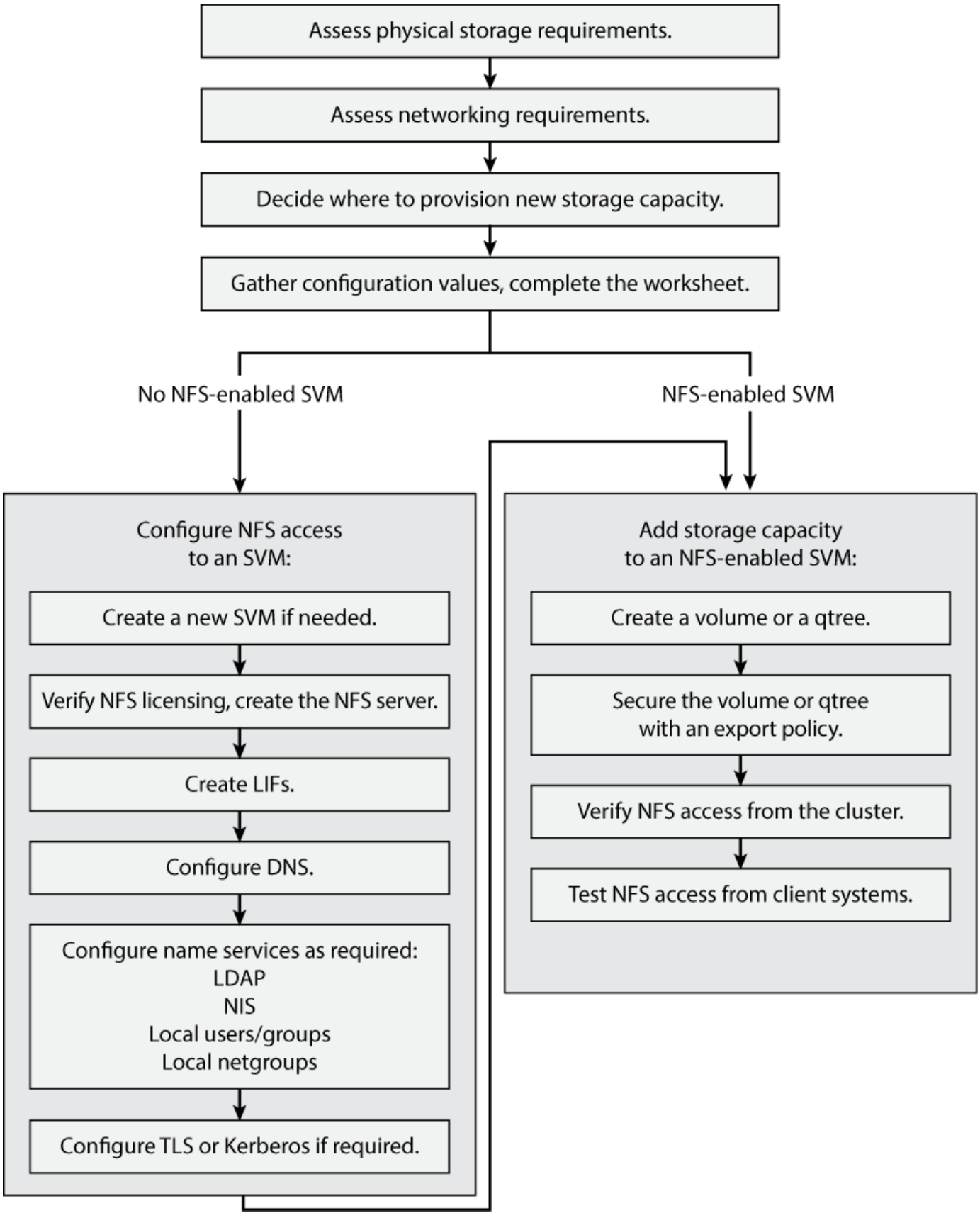
ONTAPで実行するその他の方法

実行するタスク	参照先
再設計されたSystem Manager（ONTAP 9 .7以降で使用可能）	"NFSを使用したLinuxサーバ用のNASストレージのプロビジョニング"

System Manager Classic（ONTAP 9 .7以前で使用可能）	"NFSセツテイノカイヨウ"

ONTAP NFS構成ワークフローについて学ぶ

NFSを設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存のSVMへのNFSアクセスを設定するか、すでにNFSアクセスの設定が完了している既存のSVMにボリュームまたはqtreeを追加するかによってワークフローが異なります。


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

準備

ONTAP NFS物理ストレージ要件の評価

クライアント用のNFSストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリューム用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。

   ```
   storage aggregate show
   ```

   十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. 十分なスペースを備えたアグリゲートがない場合は、コマンドを使用して既存のアグリゲートにディスクを追加する `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成し `storage aggregate create`ます。

関連情報

- "ローカル階層（アグリゲート）へのディスクの追加"
- "storage aggregate add-disks"
- "storage aggregate create"

ONTAP NFSネットワーク構成要件を評価する

クライアントにNFSストレージを提供する前に、ネットワークが正しく設定されてNFSのプロビジョニング要件を満たしていることを確認する必要があります。

開始する前に

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）
- 外部ファイアウォール

手順

1. 使用可能な物理ポートと仮想ポートを表示します。

   `network port show`

   - 可能な場合は、データネットワークの速度が最も速いポートを使用してください。
   - 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。
   - の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

2. サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットが存在し、十分な数のアドレスが使用可能であることを確認してください： +

   `network subnet show`

   の詳細については `network subnet show`、を"ONTAPコマンド リファレンス"参照してください。

   サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。

   の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

3. 使用可能なIPspaceを表示します。

   `network ipspace show`

   デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

   の詳細については `network ipspace show`、を"ONTAPコマンド リファレンス"参照してください。

4. IPv6アドレスを使用する場合は、IPv6がクラスタで有効になっていることを確認します。

   `network options ipv6 show`

   必要に応じて、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

   および `network options ipv6 modify`の詳細については `network options ipv6 show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP NFSストレージ容量プロビジョニングの詳細

新しいNFSボリュームまたはqtreeを作成する前に、そのボリュームを新規、既存のどちらのSVMに配置するかを決め、配置先のSVMでどのような設定が必要になるかを確認しておく必要があります。それによって以降のワークフローが決まります。

選択肢

- 新しいSVM、またはNFSが有効になっているが設定はまだ完了していない既存のSVMにボリュームまたはqtreeをプロビジョニングする場合は、「SVMへのNFSアクセスの設定」と「NFS対応SVMへのNFSストレージの追加」の両方の手順を実行します。

  SVMへのNFSアクセスの設定

  NFS対応SVMへのNFSストレージの追加

  次のいずれかに該当する場合は、新しいSVMを作成します。

  - クラスタでNFSを初めて有効にする場合。
  - クラスタ内の既存のSVMでNFSサポートを有効にするのが望ましくない場合。
  - クラスタ内に NFS 対応の SVM が 1 つ以上あり、分離されたネームスペースに別の NFS サーバが必要な場合（マルチテナンシーシナリオ）。NFSが有効になっているものの設定されていない既存のSVMでストレージをプロビジョニングする場合にも、このオプションを選択する必要があります。これが当てはまるのは、SANアクセス用のSVMを作成している場合や、SVM作成時にどのプロトコルも有効になっていなかった場合です。

  SVMでNFSを有効にしたあとに、ボリュームまたはqtreeのプロビジョニングに進みます。

- NFSアクセスの設定が完了している既存のSVMでボリュームまたはqtreeをプロビジョニングする場合は、「NFS対応SVMへのストレージ容量の追加」の手順を完了します。

  NFS対応SVMへのストレージ容量の追加

ONTAP NFS設定ワークシート

NFS設定ワークシートを使用すると、クライアントのNFSアクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所に関する決定に応じて、ワークシートのいずれかまたは両方のセクションを完了する必要があります。

SVMへのNFSアクセスを設定する場合は、両方のセクションを完了する必要があります。

- SVMへのNFSアクセスの設定
- NFS対応SVMへのストレージ容量の追加

NFS対応SVMにストレージ容量を追加する場合は、次の操作のみを完了する必要があります。

- NFS対応SVMへのストレージ容量の追加

- SVM を作成するためのパラメータ *

新しいSVMを作成する場合は、コマンドで次の値を指定します `vserver create`。

フィールド	説明	あなたの価値
`-vserver`	新しいSVMの名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意のSVM名を適用する別の命名規則に従います。	
`-aggregate`	新しいNFSストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-rootvolume`	SVMルート ボリュームの一意の名前を指定します。	
`-rootvolume-security-style`	SVMのUNIXセキュリティ形式を使用します。	`unix`
`-language`	このワークフローではデフォルトの言語設定を使用します。	`C.UTF-8`
`ipspace`	IPspace は、 Storage Virtual Machine （ SVM ）が属する個別の IP アドレススペースです。	

- NFS サーバ作成用のパラメータ *

新しいNFSサーバを作成し、サポートされているNFSバージョンを指定する場合は、コマンドで次の値を指定し `vserver nfs create`ます。

NFSv4以降を有効にする場合は、セキュリティを強化するためにLDAPを使用する必要があります。

フィールド	説明	あなたの価値
`-v3 -v4.0`、、、 `-v4.1 -v4.1 -pnfs`	必要に応じてNFSバージョンを有効にします。 が有効になっている場合は、ONTAP 9 .8以降でもv4.2がサポートされ `v4.1`ます。	

`-v4-id-domain`	IDマッピングドメイン名。	
`-v4-numeric-ids`	所有者IDの数値のサポート（有効または無効）。	

* LIF 作成用のパラメータ *

LIFを作成する場合は、コマンドで次の値を指定します `network interface create`。の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

Kerberosを使用する場合は、複数のLIFでKerberosを有効にする必要があります。

フィールド	説明	あなたの価値
`-lif`	新しいLIFの名前を指定します。	
`-role`	このワークフローではデータLIFのロールを使用します。	`data`
`-data-protocol`	このワークフローではNFSプロトコルのみを使用します。	`nfs`
`-home-node`	LIFに対してコマンドを実行したときにLIFが戻るノード `network interface revert`。 の詳細については `network interface revert`、を"ONTAPコマンド リファレンス"参照してください。	
`-home-port`	LIFに対してコマンドを実行したときにLIFが戻るポートまたはインターフェイスグループ `network interface revert`。	
`-address`	新しいLIFによるデータアクセスに使用する、クラスタ上のIPv4アドレスまたはIPv6アドレスを指定します。	
`-netmask`	LIFのネットワークマスクとゲートウェイ。	

-subnet	IPアドレスのプール。および -netmask`の代わりに使用して `-address、アドレスとネットマスクを自動的に割り当てます。	
-firewall-policy	このワークフローではデフォルトのデータファイアウォールポリシーを使用します。	data

- DNS ホスト名解決のパラメータ *

DNSを設定する場合は、コマンドで次の値を指定します vserver services name-service dns create。

フィールド	説明	あなたの価値
-domains	最大5つのDNSドメイン名。	
-name-servers	DNSネームサーバごとに最大3つのIPアドレス。	

ネームサービス情報

- ローカルユーザー作成用のパラメータ *

コマンドを使用してローカルユーザを作成する場合は、次の値を指定し `vserver services name-service unix-user create`ます。Uniform Resource Identifier（URI）からUNIXユーザを含むファイルをロードしてローカルユーザを設定する場合は、これらの値を手動で指定する必要はありません。

	ユーザ名 (-user)	ユーザID (-id)	グループID (-primary-gid)	フルネーム (-full-name)
例	johnm	123	100	John Miller
1				
2				
3				
…				
n				

- ローカルグループを作成するためのパラメータ *

コマンドを使用してローカルグループを作成する場合は、次の値を指定し `vserver services name-service

unix-group create`ます。UNIXグループを含むファイルをURIからロードしてローカルグループを設定する場合は、これらの値を手動で指定する必要はありません。

	グループ名(-name)	グループID(-id)
例	エンジニアリング	100
1		
2		
3		
…		
n		

- NISのパラメータ*

コマンドでは、次の値を指定します `vserver services name-service nis-domain create`。

。 `-nis-servers` NIS サーバーのホスト名または IP アドレスを指定するフィールド。

フィールド	説明	あなたの価値
`-domain`	SVMが名前検索に使用するNISドメインを指定します。	
`-active`	アクティブなNISドメインサーバを指定します。	`true`または `false`
`-nis-servers`	ドメイン設定で使用するNISサーバのIPアドレスおよびホスト名をカンマで区切って指定します。	

- LDAPのパラメータ*

コマンドでは、次の値を指定します `vserver services name-service ldap client create`。

また、自己署名ルートCA証明書ファイルも必要 `.pem`です。

フィールド	説明	あなたの価値
`-vserver`	LDAPクライアント設定を作成するSVMの名前を指定します。	

フィールド	説明	あなたの価値
-client-config	新しいLDAPクライアント設定に割り当てる名前。	
-ldap-servers	LDAPサーバのIPアドレスおよびホスト名をカンマで区切って指定します。	
-query-timeout	このワークフローのデフォルトの秒数を使用し `3`ます。	3
-min-bind-level	最小バインド認証レベルを指定します。デフォルトはです anonymous。署名と封印が設定されている場合はに設定する必要があります sasl。	
-preferred-ad-servers	1つ以上の優先Active Directoryサーバ（カンマで区切ったIPアドレス）	
-ad-domain	Active Directoryドメイン。	
-schema	使用するスキーマテンプレート。デフォルトまたはカスタムのスキーマを使用できます。	
-port	このワークフローにはデフォルトのLDAPサーバポートを使用し `389`ます。	389
-bind-dn	バインドユーザの識別名。	
-base-dn	ベース識別名。デフォルトは（root）です ""。	
-base-scope	このワークフローのデフォルトのベース検索範囲を使用します subnet。	subnet
-session-security	LDAPの署名または署名と封印を有効にします。デフォルトはです none。	
-use-start-tls	LDAP over TLSを有効にします。デフォルトはです false。	

• Kerberos 認証のパラメータ *

コマンドでは、次の値を指定します `vserver nfs kerberos realm create`。一部の値は、Microsoft Active DirectoryをKey Distribution Center（KDC；キー配布センター）サーバとして使用するか、MITまたはその他のUNIX KDCサーバとして使用するかによって異なります。

フィールド	説明	あなたの価値
`-vserver`	KDCと通信するSVMを指定します。	
`-realm`	Kerberos Realmを指定します。	
`-clock-skew`	クライアントとサーバ間で許容されるクロックスキュー。	
`-kdc-ip`	KDCのIPアドレス。	
`-kdc-port`	KDCポート番号。	
`-adserver-name`	Microsoft KDC のみ： AD サーバ名を指定します。	
`-adserver-ip`	Microsoft KDC のみ： AD サーバの IP アドレスを指定します。	
`-adminserver-ip`	UNIX KDC のみ：管理サーバの IP アドレスを指定します。	
`-adminserver-port`	UNIX KDC のみ：管理サーバのポート番号を指定します。	
`-passwordserver-ip`	UNIX KDC のみ：パスワードサーバの IP アドレスを指定します。	
`-passwordserver-port`	UNIX KDC のみ：パスワードサーバのポートを指定します。	
`-kdc-vendor`	KDCベンダー。	`{Microsoft`
`Other}`	`-comment`	必要なコメントを指定します。

コマンドでは、次の値を指定します `vserver nfs kerberos interface enable`。

フィールド	説明	あなたの価値

-vserver	Kerberos設定を作成するSVMの名前を指定します。	
-lif	Kerberosを有効にするデータLIFを指定します。Kerberosは複数のLIFで有効にすることができます。	
-spn	サービスプリンシパル名（SPN）	
-permitted-enc-types	Kerberos over NFSで許可される暗号化タイプ。クライアントの機能に応じて推奨されます。 aes-256	
-admin-username	KDCからSPNシークレットキーを直接取得するためのKDC管理者のクレデンシャル。パスワードは必須です	
-keytab-uri	KDC管理者のクレデンシャルがない場合は、SPNキーが含まれているKDCのkeytabファイル。	
-ou	Microsoft KDCのRealmを使用してKerberosを有効にした場合にMicrosoft Active Directoryサーバアカウントが作成される組織単位（OU）。	

NFS対応SVMへのストレージ容量の追加

- エクスポートポリシーおよびルールを作成するためのパラメータ *

コマンドでは、次の値を指定します vserver export-policy create。

フィールド	説明	あなたの価値
-vserver	新しいボリュームをホストするSVMの名前を指定します。	
-policyname	新しいエクスポートポリシーの名前を指定します。	

コマンドでは、ルールごとに次の値を指定し `vserver export-policy rule create`ます。

フィールド	説明	あなたの価値
-clientmatch	クライアント一致を指定します。	

`-ruleindex`	ルールリスト内でのエクスポートルールの位置。	
`-protocol`	このワークフローではNFSを使用します。	`nfs`
`-rorule`	読み取り専用アクセスの認証方式を指定します。	
`-rwrule`	読み取り / 書き込みアクセスの認証方式を指定します。	
`-superuser`	スーパーユーザ アクセスの認証方式を指定します。	
`-anon`	匿名ユーザをマッピングするユーザIDを指定します。	

エクスポート ポリシーごとにルールを1つ以上作成する必要があります。

-ruleindex	**-clientmatch**	**-rorule**	**-rwrule**	**-superuser**	**-anon**
例	0.0.0.0/0、@rootaccess_netgroup	任意	krb5	sys	65534
1					
2					
3					
…					
n					

- ボリュームを作成するためのパラメータ *

qtreeではなくボリュームを作成する場合は、コマンドで次の値を指定します `volume create`。

フィールド	説明	あなたの価値
`-vserver`	新しいボリュームをホストする新規または既存のSVMの名前を指定します。	

`-volume`	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
`-aggregate`	新しいNFSボリュームに対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-size`	新しいボリュームのサイズとして任意の整数を指定します。	
`-user`	ボリュームのルートの所有者に設定するユーザの名前またはIDを指定します。	
`-group`	ボリュームのルートの所有者に設定するグループの名前またはIDを指定します。	
`--security-style`	このワークフローにはUNIXセキュリティ形式を使用します。	`unix`
`-junction-path`	新しいボリュームのマウント先とする、ルート（/）の下の場所を指定します。	
`-export-policy`	既存のエクスポート ポリシーを使用する場合は、ボリュームの作成時に名前を入力できます。	

- qtree を作成するためのパラメータ *

ボリュームではなくqtreeを作成する場合は、コマンドで次の値を指定します `volume qtree create`。

フィールド	説明	あなたの価値
`-vserver`	qtreeを含むボリュームが配置されているSVMの名前。	
`-volume`	新しいqtreeを格納するボリュームの名前。	
`-qtree`	新しいqtreeには、64文字以下の一意のわかりやすい名前を指定します。	

`-qtree-path`	ボリュームとqtreeを別 々 の引数として指定する代わりに、qtreeパスをの形式で `/vol/*volume_name/qtree_name*\>` 指定できます。	
`-unix-permissions`	オプション： qtree の UNIX 権限を指定します。	
`-export-policy`	既存のエクスポートポリシーを使用する場合は、qtreeの作成時に名前を入力できます。	

関連情報

- "ONTAPコマンド リファレンス"

SVMへのNFSアクセスの設定

NFSデータアクセス用の**ONTAP SVM**を作成する

クラスタ内にNFSクライアントにデータ アクセスを提供するSVMが1つもない場合は、作成する必要があります。

開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

手順

1. SVMを作成します。

   ```
   vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
   ipspace_name
   ```

   - オプションにはUNIX設定を使用し `-rootvolume-security-style`ます。
   - デフォルトのC.UTF-8オプションを使用し `-language`ます。
   - この `ipspace`設定はオプションです。

2. 新しく作成したSVMの設定とステータスを確認します。

   ```
   vserver show -vserver vserver_name
   ```

   `Allowed Protocols`フィールドには
   `nfs`を指定する必要があります。このリストは後で編集できます。

`Vserver Operational State`フィールドには状態が表示されている必要があり`running`ます。状態が表示された場合は`initializing`、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

例

次のコマンドは、データアクセス用のSVMをIPspace ipspaceAに作成します。

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて状態になっていることを示しています running。ルートボリュームには、ルールが含まれていないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

ONTAP SVM での **NFS** プロトコルの有効化を確認する

SVMでNFSを設定して使用する前に、このプロトコルが有効になっていることを確認する必要があります。

タスクの内容

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、コマンドを使用してあとから有効にすることができます `vserver add-protocols`。

作成したプロトコルは、 LIF から追加または削除することはできません。

コマンドを使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols`。

手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルを確認します。

   ```
   vserver show -vserver vserver_name -protocols
   ```

   コマンドを使用して、クラスタ内のすべてのSVMで現在有効になっているプロトコルを表示することもできます `vserver show-protocols`。

2. 必要に応じて、プロトコルを有効または無効にします。

   - NFSプロトコルを有効にするには+
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - プロトコルを無効にするには：+
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`

3. 有効 / 無効なプロトコルが正しく更新されたことを確認します。

   ```
   vserver show -vserver vserver_name -protocols
   ```

例

次のコマンドは、 vs1 という SVM で現在有効 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

次のコマンドは、vs1というSVMで有効になっているプロトコルのリストにを追加することで、NFS経由のアクセスを許可し `nfs`ます。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

ONTAP SVM 上の **NFS** クライアント アクセスを開く

SVMルートボリュームのデフォルトのエクスポートポリシーには、すべてのクライアントにNFS経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVMとそのボリュームに対するNFSクライアントのアクセスがすべて拒否されます。

タスクの内容

新しいSVMが作成されると、デフォルトのエクスポートポリシー（default）がSVMのルートボリュームに対して自動的に作成されます。SVM上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを1つ以上作成する必要があります。

デフォルトのエクスポートポリシーですべてのNFSクライアントにアクセスが許可されていることを確認してから、個 々 のボリュームまたはqtreeにカスタムのエクスポートポリシーを作成して個 々 のボリュームへの

アクセスを制限する必要があります。

手順

1. 既存のSVMを使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。

   ```
   vserver export-policy rule show
   ```

   次のようなコマンド出力が表示されます。

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                       Vserver: vs1.example.com
                                   Policy Name: default
                                    Rule Index: 1
                               Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                      Superuser Security Types: any
                  Honor SetUID Bits in SETATTR: true
                     Allow Creation of Devices: true
   ```

   オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVM ルートボリュームのエクスポートルールを作成します。

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Kerberosで保護されたボリュームのみをSVMに格納する場合は、ルートボリュームのエクスポートルールオプション、 `-rwrule`、、を `-superuser`または `krb5i`に `krb5`設定できます `-rorule`。例：

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. コマンドを使用してルールの作成を確認します `vserver export-policy rule show`。

結果

これで、SVMで作成されたすべてのボリュームまたはqtreeに、すべてのNFSクライアントからアクセスできるようになります。

ONTAP NFSサーバーを作成する

クラスタでNFSのライセンスが有効であることを確認したら、コマンドを使用してSVM

にNFSサーバを作成し、サポートするNFSのバージョンを指定できます `vserver nfs create`。

タスクの内容

SVM は、 NFS の 1 つ以上のバージョンをサポートするように設定できます。NFSv4以降をサポートしている場合：

- NFSv4ユーザIDマッピングのドメイン名は、NFSv4サーバとターゲットクライアントで同じである必要があります。

  NFSv4サーバとクライアントで同じ名前を使用しているかぎり、LDAPまたはNISドメイン名と同じにする必要はありません。

- ターゲットクライアントがNFSv4数値ID設定をサポートしている必要があります。
- セキュリティ上の理由から、NFSv4環境でのネームサービスにはLDAPを使用する必要があります。

開始する前に

SVM を、 NFS プロトコルを許可するように設定しておく必要があります。

手順

1. クラスタ上でNFSのライセンスが有効であることを確認します。

   ```
   system license show -package nfs
   ```

   サポートされていない場合は、営業担当者にお問い合わせください。

2. NFSサーバを作成します。

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   NFSバージョンは任意に組み合わせて有効にすることができます。pNFSをサポートする場合は、オプションと `-v4.1-pnfs`オプションの両方を有効にする必要があります `-v4.1`。

   v4以降を有効にする場合は、次のオプションが正しく設定されていることも確認してください。

   - `-v4-id-domain`

     （オプション）このパラメータは、NFSv4プロトコルで定義されているユーザ名およびグループ名のドメイン部分を指定します。デフォルトでは、NISドメインが設定されている場合はONTAPが使用し、設定されていない場合はDNSドメインが使用されます。ターゲットクライアントで使用されるドメイン名と一致する値を指定する必要があります。

   - `-v4-numeric-ids`

     （オプション）このパラメータは、NFSv4の所有者属性で数値IDのサポートを有効にするかどうかを指定します。デフォルト設定はenabledですが、ターゲットクライアントがこの設定をサポートしていることを確認する必要があります。

   NFSのその他の機能を有効にするには、コマンドを使用し `vserver nfs modify`ます。

3. NFSが実行されていることを確認します。

   `vserver nfs status -vserver vserver_name`

4. NFSが必要に応じて設定されていることを確認します。

   `vserver nfs show -vserver vserver_name`

例

次のコマンドは、 NFSv3 と NFSv4.0 が有効な vs1 という名前の SVM 上に NFS サーバを作成します。

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

次のコマンドは、vs1という名前の新しいNFSサーバのステータスと設定値を確認します。

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                                Vserver: vs1
                  General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                          UDP Protocol: enabled
                          TCP Protocol: enabled
                 Default Windows User: -
                  NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

ONTAP NFS LIFを作成する

LIFは、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

開始する前に

- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネット

がすでに存在している必要があります。

サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

- LIFで処理されるトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9 .5以前では、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- Kerberos認証を使用する場合は、複数のLIFでKerberosを有効にします。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。

  および `network interface capacity details show`の詳細については `network interface capacity show`、を"ONTAPコマンド リファレンス"参照してください。

- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、同じサブネットにすでに設定されている他のLIFと同じブロードキャストドメイン内の指定したホームノード上の任意のポートを自動的に選択します。

ONTAP 9 .4以降では、FC-NVMeがサポートされます。FC-NVMe LIFを作成する場合は、次の点に注意してください。

- LIFを作成するFCアダプタでNVMeプロトコルがサポートされている必要があります。
- データLIFで使用できるデータプロトコルはFC-NVMeのみです。
- SANをサポートするStorage Virtual Machine（SVM）ごとに、管理トラフィックを処理するLIFを1つ設定する必要があります。
- NVMe LIFとネームスペースは同じノードでホストされている必要があります。
- データトラフィックを処理するNVMe LIFは、SVMごとに1つだけ設定できます。

手順

1. LIFを作成します。

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

   の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

オプション	説明

• ONTAP 9.5 以前 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
• ONTAP 9.6 以降 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- `-role`サービスポリシーを使用してLIFを作成する場合（ONTAP 9.6以降）は、パラメータは必要ありません。
- このパラメータは `-data-protocol`LIFの作成時に指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。

  `-data-protocol`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。

- `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

  オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

  の詳細については `network interface revert`、を"ONTAPコマンド リファレンス"参照してください。

- `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
- オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
- サブネットを使用してIPアドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときに、ゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
- IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内での静的ルートの作成に関する詳細については、を"ONTAPコマンド リファレンス"参照し `network route create`てください。
- オプションには `-firewall-policy`、LIFのロールと同じデフォルトを使用し `data`ます。

  必要に応じて、あとからカスタムファイアウォールポリシーを作成して追加できます。

ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false`。

  a. コマンドを使用して、LIFが正常に作成されたことを確認します `network interface show`。

  b. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

  c. Kerberosを使用する場合は、手順1~3を繰り返して追加のLIFを作成します。

  これらの各LIFでKerberosを個別に有効にする必要があります。

例

次のコマンドは、LIFを作成し、パラメータと `-netmask`パラメータを使用してIPアドレスとネットワークマスク値を指定し `-address`ます。

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワークマスク値を指定したサブネット（client1_sub）から割り当てます。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

次のコマンドは、サービスポリシーが割り当てられたNASデータLIFを作成する方法を示してい `default-data-files`ます。

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

関連情報

- "ネットワークping"
- "ネットワークインターフェイス"

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。

開始する前に

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。 `vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。

タスクの内容

詳細については、をご覧ください "SVM でのダイナミック DNS の設定"。

手順

1. SVMでDNSを有効にします。

   ```
   vserver services name-service dns create -vserver vserver_name -domains
   domain_name -name-servers ip_addresses -state enabled
   ```

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   コマンドは `vserver services name-service dns create`設定の自動検証を実行し、ONTAPがネームサーバに接続できない場合はエラーメッセージを報告します。

2. コマンドを使用して、DNSドメイン設定を表示します `vserver services name-service dns show`。

   次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. コマンドを使用して、ネームサーバのステータスを検証し `vserver services name-service dns check`ます。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver            Name Server     Status       Status Details
---------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

ネームサービスを設定する

ONTAP NFSネームサービスについて学ぶ

ストレージシステムの構成によっては、クライアントに適切なアクセス権を提供するために ONTAP でホスト、ユーザ、グループ、またはネットグループ情報を検索できるようにする必要があります。この情報を取得するためには、 ONTAP がローカルまたは外部のネームサービスにアクセスできるようにネームサービスを設定する必要があります。

NIS や LDAP などのネームサービスは、クライアント認証時の名前検索を容易にするために使用する必要があります。特に NFSv4 以降を導入する際は、セキュリティ強化のために、可能なかぎり LDAP を使用することを推奨します。外部ネームサーバが使用できない場合に備えて、ローカルのユーザとグループも設定する必要があります。

ネームサービス情報は、すべてのソースで同期を維持する必要があります。

ONTAP NFSネームサービススイッチテーブルを構成する

ONTAP がローカルまたは外部のネームサービスに問い合わせてホスト、ユーザ、グループ、ネットグループ、またはネームマッピングの情報を取得できるようにするには、ネームサービススイッチテーブルを正しく設定する必要があります。

開始する前に

ホスト、ユーザ、グループ、ネットグループ、またはネームマッピングで現在の環境に該当するように使用するネームサービスを決定しておく必要があります。

ネットグループの使用を計画する場合、ネットグループ内に指定されているすべての IPv6 アドレスは、 RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

タスクの内容

使用されていない情報ソースは含めないでください。たとえば、ご使用の環境でNISが使用されていない場合は、オプションを指定しない `-sources nis`でください。

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

   ```
   vserver services name-service ns-switch create -vserver vserver_name -database
   database_name -sources source_names
   ```

2. ネームサービススイッチテーブルに想定されるエントリが適切な順序で格納されていることを確認します。

   ```
   vserver services name-service ns-switch show -vserver vserver_name
   ```

   修正する場合は、コマンドまたは `vserver services name-service ns-switch delete`コマンドを使用する必要があります `vserver services name-service ns-switch modify。

例

次の例は、 SVM vs1 がローカルネットグループファイルを使用し、外部 NIS サーバがネットグループ情報をこの順序で検索するように、ネームサービススイッチテーブルに新しいエントリを作成します。

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

終了後

- データアクセスを提供するには、 SVM 用に指定したネームサービスを設定する必要があります。
- SVM 用のネームサービスを削除する場合は、ネームサービススイッチテーブルからも削除する必要があります。

  ネームサービススイッチテーブルからネームサービスを削除しないと、ストレージシステムへのクライアントアクセスが想定どおりに機能しない場合があります。

ローカル**UNIX**ユーザおよびグループの設定

ONTAP NFS SVMのローカル**UNIX**ユーザーとグループについて学習します

SVM 上で、認証およびネームマッピングにローカル UNIX ユーザおよびグループを使用できます。UNIX ユーザおよびグループは、手動で作成することも、 Uniform Resource Identifier （ URI ）から UNIX ユーザまたはグループを含むファイルをロードすることもできます。

クラスタ内のローカル UNIX ユーザグループおよびグループメンバーの合計数に対するデフォルトの上限値は 32 、 768 です。クラスタ管理者はこの制限を変更できます。

ONTAP NFS SVMにローカルUNIXユーザーを作成する

コマンドを使用すると、ローカルUNIXユーザを作成できます `vserver services name-service unix-user create`。ローカル UNIX ユーザは、 SVM 上に UNIX ネームサービスオプションとして作成し、ネームマッピングの処理で使用する UNIX ユーザです。

ステップ

1. ローカル UNIX ユーザを作成します。

   ```
   vserver services name-service unix-user create -vserver vserver_name -user
   user_name -id integer -primary-gid integer -full-name full_name
   ```

   `-user *user_name*`ユーザ名を指定します。ユーザ名は 64 文字以内にする必要があります。

   `-id *integer*`割り当てるユーザIDを指定します。

   `-primary-gid *integer*`プライマリグループIDを指定します。これにより、ユーザがプライマリグループに追加されます。ユーザを作成したあと、手動でユーザを目的の追加グループに追加できます。

例

次のコマンドは、johnmというローカルUNIXユーザ（フルネームは「John Miller」）をvs1というSVM上に作成します。ユーザのIDは123で、プライマリグループIDは100です。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

ONTAP NFS SVMにローカルUNIXユーザーリストをロードする

SVMで個 々 のローカルUNIXユーザを手動で作成する別の方法として、ローカルUNIXユーザのリストをUniform Resource Identifier（URI；ユニフォームリソース識別子）を使用(`vserver services name-service unix-user load-from-uri`してSVMにロードすることもできます。

手順

1. ロードするローカル UNIX ユーザのリストが含まれているファイルを作成します。

   ファイルには、次のUNIX形式でユーザ情報が含まれている必要があり `/etc/passwd`ます。

   ```
   user_name: password: user_ID: group_ID: full_name
   ```

   このコマンドを実行すると、フィールドの値とフィールド(`*home_directory*`の後のフィールドの値が`*full_name*`破棄され `*password*`*shell*`ます）。

   サポートされる最大ファイルサイズは 2.5MB です。

2. リストに重複した情報が含まれていないことを確認します。

   リストに重複したエントリが含まれている場合、リストのロードは失敗し、エラーメッセージが表示されます。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX ユーザのリストが含まれているファイルを、 URI から SVM にロードします。

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`*
   `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite{true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。

例

次のコマンドは、ローカルUNIXユーザのリストを、というURIを使用してvs1というSVM内にロードし`ftp://ftp.example.com/passwd`ます。URI を使用してロードした情報によって SVM 内の既存のユーザが上書きされることはありません。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

ONTAP NFS SVMにローカル**UNIX**グループを作成する

コマンドを使用すると、SVMに対してローカルなUNIXグループを作成できます `vserver services name-service unix-group create`。ローカル UNIX グループはローカル UNIX ユーザとともに使用されます。

ステップ

1. ローカル UNIX グループを作成します。

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`*`グループ名を指定します。グループ名は64文字以下にする必要があります。

   `-id` *`integer`*`割り当てるグループIDを指定します。

例

次のコマンドは、 vs1 という名前の SVM 上に eng という名前のローカルグループを作成します。グループID

は101です。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

ONTAP NFS SVMのローカル**UNIX**グループにユーザーを追加する

コマンドを使用すると、SVMに対してローカルなUNIXグループにユーザを追加できます `vserver services name-service unix-group adduser`。

ステップ

1. ローカル UNIX グループにユーザを追加します。

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` `*group_name*`ユーザのプライマリグループに加えて、ユーザを追加するUNIXグループの名前を指定します。

例

次のコマンドは、 vs1 という SVM の eng というローカル UNIX グループに、 max という名前のユーザを追加します。

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

ONTAP NFS SVM 上の **URI** からローカル **UNIX** グループをロードする

個 々 のローカルUNIXグループを手動で作成する別の方法として、コマンドを使用して、ローカルUNIXグループのリストをUniform Resource Identifier（URI）からSVMにロードすることができます `vserver services name-service unix-group load-from-uri`。

手順

1. ロードするローカル UNIX グループのリストが含まれているファイルを作成します。

   ファイルには、UNIX形式のグループ情報が含まれている必要があり `/etc/group`ます。

   `group_name: password: group_ID: comma_separated_list_of_users`

   このコマンドを実行すると、フィールドの値が破棄され `*password*`ます。

   サポートされる最大ファイルサイズは 1MB です。

   グループファイルの 1 行の最大長は、 32 、 768 文字です。

2. リストに重複した情報が含まれていないことを確認します。

   重複するエントリがリストに含まれていてはいけません。含まれていると、リストのロードに失敗します。SVMにすでにエントリがある場合は、パラメータをに `true`設定して既存のエントリをすべて新しいファイルで上書きするか、新しいファイルに既存のエントリと重複するエントリが一切含まれないようにする必要があります `-overwrite`。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX グループのリストが含まれているファイルを、 URI から SVM にロードします。

   ```
   vserver services name-service unix-group load-from-uri -vserver vserver_name
   -uri {ftp|http|ftps|https}://uri -overwrite {true|false}
   ```

   `-overwrite true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。このパラメータをに指定する `true`と、ONTAPは、指定したSVMの既存のローカルUNIXグループデータベース全体を、ロードするファイルのエントリで置き換えます。

例

次のコマンドは、ローカルUNIXグループのリストを、というURIを使用してvs1というSVM内にロードし `ftp://ftp.example.com/group`ます。URI を使用してロードした情報によって SVM 内の既存のグループが上書きされることはありません。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

ネットグループの使用

ONTAP NFS SVM 上のネットグループについて学ぶ

ネットグループは、ユーザ認証に使用したり、エクスポートポリシールールでクライアントを照合したりするために使用できます。外部ネームサーバ（LDAPまたはNIS）からネットグループへのアクセスを提供することも、コマンドを使用してUniform Resource Identifier（URI）からSVMへネットグループをロードすることもできます `vserver services name-service netgroup load`。

開始する前に

ネットグループを使用する前に、次の条件を満たしていることを確認する必要があります。

- ネットグループ内のすべてのホストは、ソース（NIS、LDAP、またはローカルファイル）に関係なく、フォワードおよびリバースDNSルックアップの一貫性を提供するために、フォワード（A）およびリバース

（PTR）の両方のDNSレコードを持つ必要があります。

さらに、クライアントのIPアドレスに複数のPTRレコードがある場合、それらのホスト名はすべてネットグループのメンバーであり、対応するAレコードを持っている必要があります。

- ソース（NIS、LDAP、またはローカルファイル）に関係なく、ネットグループ内のすべてのホストの名前のスペルが正しく、大文字と小文字が正しい必要があります。ネットグループで使用されているホスト名に大文字と小文字の不一致があると、予期しない動作（エクスポートチェックの失敗など）が発生する可能性があります。
- ネットグループに指定されているすべてのIPv6アドレスは、RFC 5952の指定に従って短縮および圧縮する必要があります。

  たとえば、 2011 ： hu9 ： 0 ： 0 ： 0 ： 0 ： 3 ： 1 は 2011 ： hu9 ： 3 ： 1 に短縮する必要があります。

タスクの内容

ネットグループについては次の処理を実行できます。

- コマンドを使用すると、クライアントIPが特定のネットグループのメンバーであるかどうかを確認できます `vserver export-policy netgroup check-membership`。
- コマンドを使用すると、クライアントがネットグループの一部であるかどうかを確認できます `vserver services name-service getxxbyyy netgrp`。

  検索を実行するための基盤となるサービスは、設定されているネームサービススイッチの順序に基づいて選択されます。

ONTAP NFS SVM 上の URI からネットグループをロードする

エクスポートポリシールールでクライアントの照合に使用できる方法の 1 つは、ネットグループにリストされているホストを使用することです。ネットグループは、外部ネームサーバに格納されているネットグループを使用する代わりに、Uniform Resource Identifier（URI）を使用(`vserver services name-service netgroup load`してSVMにロードできます。

開始する前に

ネットグループファイルは、 SVM にロードする前に、次の要件を満たしている必要があります。

- ファイルは、 NIS の設定に使用されるのと同じ適切なネットグループテキストファイル形式を使用する必要があります。

  ONTAP は、ロードを行う前にネットグループテキストファイル形式をチェックします。ファイルにエラーが含まれている場合、ファイルはロードされず、ファイルで実行する必要のある修正を示すメッセージが表示されます。エラーを修正後に、ネットグループファイルを指定した SVM に再ロードできます。

- ネットグループファイル内のホスト名に含まれる英文字は、すべて小文字にする必要があります。
- サポートされる最大ファイルサイズは 5MB です。
- ネットグループでサポートされる最大ネストレベルは 1000 です。
- ネットグループファイルでホスト名を定義する際に使用できるのは、プライマリ DNS ホスト名のみで

す。

エクスポートへのアクセスに関する問題を回避するために、ホスト名の定義には DNS CNAME やラウンドロビンレコードを使用しないでください。

- ネットグループファイル内の 3 つの値のうちユーザおよびドメインの部分は、 ONTAP でサポートされていないので空にしておく必要があります。

  ホスト / IP の部分のみがサポートされます。

タスクの内容

ONTAP は、ローカルネットグループファイルを対象としたホスト単位のネットグループ検索をサポートしています。ネットグループファイルをロードしたあと、ホスト単位のネットグループ検索を有効にするために netgroup.byhost マップが ONTAP によって自動的に作成されます。これにより、エクスポートポリシールールを処理してクライアントアクセスを評価する際のローカルネットグループ検索にかかる時間が大幅に短縮されます。

ステップ

1. URI から SVM にネットグループをロードします。

   ```
   vserver services name-service netgroup load -vserver vserver_name -source
   {ftp|http|ftps|https}://uri
   ```

   ネットグループファイルのロードとnetgroup.byhostマップの構築には数分かかることがあります。

   ネットグループの更新が必要な場合は、ネットグループファイルを編集し、更新されたファイルを SVM にロードすることができます。

例

次のコマンドは、HTTPのURLを使用して、ネットグループ定義をvs1というSVMにロードし`http://intranet/downloads/corp-netgroup`ます。

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVMネットグループ定義を確認する

SVMにネットグループをロードしたら、コマンドを使用してネットグループの定義のステータスを確認できます `vserver services name-service netgroup status`。これにより、ネットグループの定義が SVM の基盤となるすべてのノードで一貫した状態になっているかどうかを確認することができます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. ネットグループの定義のステータスを確認します。

```
vserver services name-service netgroup status
```

追加情報をより詳細なビューで表示できます。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

権限レベルを設定したあと、次のコマンドを実行すると、すべての SVM のネットグループのステータスが表示されます。

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- --------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

ONTAP NFS SVMのNISドメイン構成を作成する

環境でNetwork Information Service（NIS；ネットワーク情報サービス）がネームサービスに使用されている場合は、コマンドを使用して、SVMのNISドメイン設定を作成する必要があります `vserver services name-service nis-domain create`。

開始する前に

SVMにNISドメインを設定するには、設定済みのすべてのNISサーバが使用可能で到達可能である必要があります。

ディレクトリ検索での NIS の使用を予定している場合、 NIS サーバ内のマップに 1 、 024 文字を超えるエントリを持たせることはできません。この制限に従っていないNISサーバを指定しないでください。そうしない

と、NISエントリに依存するクライアントアクセスが失敗する可能性があります。

タスクの内容

NISデータベースにマップが含まれている場合 `netgroup.byhost`、ONTAPはこのマップを使用して検索を高速化できます。 `netgroup.byhost`ディレクトリ内のマップと `netgroup`マップは、クライアントアクセスに関する問題を回避するために、常に同期されている必要があります。nis.7以降では、コマンドを使用してONTAP 9 `netgroup.byhost`エントリをキャッシュでき `vserver services name-service nis-domain netgroup-database`ます。

ホスト名解決にNISを使用することはサポートされていません。

手順

1. NISドメイン設定を作成します。

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   最大10台のNISサーバを指定できます。

   。 `-nis-servers` NIS サーバーのホスト名または IP アドレスを指定するフィールド。

2. ドメインが作成されたことを確認します。

   ```
   vserver services name-service nis-domain show
   ```

例

次のコマンドは、という名前のSVM上に、IPアドレスのNISサーバを使用して `192.0.2.180`、という名前の`vs1`NISドメインのNISドメイン設定を作成し `nisdomain`ます。

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAPを使用

ONTAP NFS SVM での **LDAP** ネームサービスの使用について学習します

現在の環境でLDAPがネームサービスに使用されている場合は、LDAP管理者と協力して要件と適切なストレージシステム構成を決定し、SVMをLDAPクライアントとして有効にする必要があります。

10.1以降では、チャネルバインドが**ONTAP 9**接続とネームサービス**LDAP**接続の両方でデフォルトでサポートされます。**ONTAP**は、**Start-TLS**または**LDAPS**が有効で、セッションセキュリティが署名または封印のいずれかに設定されている場合にのみ、**LDAP**接続でチャネルバインディングを試行します。ネームサーバとの**LDAP**チャネルバインドを無効または再度有効にするには、コマンドでパラメータを **`ldap client modify`**使用し **`-try-channel-binding`**ます。

詳細については、を参照してください "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"。

- ONTAP用にLDAPを設定する前に、サイト環境がLDAPサーバとクライアントの設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAPサーバのドメイン名がLDAPクライアントのエントリと一致している必要があります。
  - LDAPサーバでサポートされるLDAPユーザパスワードのハッシュタイプには、ONTAPでサポートされるハッシュタイプが含まれている必要があります。
    - Crypt（すべてのタイプ）およびSHA-1（SHA、SSHA）。
    - ONTAP 9 .8以降では、SHA-2ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384、およびSSHA-512）もサポートされます。
  - LDAPサーバでセッションセキュリティ対策が必要な場合は、LDAPクライアントで設定する必要があります。

    次のセッションセキュリティオプションを使用できます。
    - LDAP署名（データ整合性チェックを提供）およびLDAP署名と封印（データ整合性チェックと暗号化を提供）
    - START TLS
    - LDAPS （ LDAP over TLS または SSL ）
  - 署名および封印されたLDAPクエリを有効にするには、次のサービスを設定する必要があります。
    - LDAPサーバは、GSSAPI（Kerberos）SASLメカニズムをサポートしている必要があります。
    - LDAPサーバには、DNS A/AAAAレコードと、DNSサーバで設定されたPTRレコードが必要です。
    - Kerberosサーバには、DNSサーバ上にSRVレコードが存在する必要があります。
  - START TLSまたはLDAPSを有効にするには、次の点を考慮する必要があります。
    - NetAppでは、LDAPSではなくStart TLSを使用することを推奨します。
    - LDAPSを使用する場合は、ONTAP 9 .5以降で、TLSまたはSSLに対してLDAPサーバが有効になっている必要があります。ONTAP 9ではSSLはサポートされていません。0-9.4
    - 証明書サーバがドメインで設定済みである必要があります。
  - LDAPリファーラル追跡を有効にするには（ONTAP 9 .5以降で）、次の条件を満たす必要があります。
    - 両方のドメインに次のいずれかの信頼関係を設定する必要があります。
      - 双方向
      - 一方向（プライマリがリファーラルドメインを信頼する場合）
      - 親子
    - 参照されるすべてのサーバ名を解決するようにDNSを設定する必要があります。
    - bind-as-cifs-server が true に設定されている場合、認証には両ドメインのパスワードが同じであることが必要です。

次の設定はLDAPリファーラル追跡ではサポートされていません。

- すべてのONTAPバージョン：
  - 管理 SVM 上の LDAP クライアント
- ONTAP 9.8 以前では（ 9.9.1 以降でサポートされています）：
  - LDAPの署名と封印（ `-session-security`オプション）
  - 暗号化されたTLS接続（ `-use-start-tls`オプション）
  - LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap`オプション）

- SVMでLDAPクライアントを設定するときは、LDAPスキーマを入力する必要があります。

  ほとんどの場合、デフォルトのONTAPスキーマのいずれかが適切です。ただし、環境で使用するLDAPスキーマがこれらと異なる場合は、LDAPクライアントを作成する前に、ONTAP用の新しいLDAPクライアントスキーマを作成する必要があります。環境の要件については、LDAP管理者にお問い合わせください。

- ホスト名解決にLDAPを使用することはサポートされていません。

詳細情報

- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"
- "ONTAP SMB SVMへの自己署名ルートCA証明書のインストール"

ONTAP NFS SVM用の新しい**LDAP**クライアントスキーマを作成する

環境で使用するLDAPスキーマがONTAPのデフォルトと異なる場合は、LDAPクライアント設定を作成する前に、ONTAP用の新しいLDAPクライアントスキーマを作成する必要があります。

タスクの内容

ほとんどのLDAPサーバでは、ONTAPが提供するデフォルトスキーマを使用できます。

- MS-AD-BIS（Windows Server 2012以降のほとんどのADサーバで推奨されるスキーマ）
- AD-IDMU（Windows 2008、Windows Server 2012、およびそれ以降のADサーバ）
- AD-SFU（Windows 2003以前のADサーバ）
- RFC-2307（UNIX LDAPサーバ）

デフォルト以外のLDAPスキーマを使用する必要がある場合は、LDAPクライアント設定を作成する前にスキーマを作成する必要があります。新しいスキーマを作成する前に、LDAP管理者に問い合わせてください。

ONTAPが提供するデフォルトのLDAPスキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、それに応じてコピーを変更します。

手順

1. 既存のLDAPクライアントスキーマテンプレートを表示して、コピーするスキーマを特定します。

```
vserver services name-service ldap client schema show
```

2. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

3. 既存のLDAPクライアントスキーマのコピーを作成します。

```
vserver services name-service ldap client schema copy -vserver vserver_name
-schema existing_schema_name -new-schema-name new_schema_name
```

4. 新しいスキーマを変更し、環境に合わせてカスタマイズします。

```
vserver services name-service ldap client schema modify
```

5. admin権限レベルに戻ります。

```
set -privilege admin
```

ONTAP NFSアクセス用の**LDAP**クライアント構成を作成する

環境内の外部LDAPサービスまたはActive Directoryサービスにアクセスする場合は、まずストレージシステム上にLDAPクライアントを設定する必要があります。

開始する前に

Active Directoryドメイン解決リストの最初の3つのサーバのいずれかが稼働し、データを提供している必要があります。そうしないと、このタスクは失敗します。

複数のサーバがあり、そのうちどの時点でも3台以上のサーバがダウンしています。

手順

1. LDAP管理者に問い合わせて、このコマンドの適切な設定値を確認し `vserver services name-service ldap client create`ます。

   a. LDAPサーバへのドメインベースまたはアドレスベースの接続を指定します。

   `-ad-domain`オプションと `-servers`オプションを同時に指定することはできません。

   - オプションを使用し `-ad-domain`て、Active DirectoryドメインでLDAPサーバ検出を有効にします。
     - オプションを使用すると `-restrict-discovery-to-site`、LDAPサーバ検出を、指定したドメインのCIFSデフォルトサイトに制限できます。このオプションを使用する場合は、でCIFSのデフォルトサイトを指定する必要もあり `-default-site`ます。
   - オプションを使用すると、優先されるActive Directoryサーバをカンマで区切ってIPアドレスで指定できます `-preferred-ad-servers`。クライアントが作成されたら、コマンドを使用してこのリストを変更できます `vserver services name-service ldap client modify`。

- オプションを使用する `-servers`と、1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）をIPアドレスでカンマで区切って指定できます。

  > は非推奨です。 `-ldap-servers`フィールドは `-servers`分野。このフィールドには、LDAPサーバのホスト名またはIPアドレスを指定できます。

b. デフォルトまたはカスタムのLDAPスキーマを指定します。

   ほとんどのLDAPサーバでは、ONTAPが提供するデフォルトの読み取り専用スキーマを使用できます。他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。他のスキーマを使用する場合は、デフォルトのスキーマ（読み取り専用）をコピーし、コピーを変更することによって、独自のスキーマを作成できます。

   デフォルトのスキーマ：

   - MS-AD-BIS

     RFC-2307bisに基づいて、Windows Server 2012以降のほとんどの標準的なLDAP環境で推奨されるLDAPスキーマです。

   - `AD-IDMU`

     Active Directory Identity Management for UNIXに基づいて、このスキーマはWindows 2008 、Windows 2012、およびそれ以降のほとんどのADサーバに適しています。

   - `AD-SFU`

     Active Directory Services for UNIXに基づいて、このスキーマはWindows 2003以前のほとんどのADサーバに適しています。

   - `RFC-2307`

     RFC-2307 （ネットワーク情報サービスとして LDAP を使用するためのアプローチ）に基づいて、このスキーマはほとんどの UNIX AD サーバに適しています。

c. バインド値を選択します。

   - `-min-bind-level {anonymous|simple|sasl}`最小バインド認証レベルを指定します。

     デフォルト値はです **`anonymous`**。

   - `-bind-dn *LDAP_DN*`バインドユーザを指定します。

     Active Directoryサーバの場合は、アカウント（domain\user）またはプリンシパル（user@domain.com）の形式でユーザを指定する必要があります。それ以外の場合は、識別名（CN=user、DC=domain、DC=com）の形式でユーザを指定する必要があります。

   - `-bind-password *password*`バインドパスワードを指定します。

d. 必要に応じて、セッションセキュリティオプションを選択します。

   LDAPの署名と封印、またはLDAP over TLS（LDAPサーバで必要な場合）を有効にすることができます。

- `--session-security {none|sign|seal}`

  署名(sign、データ整合性）、署名と封印(seal、データの整合性と暗号化を有効にすることができます。また、 none`署名と封印のどちらも有効にしないことも可能です。デフォルト値はです `none。

  {sasl`バインド認証をにフォールバックする場合、または `**simple**`署名と封印のバインドが失敗した場合以外は、} `**anonymous**`も設定する必要があります `-min-bind-level。

- `-use-start-tls{true|false}`

  に設定し、LDAPサーバでサポートされている場合、 **true**`LDAPクライアントはサーバへの暗号化されたTLS接続を使用します。デフォルト値はです `**false**。このオプションを使用するには、LDAPサーバの自己署名ルートCA証明書をインストールする必要があります。

  > Storage VMにSMBサーバがドメインに追加されていて、LDAPサーバがSMBサーバのホームドメインのドメインコントローラの1つである場合は、コマンドを使用してオプションを `vserver cifs security modify`変更できます `-session-security-for-ad-ldap。

e. ポート、クエリ、およびベースの値を選択します。

デフォルト値を推奨しますが、実際の環境に適しているかどうかをLDAP管理者に確認する必要があります。

- `-port *port*`LDAPサーバポートを指定します。

  デフォルト値はです 389。

Start TLSを使用してLDAP接続を保護する場合は、デフォルトのポート389を使用する必要があります。Start TLSはLDAPのデフォルトポート389経由でプレーンテキスト接続として開始され、その後TLS接続にアップグレードされます。ポートを変更すると、Start TLSが失敗します。

- `-query-timeout *integer*`クエリータイムアウトを秒単位で指定します。

  指定できる範囲は1～10秒です。デフォルト値は秒です 3。

- `-base-dn *LDAP_DN*`ベースDNを指定します。

  必要に応じて複数の値を入力できます（LDAPリファーラル追跡が有効な場合など）。デフォルト値は（root）です ""。

- `-base-scope{base|onelevel|subtree}` は、ベース検索範囲を指定します。

  デフォルト値はです subtree。

- `-referral-enabled{true|false}` LDAPリファーラル追跡を有効にするかどうかを指定します。

  ONTAP 9 .5以降では、必要なレコードが参照先のLDAPサーバに存在することを示すLDAPリファーラル応答がプライマリLDAPサーバから返された場合に、ONTAP LDAPクライアントが他のLDAPサーバへのルックアップ要求を参照できるようになりました。デフォルト値はです

false。

参照されたLDAPサーバに存在するレコードを検索するには、参照されたレコードのベースDNをLDAPクライアント設定の一部としてベースDNに追加する必要があります。

2. Storage VMにLDAPクライアント設定を作成します。

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

LDAPクライアント設定を作成するときは、Storage VM名を指定する必要があります。

3. LDAPクライアント設定が正常に作成されたことを確認します。

```
vserver services name-service ldap client show -client-config
client_config_name
```

例

次のコマンドでは、LDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

次のコマンドでは、署名と封印が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。また、LDAPサーバ検出は指定したドメインの特定サイトに制限されます。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

次のコマンドでは、LDAPリファーラル追跡が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1にldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

次のコマンドでは、ベースDNを指定することで、Storage VM vs1でldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

次のコマンドでは、リファーラル追跡を有効にすることで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

LDAPクライアント設定を**ONTAP NFS SVM**に関連付ける

SVMでLDAPを有効にするには、コマンドを使用してLDAPクライアント設定をSVMに関連付ける必要があります `vserver services name-service ldap create`。

開始する前に

- LDAPドメインがネットワーク内にすでに存在し、SVMが配置されているクラスタからアクセスできる必要があります。
- LDAPクライアント設定がSVM上に存在している必要があります。

手順

1. SVMでLDAPを有効にします。

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > その `vserver services name-service ldap create`コマンドは自動構成検証を実行し、ONTAP がネーム サーバに接続できない場合はエラー メッセージを報告します。

   次のコマンドは、「vs1」SVMでLDAPを有効にし、「ldap1」LDAPクライアント設定を使用するように設定します。

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. vserver services name-service ldap checkコマンドを使用して、ネームサーバのステータスを検証します。

   次のコマンドは、SVM vs1のLDAPサーバを検証します。

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

ONTAP NFS SVMの**LDAP**ソースを確認する

ネームサービスのLDAPソースがSVMのネームサービススイッチテーブルに正しく表示されていることを確認する必要があります。

手順

1. 現在のネームサービススイッチテーブルの内容を表示します。

   `vserver services name-service ns-switch show -vserver svm_name`

   次のコマンドは、 SVM My_SVM の結果を表示します。

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
My_SVM          hosts          files,
                               dns
My_SVM          group          files,ldap
My_SVM          passwd         files,ldap
My_SVM          netgroup       files
My_SVM          namemap        files
5 entries were displayed.
```

   `namemap`ネームマッピング情報を検索するソースとその検索順序を指定します。UNIX のみの環境では、このエントリは必要ありません。ネームマッピングは、 UNIX と Windows の両方を使用する混在環境でのみ必要になります。

2. 必要に応じてエントリを更新し `ns-switch`ます。

ns-switch エントリの更新対象	入力するコマンド
ユーザ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
グループ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
ネットグループ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

NFSでKerberosを使用してセキュリティを強化

セキュリティ認証にONTAP NFSでKerberosを使用する方法について学習します

ご使用の環境でKerberosが強力な認証に使用されている場合は、Kerberos管理者と協力して要件および適切なストレージシステム構成を決定し、SVMをKerberosクライアントとして有効にする必要があります。

環境が次のガイドラインを満たしている必要があります。

- ONTAP で Kerberos を設定するには、 Kerberos のサーバとクライアントの設定に適したベストプラクティスに従ってサイトが導入されている必要があります。
- Kerberos 認証を必須とする場合は、可能であれば NFSv4 以降を使用します。

  NFSv3 でも Kerberos を使用できますが、Kerberos の高度なセキュリティ機能をフルに活用するには、ONTAP を NFSv4 以降に導入する必要があります。

- サーバアクセスの冗長化を促すため、同じ SPN を使ってクラスタ内の複数のノードのデータ LIF で Kerberos を有効にする必要があります。
- Kerberos を SVM で有効にする場合は、 NFS クライアントの設定に応じて、次のいずれかのセキュリティ方式をボリュームまたは qtree のエクスポートルールに指定する必要があります。
  - `krb5`（Kerberos v5プロトコル）
  - `krb5i`（Kerberos v5プロトコルとチェックサムによる整合性チェック）
  - `krb5p`（Kerberos v5プロトコルとプライバシーサービス）

Kerberos のサーバとクライアントのほかに、次の外部サービスを Kerberos を使用する ONTAP 用に設定する必要があります。

- ディレクトリサービス

  Active Directory や OpenLDAP などのセキュアなディレクトリサービスを環境に導入し、 SSL / TLS 経由

の LDAP を使用するように設定してください。NIS を使用すると、要求がクリアテキストで送信されセキュアではないため、 NIS は使用しないでください。

- NTP

  NTPを実行している稼働中のタイムサーバが必要です。これは、時間のずれによるKerberos認証の失敗を防ぐために必要です。

- ドメイン名解決（DNS）

  各UNIXクライアントおよび各SVM LIFについて、KDCのフォワードルックアップゾーンとリバースルックアップゾーンに適切なサービスレコード（SRV）が登録されている必要があります。すべての参加者は、DNSを介して適切に解決できる必要があります。

ONTAP SVM 上の NFS Kerberos 構成の UNIX 権限を確認する

Kerberos では、特定の UNIX 権限が SVM ルートボリューム用およびローカルのユーザおよびグループ用に設定されている必要があります。

手順

1. SVM ルートボリュームについて、関連する権限を表示します。

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   SVMのルートボリュームを次のように設定しておく必要があります。

名前	設定
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	755

   これらの値が表示されない場合は、コマンドを使用し `volume modify`て更新します。

2. ローカル UNIX ユーザを表示します。

   `vserver services name-service unix-user show -vserver vserver_name`

   SVMで次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザID	プライマリグループID	コメント
NFS	500	0	GSS INIT フェーズで必要。 NFSクライアントユーザSPNの最初のコンポーネントがユーザとして使用されます。 NFSクライアントユーザのSPNに対するKerberos-UNIXネームマッピングがある場合は、nfsユーザは必要ありません。
root	0	0	マウントに必要。

これらの値が表示されていない場合は、コマンドを使用して更新できます `vserver services name-service unix-user modify`。

3. ローカル UNIX グループを表示します。

   `vserver services name-service unix-group show -vserver vserver _name`

   SVMで次のUNIXグループを設定しておく必要があります。

グループ名	グループID
デーモン	1
root	0

これらの値が表示されていない場合は、コマンドを使用して更新できます `vserver services name-service unix-group modify`。

ONTAP SVM で **NFS Kerberos** レルム構成を作成する

環境で ONTAP から外部 Kerberos サーバにアクセスする場合は、まず既存の Kerberos Realm を使用するように SVM を設定する必要があります。そのためには、Kerberos KDCサーバの設定値を収集し、コマンドを使用してSVMにKerberos Realm設定を作成する必要があり `vserver nfs kerberos realm create`ます。

開始する前に

認証の問題を回避するために、クラスタ管理者はストレージシステム、クライアント、および KDC サーバ上で NTP を設定しておく必要があります。クライアントとサーバの時間差（クロックスキュー）は、認証エラーの一般的な原因です。

手順

1. Kerberos管理者に問い合わせて、コマンドで指定する適切な設定値を決定し `vserver nfs kerberos realm create`ます。
2. SVM で Kerberos Realm の設定を作成します。

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. Kerberos Realmの設定が正常に作成されたことを確認します。

   ```
   vserver nfs kerberos realm show
   ```

例

次のコマンドは、 Microsoft Active Directory サーバを KDC サーバとして使用する NFS Kerberos Realm 設定を SVM vs1 で作成します。Kerberos Realm は AUTH.EXAMPLE.COM です。Active Directory サーバの名前は ad-1 で、 IP アドレスは 10.10.8.14 です。許容されるクロックスキューは 300 秒（デフォルト）です。KDC サーバの IP アドレスは 10.10.8.14 で、ポート番号は 88 （デフォルト）です。「Microsoft Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

次のコマンドは、 MIT KDC を使用する NFS Kerberos Realm 設定を SVM vs1 で作成します。Kerberos Realm は SECURITY.EXAMPLE.COM です。許容されるクロックスキューは300秒です。KDC サーバの IP アドレスは 10.10.9.1 で、ポート番号は 88 です。KDC ベンダーは UNIX ベンダーを示す Other です。管理サーバの IP アドレスは 10.10.9.1 で、ポート番号は 749 （デフォルト）です。パスワードサーバの IP アドレスは 10.10.9.1 で、ポート番号は 464 （デフォルト）です。「UNIX Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

ONTAP SVMのNFS Kerberos許可暗号化タイプを設定する

デフォルトでは、 ONTAP は、 DES 、 3DES 、 AES-128 、および AES-256 の暗号化タイプをサポートします。コマンドでパラメータを指定する `-permitted-enc -types`と、SVMごとに許可される暗号化タイプを、特定の環境のセキュリティ要件に合わせて設定できます `vserver nfs modify`。

タスクの内容

クライアントの互換性を最大限に高めるために、ONTAPはデフォルトで弱いDES暗号化と強いAES暗号化の両方をサポートしています。つまり、たとえば、セキュリティを強化する必要があり、環境でサポートされている場合は、この手順を使用してDESと3DESを無効にし、クライアントにAES暗号化のみの使用を要求できます。

使用可能な最も強力な暗号化を使用する必要があります。ONTAP の場合は AES-256 です。この暗号化レベルが環境でサポートされていることを、 KDC 管理者に確認する必要があります。

- SVMでAES全体（AES-128とAES-256の両方）を有効または無効にすると、システムが停止します。元のDESプリンシパル/ keytabファイルが削除され、SVMのすべてのLIFでKerberos設定を無効にする必要があるためです。

  この変更を行う前に、SVMでNFSクライアントがAES暗号化を使用していないことを確認する必要があります。

- DES や 3DES の有効化または無効化は、 LIF での Kerberos 設定の変更を一切必要としません。

ステップ

1. 許可されている暗号化タイプを有効または無効にします。

有効または無効にする対象	実行する手順
DES または 3DES	a. SVMのNFS Kerberosで許可されている暗号化タイプを設定します。+ `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* 暗号化タイプが複数ある場合はカンマで区切ります。 b. 変更が成功したことを確認します。+ `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

有効または無効にする対象	実行する手順

AES-128またはAES-256	a. Kerberosが有効になっているSVMとLIFを特定します。+
	`vserver nfs kerberos interface show`
	b. 変更対象のNFS Kerberosで許可されている暗号化タイプが設定されているSVM上のすべてのLIFでKerberosを無効にします。+
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	c. SVMのNFS Kerberosで許可されている暗号化タイプを設定します。+
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	暗号化タイプが複数ある場合はカンマで区切ります。
	d. 変更が成功したことを確認します。+
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	e. SVM上のすべてのLIFでKerberosを再度有効にします。+
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	f. すべてのLIFでKerberosが有効になっていることを確認します。+
	`vserver nfs kerberos interface show`

ONTAP LIFで**NFS Kerberos**を有効にする

コマンドを使用すると、データLIFでKerberosを有効にできます `vserver nfs kerberos interface enable`。これにより、SVMでNFSのKerberosセキュリティサービスを使用できます。

タスクの内容

Active Directory KDC を使用する場合、使用される SPN の最初の 15 文字は Realm またはドメイン内の SVM 間で一意である必要があります。

手順

1. NFS Kerberos 設定を作成します。

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
logical_interface -spn service_principal_name
```

ONTAP で Kerberos インターフェイスを有効にするには、 KDC の SPN 用のシークレットキーが必要です。

Microsoft KDC の場合、 KDC に接続があると、シークレットキーを取得するためのユーザ名とパスワードのプロンプトが CLI で発行されます。Kerberos Realmの別のOUでSPNを作成する必要がある場合は、オプションのパラメータを指定できます `-ou`。

Microsoft 以外の KDC の場合は、次の 2 つのうちいずれかの方法を使用してシークレットキーを取得できます。

状況	コマンドとともに含める必要のあるパラメータ
KDC からキーを直接取得するための KDC 管理者のクレデンシャルが必要です	`-admin-username` *`kdc_admin_username`*
KDC 管理者のクレデンシャルはないが、キーが含まれている、 KDC の keytab ファイルはある	`-keytab-uri` {ftp

2. LIFでKerberosが有効になったことを確認します。

   `vserver nfs kerberos-config show`

3. 複数の LIF で Kerberos を有効にするには、手順 1 と 2 を繰り返します。

例

次のコマンドは、 vs1 という SVM の NFS Kerberos 設定を、 OU lab2ou 内の SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM を使用して、 ves03-d1 という論理インターフェイス ves03-d1 に対して作成して検証します。

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

NFS対応SVMにストレージ容量を追加する

ONTAP NFS対応SVMにストレージ容量を追加する方法について学習します

NFS 対応 SVM にストレージ容量を追加するには、ストレージコンテナを提供するボリュームまたは qtree を作成し、そのコンテナのエクスポートポリシーを作成または変更する必要があります。その後、クラスタからの NFS クライアントアクセスを確認し、クライアントシステムからのアクセスをテストできます。

開始する前に

- SVMでNFSの設定が完了している必要があります。
- SVM ルートボリュームのデフォルトのエクスポートポリシーに、すべてのクライアントへのアクセスを許可するルールが含まれている必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Kerberos 設定への追加または変更が完了している必要があります。

ONTAP NFSエクスポートポリシーを作成する

エクスポートルールを作成する前に、それらを保持するエクスポートポリシーを作成する必要があります。エクスポートポリシーは、コマンドを使用して作成できます `vserver export-policy create`。

手順

1. エクスポートポリシーを作成します。

   ```
   vserver export-policy create -vserver vserver_name -policyname policy_name
   ```

   ポリシー名の最大文字数は256文字です。

2. エクスポートポリシーが作成されたことを確認します。

   ```
   vserver export-policy show -policyname policy_name
   ```

例

次のコマンドは、 vs1 という SVM で、 exp1 という名前のエクスポートポリシーを作成し、作成を確認します。

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

ONTAP NFSエクスポートポリシーにルールを追加する

エクスポートポリシーにルールがないと、クライアントはデータにアクセスできませ

ん。新しいエクスポートルールを作成するには、クライアントを特定してクライアント照合形式を選択し、アクセスとセキュリティのタイプを選択し、匿名ユーザIDマッピングを指定し、ルールインデックス番号を選択して、アクセスプロトコルを選択する必要があります。その後、コマンドを使用して、新しいルールをエクスポートポリシーに追加できます `vserver export-policy rule create`。

開始する前に

- エクスポートルールを追加するエクスポートポリシーを用意しておく必要があります。
- データ SVM で DNS が正しく設定されている必要があり、 DNS サーバに NFS クライアント用の正しいエントリが存在する必要があります。

  その理由は、特定のクライアント照合形式で ONTAP がデータ SVM の DNS 設定を使用して DNS ルックアップを実行することと、エクスポートポリシールールの照合が失敗するとクライアントがデータにアクセスできなくなる可能性があることです。

- Kerberosで認証する場合は、NFSクライアントで次のいずれのセキュリティ方式が使用されているかを確認しておく必要があります。
  - `krb5`（Kerberos v5プロトコル）
  - `krb5i`（Kerberos v5プロトコルとチェックサムによる整合性チェック）
  - `krb5p`（Kerberos v5プロトコルとプライバシーサービス）

タスクの内容

エクスポートポリシーの既存のルールがクライアント一致とアクセスの要件を満たしている場合は、新しいルールを作成する必要はありません。

Kerberosで認証する場合に、SVMのすべてのボリュームにKerberos経由でアクセスできる場合は `-superuser`、 `krb5i`ルートボリュームのエクスポートルールオプション、 `-rwrule`、、を、または `krb5p`に `krb5`設定できます `-rorule`。

手順

1. 新しいルールのクライアントとクライアント照合形式を特定します。

   オプションは `-clientmatch`、ルールを適用するクライアントを指定します。クライアント一致の値は1つまたは複数指定できます。複数の値を指定する場合はカンマで区切る必要があります。次のいずれかの形式で指定できます。

クライアント照合形式	例
先頭に文字が付いたドメイン名	`.example.com`または `.example.com,.example.net,...`
ホスト名	`host1`または `host1,host2, ...`
IPv4アドレス	`10.1.12.24`または `10.1.12.24,10.1.12.25, ...`

クライアント照合形式	例
サブネット マスクをビット数で表したIPv4アドレス	`10.1.12.10/4`または `10.1.12.10/4,10.1.12.11/4,...`
IPv4アドレスとネットワークマスク	`10.1.16.0/255.255.255.0`または `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
ドット付き形式のIPv6アドレス	`::1.2.3.4`または `::1.2.3.4,::1.2.3.5,...`
サブネットマスクをビット数で表したIPv6アドレス	`ff::00/32`または `ff::00/32,ff::01/32,...`
先頭に@文字が付いた単一のネットグループ	`@netgroup1`または `@netgroup1,@netgroup2,...`

クライアント定義のタイプを組み合わせることもできます（例：） `.example.com,@netgroup1`。

IPアドレスを指定する場合は、次の点に注意してください。

- 10.1.12.10-10.1.12.70などのIPアドレス範囲を入力することはできません。

  この形式のエントリはテキスト文字列と解釈され、ホスト名として扱われます。

- クライアントアクセスのきめ細かな管理のためにエクスポートルールで個々の IP アドレスを指定する際には、動的（ DHCP など）または一時的（ IPv6 など）に割り当てられている IP アドレスを指定しないでください。

  そうしないと、IPアドレスが変更されると、クライアントはアクセスを失います。

- ff ： 12/ff ： 00 のように、 IPv6 アドレスとネットワークマスクを入力することはできません。

2. クライアント一致のアクセスタイプとセキュリティタイプを選択します。

   指定したセキュリティタイプで認証するクライアントには、次のアクセスモードを1つ以上指定できます。

   - `-rorule`（読み取り専用アクセス）
   - `-rwrule`（読み取り/書き込みアクセス）
   - `-superuser`（ルートアクセス）

   > ⓘ 特定のセキュリティタイプの読み取り/書き込みアクセスは、エクスポートルールでそのセキュリティタイプの読み取り専用アクセスも許可されている場合にのみ許可されます。読み取り専用パラメータで読み取り/書き込みパラメータよりも限定的なセキュリティタイプを指定すると、クライアントに対して読み取り/書き込みアクセスが許可されない可能性があります。スーパーユーザアクセスについても同様です。

1つのルールに対して複数のセキュリティタイプをカンマで区切って指定できます。セキュリティタイプとしてまたはを `never`指定する場合は `any`、他のセキュリティタイプは指定しないでください。次の有効なセキュリティタイプから選択します。

セキュリティタイプの設定	一致するクライアントからエクスポートされたデータへのアクセス
`any`	受信セキュリティタイプに関係なく、常に。
`none`	単独で指定した場合、どのセキュリティタイプのクライアントにも匿名アクセスが許可されます。他のセキュリティタイプと一緒に指定すると、指定したセキュリティタイプのクライアントにアクセスが許可され、それ以外のセキュリティタイプのクライアントには匿名アクセスが許可されます。
`never`	受信セキュリティタイプに関係なく、なし。
`krb5`	Kerberos 5によって認証されます。認証のみ：各要求および応答のヘッダーが署名されます。
`krb5i`	Kerberos 5iによって認証されます。認証および整合性：各要求および応答のヘッダーと本文が署名されます。
`krb5p`	Kerberos 5pによって認証されます。認証、整合性、およびプライバシー：各要求および応答のヘッダーと本文が署名され、 NFS データペイロードが暗号化されます。
`ntlm`	CIFS NTLMによって認証されます。
`sys`	NFS AUTH_SYSで認証されます。

推奨されるセキュリティタイプは `sys`、または（Kerberosを使用する場合） `krb5`、、 `krb5i`、、または `krb5p`です。

NFSv3でKerberosを使用している場合は `-rwrule`、に加えて `krb5`エクスポートポリシールールでアクセスを `sys`許可する必要があります `-rorule`。これは、Network Lock Manager（NLM）によるエクスポートへのアクセスを許可する必要があるためです。

3. 匿名ユーザIDマッピングを指定します。

`-anon`オプションは、ユーザIDが0（ゼロ）で到着するクライアント要求にマッピングされるUNIXユーザIDまたはユーザ名を指定します。このユーザIDは通常ユーザ名rootに関連付けられています。デフォルト値はです`65534`。NFS クライアントは通常、ユーザ ID 65534 をユーザ名 nobody と関連付けます（ _root squashing_ ） 。ONTAPでは、このユーザIDはユーザpcuserに関連付けられています。ユーザIDが0のクライアントからのアクセスを無効にするには、の値を指定し `65535`ます。

4. ルールインデックスの順序を選択します。

   オプションは -ruleindex、ルールのインデックス番号を指定します。ルールはインデックス番号のリスト内の順序に従って評価され、インデックス番号が小さいルールが最初に評価されます。たとえば、インデックス番号が1のルールは、インデックス番号が2のルールよりも先に評価されます。

追加対象	そしたら...。
エクスポートポリシーへの最初のルール	と入力し`1`ます。
追加のルールをエクスポートポリシーに	a. ポリシー内の既存のルールを表示します。+ `vserver export-policy rule show -instance -policyname your_policy` b. 評価する順序に応じて、新しいルールのインデックス番号を選択します。

5. 該当するNFSアクセス値を選択します{nfs|nfs3|nfs4：}。

   nfs`任意のバージョンに一致し `nfs3、 `nfs4`特定のバージョンだけに一致します。

6. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. エクスポートポリシーのルールを表示して、新しいルールが存在することを確認します。

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   このコマンドは、エクスポートポリシーに適用されているルールのリストを含む、エクスポートポリシーの概要を表示します。ONTAPは、各ルールにルールインデックス番号を割り当てます。ルールインデックス番号を確認したら、その番号を使用して、指定したエクスポートルールに関する詳細情報を表示できます。

8. エクスポートポリシーに適用されたルールが正しく設定されていることを確認します。

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

例

次のコマンドは、 rs1 というエクスポートポリシーで vs1 という SVM に対するエクスポートルールを作成し、作成を確認します。このルールのインデックス番号は1です。このルールは、ドメインeng.company.comおよびネットグループ@netgroup1内のすべてのクライアントに一致します。このルールは、すべてのNFSアクセスを有効にします。AUTH_SYSで認証されたユーザに対する読み取り専用アクセスと読み取り/書き込みアクセスを有効にします。UNIXユーザIDが0（ゼロ）のクライアントは、Kerberosで認証されないかぎり匿名化されます。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

次のコマンドは、 expol2 というエクスポートポリシーで vs2 という SVM に対するエクスポートルールを作成し、作成を確認します。このルールのインデックス番号は21です。このルールは、クライアントをネットグループdev_netgroup_mainのメンバーと照合します。このルールは、すべてのNFSアクセスを有効にします。AUTH_SYSで認証されたユーザの読み取り専用アクセスを有効にし、読み取り/書き込みアクセスとrootアクセスにはKerberos認証を必要とします。UNIXユーザIDが0（ゼロ）のクライアントは、Kerberos以外で認証されないかぎり、ルートアクセスを拒否されます。

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                  Vserver: vs2
                              Policy Name: expol2
                               Rule Index: 21
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                           @dev_netgroup_main
                            RO Access Rule: sys
                            RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

ボリュームまたは**qtree**のストレージコンテナを作成する

ONTAP NFSボリュームを作成する

コマンドを使用すると、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create`。

タスクの内容

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームの作成時に指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、コマンドを使用して、SVMネームスペースでボリュームを_mount_theにする必要があります `volume mount`。

開始する前に

- NFSがセットアップされ、実行されている必要があります。
- SVMのセキュリティ形式がUNIXである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する

`volume create`か、 `-activity-tracking-state`に設定します `on。

容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。の詳細については volume create、を"ONTAPコマンド リファレンス"参照してください。

手順

1. ジャンクションポイントを設定してボリュームを作成します。

   volume create -vserver *svm_name* -volume *volume_name* -aggregate *aggregate_name* -size {*integer*[KB|MB|GB|TB|PB]} -security-style unix -user *user_name_or_number* -group *group_name_or_number* -junction-path *junction_path* [-policy *export_policy_name*]

   の選択肢は `-junction-path`次のとおりです。

   - ルートの直下。例： */new_vol*

     新しいボリュームを作成し、 SVM のルートボリュームに直接マウントされるように指定することができます。

   - 既存のディレクトリの下（例： */existing_dir/new_vol*

     新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

     たとえば、新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は */new_dir/new_vol*、SVMのルートボリュームにジャンクションされている新しい親ボリュームを最初に作成する必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

   + 既存のエクスポートポリシーを使用する場合は、ボリュームの作成時に指定できます。エクスポートポリシーは、あとからコマンドを使用して追加することもできます volume modify。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

   volume show -vserver *svm_name* -volume *volume_name* -junction

例

次のコマンドは、 SVM vs1.example.com およびアグリゲート aggr1 上に、 users1 という名前の新しいボリュームを作成します。新しいボリュームは、で使用でき `/users`ます。ボリュームのサイズは750GBで、ボリュームギャランティのタイプはvolume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

次のコマンドは、SVM「vs1.example.com」とアグリゲート「aggr1」に「home4」という名前の新しいボリュームを作成します。ディレクトリは /eng/`vs1 SVMのネームスペース内にすでに存在し、新しいボリュームがで使用可能になります `/eng/home。これがネームスペースのホームディレクトリになります。/eng/`ボリュームのサイズは750GBで、ボリュームギャランティのタイプは（デフォルト）です `volume。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

ONTAP NFS qtreeを作成する

コマンドを使用すると、データを含むqtreeを作成し、そのプロパティを指定できます volume qtree create。

開始する前に

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVMのセキュリティ形式がUNIXで、NFSが設定されて実行されている必要があります。

手順

1. qtree を作成します。

   ```
   volume qtree create -vserver vserver_name { -volume volume_name -qtree
   qtree_name | -qtree-path qtree path } -security-style unix [-policy
   export_policy_name]
   ```

   ボリュームとqtreeを別 々 の引数として指定するか、の形式でqtreeパスの引数を指定できます /vol/volume_name/_qtree_name。

デフォルトでは、 qtree は親ボリュームのエクスポートポリシーを継承しますが、独自のものを使用するように設定することもできます。既存のエクスポートポリシーを使用する場合は、 qtree の作成時にポリシーを指定できます。エクスポートポリシーは、あとからコマンドを使用して追加することもできます `volume qtree modify`。

2. qtree が必要なジャンクションパスで作成されたことを確認します。

   ```
   volume qtree show -vserver vserver_name { -volume volume_name -qtree
   qtree_name | -qtree-path qtree path }
   ```

例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成し`/vol/data1`ます。

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

エクスポート ポリシーを使用した**NFS**アクセスの保護

エクスポートポリシーを使用して **ONTAP NFS** アクセスを保護する方法について学習します。

エクスポートポリシーを使用すると、ボリュームまたはqtreeへのNFSアクセスを、特定のパラメータに一致するクライアントだけに制限できます。新しいストレージをプロビジョニングする際に、既存のポリシーとルールを使用するか、既存のポリシーにルールを追加するか、新しいポリシーとルールを作成できます。エクスポートポリシーの設定も確認できます。

ONTAP 9 .3以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にして、すべてのルール違反をエラールールリストに記録できます。 `vserver export-policy config-checker`コマンドはチェッカーを呼び出して結果を表示します。この結果を使用して、設定を検証し、エラーのあるルールをポリシーから削除できます。このコマンドで検証されるのは、ホスト名、ネットグループ、匿名ユーザのエクスポート設定のみです。

ONTAP NFSエクスポートルールの処理順序を管理する

コマンドを使用すると、既存のエクスポートルールのインデックス番号を手動で設定できます `vserver export-policy rule setindex`。これにより、 ONTAP がクライアント要求に対してエクスポートルールを適用する優先順位を指定できます。

タスクの内容

新しいインデックス番号がすでに使用されている場合は、指定した場所にルールが挿入され、それに応じてリストの順序が変更されます。

ステップ

1. 指定したエクスポートルールのインデックス番号を変更します。

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

例

次のコマンドは、 vs1 という SVM の rs1 というエクスポートポリシーのインデックス番号を 3 から 2 に変更します。

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

ONTAP NFSエクスポートポリシーをボリュームに割り当てる

SVM内の各ボリュームには、クライアントがボリューム内のデータにアクセスできるように、エクスポートルールを含むエクスポートポリシーを関連付ける必要があります。

タスクの内容

エクスポートポリシーは、ボリュームの作成時、またはボリュームの作成後にいつでも、ボリュームに関連付けることができます。1 つのボリュームに関連付けることができるのは 1 つのエクスポートポリシーだけですが、 1 つのポリシーを多数のボリュームに関連付けることができます。

手順

1. ボリュームの作成時にエクスポートポリシーを指定しなかった場合は、ボリュームにエクスポートポリシーを割り当てます。

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. ポリシーがボリュームに割り当てられたことを確認します。

```
volume show -volume volume_name -fields policy
```

例

次のコマンドは、エクスポートポリシー nfs_policy を vs1 という SVM 上のボリューム vol1 に割り当てて、割り当てを確認します。

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

ONTAP NFSエクスポートポリシーをqtreeに割り当てる

ボリューム全体をエクスポートする代わりに、ボリュームの特定の qtree をエクスポートしてクライアントから直接アクセスできるようにすることもできます。qtree をエクスポートするには、 qtree にエクスポートポリシーを割り当てます。エクスポートポリシーの割り当ては、新しい qtree の作成時に行うことも、既存の qtree の変更によって行うこともできます。

開始する前に

エクスポートポリシーが存在している必要があります。

タスクの内容

qtree では、作成時に指定しなかった場合、格納先ボリュームの親のエクスポートポリシーがデフォルトで継承されます。

エクスポートポリシーは、 qtree の作成時、または qtree の作成後にいつでも、 qtree に関連付けることができます。1 つの qtree に関連付けることができるのは 1 つのエクスポートポリシーだけですが、 1 つのポリシーを多数の qtree と関連付けることができます。

手順

1. qtree の作成時にエクスポートポリシーを指定しなかった場合は、 qtree にエクスポートポリシーを割り当てます。

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. ポリシーが qtree に割り当てられたことを確認します。

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

例

次のコマンドは、エクスポートポリシー nfs_policy を vs1 という SVM 上の qtree qt1 に割り当てて、割り当てを確認します。

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

クラスタからの**ONTAP NFS**クライアントアクセスを確認する

UNIX 管理ホストで UNIX ファイル権限を設定することにより、選択したクライアントに共有へのアクセスを許可できます。クライアントアクセスを確認するには、コマンドを使用し `vserver export-policy check-access`、必要に応じてエクスポートルールを調整します。

手順

1. クラスタで、コマンドを使用してエクスポートへのクライアントアクセスを確認します `vserver export-policy check-access`。

   次のコマンドは、 IP アドレスが 1.2.3.4 の NFSv3 クライアントによるボリューム home2 への読み取り / 書き込みアクセスをチェックします。コマンド出力には、ボリュームでエクスポートポリシーが使用されていること、およびアクセスが拒否されたことが示されています `exp-home-dir`。

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
   -type read-write
                                        Policy    Policy     Rule
   Path                    Policy       Owner     Owner Type Index  Access
   ----------------------- ------------ --------- ---------- ------
   ----------
   /                       default      vs1_root  volume          1 read
   /eng                    default      vs1_root  volume          1 read
   /eng/home2              exp-home-dir home2     volume          1 denied

   3 entries were displayed.
   ```

2. 出力を確認して、エクスポートポリシーが意図したとおりに機能してクライアントアクセスが想定どおりに動作しているかどうかを判断します。

   具体的には、ボリュームまたは qtree によって使用されたエクスポートポリシーと、結果としてクライアントが行ったアクセスのタイプを確認する必要があります。

3. 必要に応じて、エクスポートポリシールールを再設定します。

新しいストレージオブジェクトに対する NFS アクセスの確認が完了したら、設定をテストする必要があります。設定をテストするには、 NFS 管理ホストにログインし、 SVM に対するデータの読み取りと書き込みが可能かどうかを確認します。その後、 root 以外のユーザとしてクライアントシステム上で処理を繰り返します。

開始する前に

- クライアントシステムに、前に指定したエクスポートルールで許可されている IP アドレスが割り当てられている必要があります。
- root ユーザのログイン情報が必要です。

手順

1. クラスタで、新しいボリュームをホストしている LIF の IP アドレスを確認します。

   `network interface show -vserver svm_name`

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. 管理ホストクライアントシステムに root ユーザとしてログインします。
3. ディレクトリをマウントフォルダに変更します。

   `cd /mnt/`

4. 新しいフォルダを作成し、 SVM の IP アドレスを使用してマウントします。

   a. 新しいフォルダの作成：+
   `mkdir /mnt/folder`

   b. この新しいディレクトリに新しいボリュームをマウントします。+
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. ディレクトリを新しいフォルダに変更します。+
   `cd folder`

   次のコマンドでは、 test1 という名前のフォルダを作成し、 IP アドレス 192.0.2.130 のボリューム vol1 をマウントフォルダ test1 にマウントして、ディレクトリを新しい test1 に変更しています。

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 新しいファイルを作成し、そのファイルが存在することを確認して、テキストを書き込みます。

   a. テストファイルを作成します。+
   `touch filename`

   b. ファイルが存在することを確認します。:+
   `ls -l filename`

c. 入力：+
`cat > filename`

テキストを入力してから Ctrl+D を押してテストファイルにテキストを書き込みます。

d. テストファイルの内容を表示します。+
`cat filename`

e. テストファイルを削除します。+
`rm filename`

f. 親ディレクトリに戻ります。+
`cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. root として、マウントされたボリュームに対する必要な UNIX の所有権と権限を設定します。
7. エクスポートルールで特定されている UNIX クライアントシステムで、新しいボリュームへのアクセス権を持つ許可されたユーザとしてログインし、手順 3 ~ 5 を繰り返して、ボリュームのマウントとファイルの作成が可能なことを確認します。

ONTAP NFSの追加情報はどこで入手できますか

NFSクライアントアクセスをテストしたあと、NFSの追加設定を行ったり、SANアクセスを追加したりできます。プロトコルアクセスが完了したら、Storage Virtual Machine（SVM）のルートボリュームを保護する必要があります。

NFSの設定

NFSアクセスについてさらに詳しく設定するには、次の情報やテクニカルレポートを参照してください。

- "NFSの管理"

  NFSを使用したファイルアクセスを設定および管理する方法について説明します。

- "NetAppテクニカルレポート4067：『NFS Best Practice and Implementation Guide』"

  NFSv3およびNFSv4の運用ガイドであり、NFSv4を中心にONTAPオペレーティングシステムの概要を説明しています。

- "NetAppテクニカルレポート4073：『Secure Unified Authentication』"

NFSストレージ認証用にUNIXベースのKerberosバージョン5（krb5）サーバを使用し、KDCおよびLightweight Directory Access Protocol（LDAP）のアイデンティティプロバイダとしてWindows Server Active Directory（AD）を使用するようにONTAPを設定する方法について説明します。

- "NetAppテクニカルレポート3580：『NFSv4の拡張機能とベストプラクティスガイド：Data ONTAPでの実装』"

  ONTAPを実行するシステムに接続されたAIX、Linux、またはSolarisクライアントにNFSv4のコンポーネントを実装する際のベストプラクティスを紹介しています。

ネットワーク構成

ネットワーク機能とネームサービスについてさらに詳しく設定するには、次の情報およびテクニカルレポートを参照してください。

- "NFSの管理"

  ONTAPネットワークを設定および管理する方法について説明します。

- "NetAppテクニカルレポート4182：『clustered Data ONTAP構成でのイーサネットストレージの設計時の考慮事項とベストプラクティス』"

  ONTAPネットワーク構成の実装について説明し、一般的なネットワーク導入シナリオとベストプラクティスの推奨事項を提供します。

- "NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

  認証用にLDAP、NIS、DNS、およびローカルファイルを設定する方法について説明します。

SANプロトコルの設定

新しいSVMに対するSANアクセスを提供または変更する場合は、FCまたはiSCSIの設定情報を使用します。この情報は、複数のホストオペレーティングシステムに関するものです。

ルートボリュームの保護

SVMでプロトコルを設定したら、ルートボリュームを保護してください。

- "データ保護"

  負荷共有ミラーを作成してSVMルートボリュームを保護する方法について説明しています。これは、NAS対応のSVMに対するNetAppのベストプラクティスです。また、SVMルートボリュームを負荷共有ミラーから昇格させてボリュームの障害や損失からリカバリする簡単な方法についても説明しています。

ONTAPエクスポートと7-Modeエクスポートの違い

ONTAPエクスポートと**7-Mode**エクスポートの違い

ONTAPでNFSエクスポートを実装する方法に精通していない場合は、7-ModeとONTAPのエクスポート設定ツールを比較したり、サンプルの7-Modeファイルをクラスタ化され

たポリシーやルールと比較し `/etc/exports`たりできます。

ONTAPにはファイルもコマンドもあり `exportfs`ませ `/etc/exports`ん。代わりに、エクスポートポリシーを定義する必要があります。エクスポートポリシーを使用すると、7-Modeとほぼ同じ方法でクライアントアクセスを制御できますが、同じエクスポートポリシーを複数のボリュームで再利用するなどの機能が追加されています。

関連情報

"NFSの管理"

"NetAppテクニカルレポート4067：『NFS Best Practice and Implementation Guide』"

7-Modeと**ONTAP**の**NFS**エクスポートの比較について学ぶ

ONTAPでのエクスポートの定義と使用方法は、7-Mode環境とは異なります。

相違点	7-Mode	ONTAP
エクスポートの定義方法	エクスポートはファイルで定義され `/etc/exports`ます。	エクスポートは、SVM内でエクスポートポリシーを作成することによって定義されます。SVMには複数のエクスポートポリシーを含めることができます。
エクスポートの範囲	• エクスポートは指定したファイルパスまたはqtreeに適用されます。 • ファイルパスまたはqtreeごとに、に個別のエントリを作成する必要があります `/etc/exports`。 • エクスポートは、ファイルに定義されている場合にのみ保持され `/etc/exports`ます。	• エクスポートポリシーは、ボリューム内のすべてのファイルパスとqtreeを含むボリューム全体に適用されます。 • エクスポートポリシーは、必要に応じて複数のボリュームに適用できます。 • すべてのエクスポートポリシーは、システムの再起動後も維持されます。
フェンシング（特定のクライアントに対して同じリソースへの別のアクセスを指定すること）	特定のクライアントに単一のエクスポートされたリソースへの異なるアクセスを提供するには、各クライアントとその許可されているアクセスをファイル内でリストする必要が `/etc/exports`あります。	エクスポートポリシーは、複数のエクスポートルールで構成されています。各エクスポートルールでは、リソースに対する特定のアクセス権限が定義され、その権限を持つクライアントがリストされます。特定のクライアントに対して異なるアクセスを指定するには、アクセス権限の特定のセットごとにエクスポートルールを作成し、それらの権限を持つクライアントをリストして、エクスポートポリシーにルールを追加する必要があります。

名前のエイリアス設定	エクスポートを定義するときに、エクスポートの名前をファイルパスの名前とは別の名前にすることができます。このようなエクスポートをファイルで定義する場合は、パラメータを `/etc/exports` 使用する必要があります `-actual`。	エクスポートされたボリュームの名前として、実際のボリューム名とは異なる名前を選択できます。そのためには、カスタムジャンクションパス名を持つボリュームをSVMネームスペース内でマウントする必要があります。 デフォルトでは、ボリュームはそのボリューム名でマウントされます。ボリュームのジャンクションパス名をカスタマイズするには、アンマウントし、名前を変更してから再マウントする必要があります。

ONTAP NFSエクスポートポリシーの例について学ぶ

エクスポートポリシーの例を確認すると、 ONTAP でのエクスポートポリシーの動作について理解を深めることができます。

7-Mode エクスポートの ONTAP 実装例

次の例は、ファイルに出力されている7-Modeエクスポートを示してい `/etc/export` ます。

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

このエクスポートをクラスタエクスポートポリシーとして再現するには、 3 つのエクスポートルールを含むエクスポートポリシーを作成し、そのエクスポートポリシーをボリューム vol1 に割り当てる必要があります。

ルール	要素	値
ルール1	`-clientmatch`（クライアント仕様）	`@readonly_netgroup`
`-ruleindex`（ルールリスト内でのエクスポートルールの位置）	`1`	`-protocol`
`nfs`	`-rorule`（読み取り専用アクセスを許可）	`sys`（クライアントはAUTH_SYSで認証されます）

ルール	要素	値
-rwrule（読み取り/書き込みアクセスを許可）	never	-superuser（スーパーユーザアクセスを許可）
none（root_squashed_to anon）	ルール2	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	ルール3
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. exp_vol1というエクスポートポリシーを作成します。

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. 基本コマンドに対して、次のパラメータを指定して 3 つのルールを作成します。
   - 基本コマンド：+
     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```
   - ルールパラメータ：
     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none+ -clientmatch @rootaccess_netgroup -ruleindex
     2 -protocol nfs -rorule sys -rwrule sys -superuser sys -clientmatch
     @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule
     sys -rwrule sys -superuser none
     ```

3. ボリュームvol1にポリシーを割り当てます。

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

7-Mode エクスポートの統合の例

次の例は、qtree 10個につき1行で構成された7-Modeのファイルを示してい `/etc/export`ます。

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

ONTAPでは、qtreeごとに、を含むルールが設定されたポリシーとを含むルールが設定 `-clientmatch host2057s`されたポリシーのどちらかが必要です。 `-clientmatch host1519s`

1. exp_vol1q1 と exp_vol1q2 という 2 つのエクスポートポリシーを作成します。
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. 各ポリシーのルールを作成します。
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. ポリシーを qtree に適用します。
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [続く 4 つの qtree …]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [続く 4 つの qtree …]

これらのホスト用に qtree をあとから追加する必要がある場合は、同じエクスポートポリシーを使用します。

CLIを使用したNFSの管理

NFSプロトコルのONTAPファイルアクセスについて学ぶ

ONTAPには、NFSプロトコルで使用できるファイルアクセス機能があります。NFSサーバを有効にし、ボリュームまたはqtreeをエクスポートできます。

これらの手順は、次の状況で実行します。

- ONTAP NFSプロトコルの機能の範囲について理解する必要がある。

- NFSの基本的な設定ではなく、あまり一般的でない設定タスクとメンテナンスタスクを実行する。
- System Managerや自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

NASファイルアクセスについて理解する

ネームスペースとジャンクションポイント

ONTAP NASのネームスペースとジャンクションポイントについて学ぶ

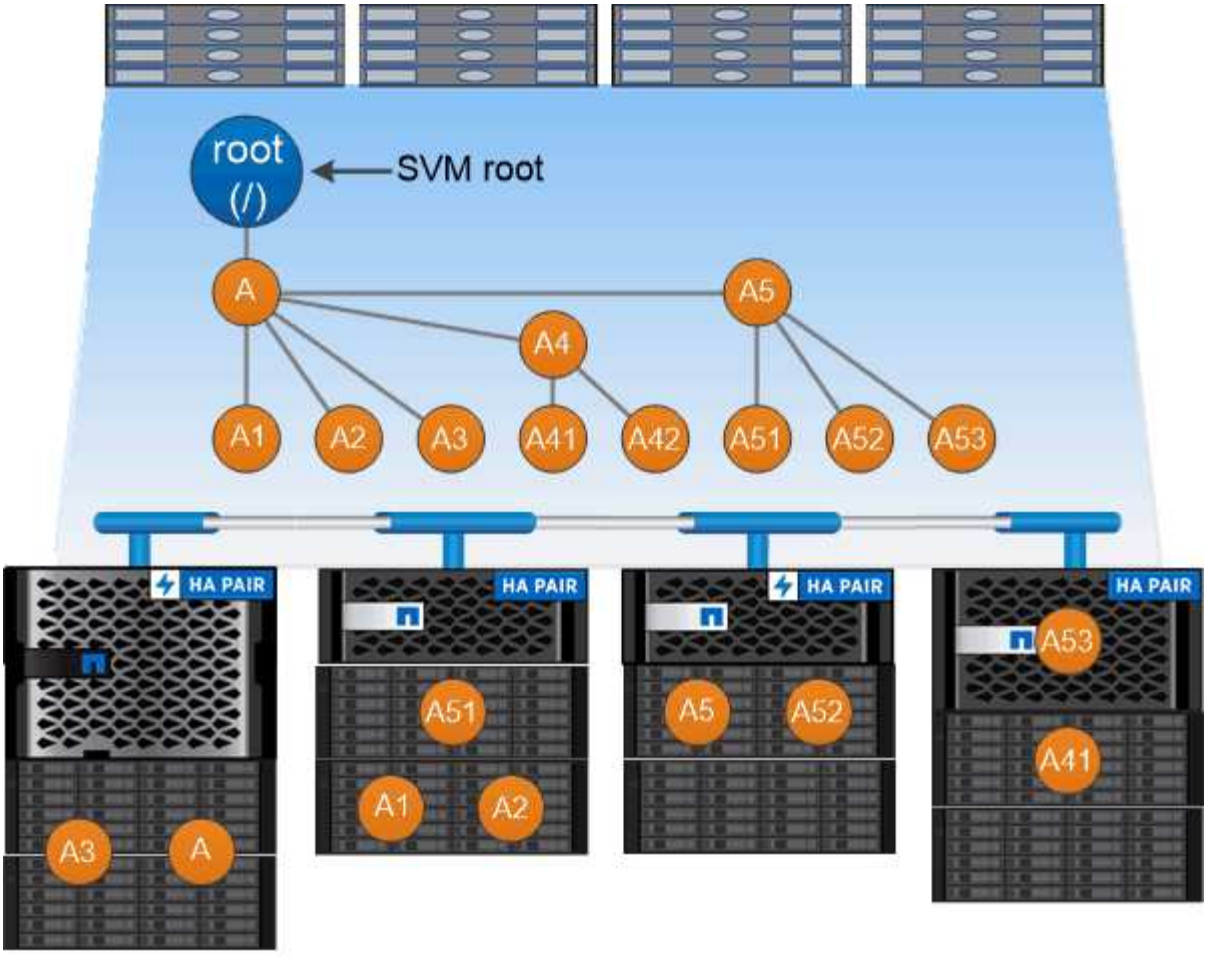
nas_namespace _ は、 _junction points_to によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限があるクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

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

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

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

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



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

例

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

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

ONTAP NASネームスペースアーキテクチャについて学ぶ

SVM ネームスペースを作成するときに使用できる一般的な NAS ネームスペースアーキテクチャがいくつかあります。ビジネスやワークフローのニーズに合ったネームスペースアーキテクチャを選択できます。

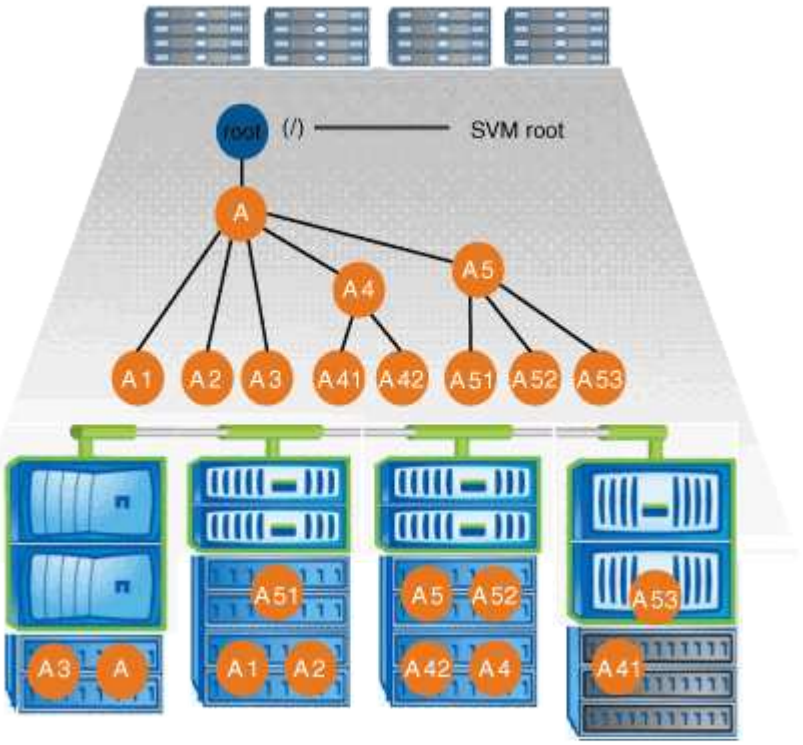
ネームスペースの最上位は常にルートボリュームで、スラッシュ（/）で表されます。ルートの下のネームスペースアーキテクチャは、次の3つの基本カテゴリに分類されます。

- ネームスペースのルートへのジャンクションが1つだけの単一分岐ツリー

- ネームスペースのルートへのジャンクションポイントが複数ある複数分岐ツリー
- ネームスペースのルートへの個別のジャンクションポイントを持つ複数のスタンドアロンボリューム

単一分岐ツリーを使用するネームスペース

単一分岐のツリーを使用するアーキテクチャには、 SVM ネームスペースのルートへの単一の挿入ポイントがあります。単一の挿入ポイントには、ジャンクションされたボリュームまたはルート直下のディレクトリを指定できます。他のすべてのボリュームは、単一の挿入ポイント（ボリュームまたはディレクトリ）の下のジャンクションポイントでマウントされます。

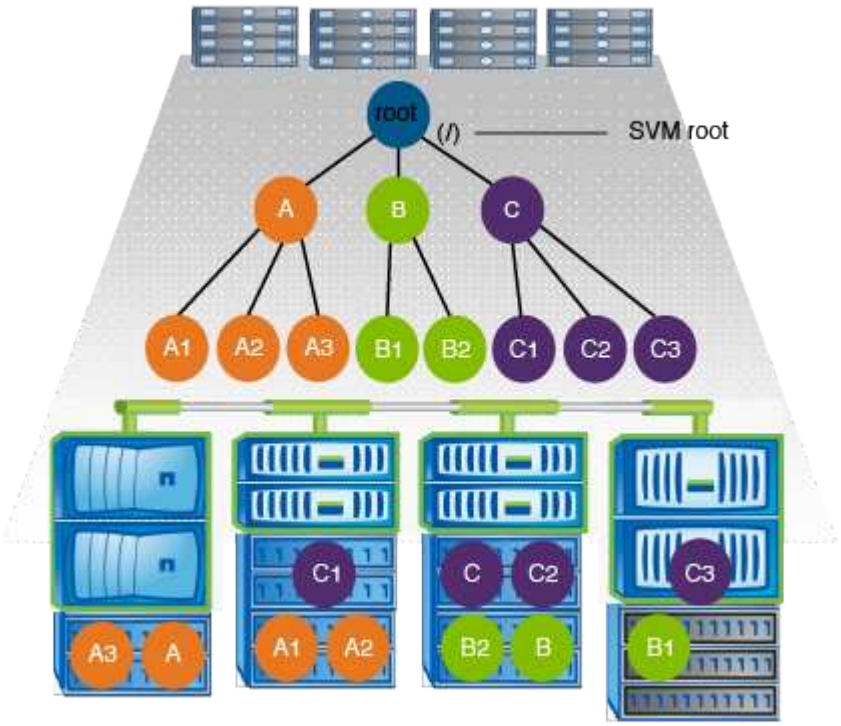


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、すべてのボリュームが単一の挿入ポイントの下で結合された以下のような構成になります。これは「 `d ATA` 」というディレクトリです。

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     corp1       true     /data/dir1/corp1         RW_volume
vs1     corp2       true     /data/dir1/corp2         RW_volume
vs1     data1       true     /data/data1              RW_volume
vs1     eng1        true     /data/data1/eng1         RW_volume
vs1     eng2        true     /data/data1/eng2         RW_volume
vs1     sales       true     /data/data1/sales        RW_volume
vs1     vol1        true     /data/vol1               RW_volume
vs1     vol2        true     /data/vol2               RW_volume
vs1     vol3        true     /data/vol3               RW_volume
vs1     vs1_root    -        /                        -
```

複数分岐ツリーを使用するネームスペース

複数分岐のツリーを使用するネームスペースには、 SVM ネームスペースのルートへの複数の挿入ポイントがあります。挿入ポイントは、ルートの下にジャンクションされたボリュームまたはディレクトリのいずれかです。他のすべてのボリュームは、挿入ポイントの下のジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。

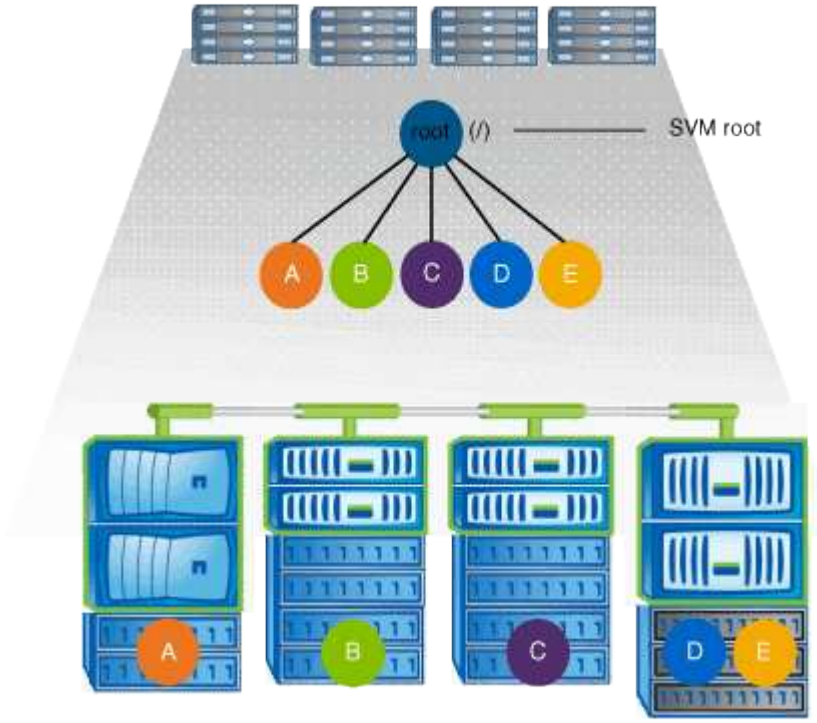


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、 SVM のルートボリュームへの 3 つの挿入ポイントがある以下のような構成になります。2 つの挿入ポイントは、「 `d ata" 」と「 projects' 」という名前のディレクトリです。挿入ポイントの 1 つは「 audit 」という名前の結合されたボリュームです。

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

複数のスタンドアロンボリュームを使用するネームスペース

スタンドアロンボリュームを使用するアーキテクチャでは、すべてのボリュームに SVM ネームスペースのルートへの挿入ポイントがありますが、それらのボリュームは別のボリュームの下でジャンクションされません。各ボリュームには一意のパスがあり、ルート直下でジャンクションされるか、ルートより下のディレクトリでジャンクションされます。



たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 5 つの挿入ポイントがあり、それぞれが 1 つのボリュームへのパスを表す以下のような構成になります。

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

ONTAPによるファイルアクセスの制御方法

ONTAP NASファイルアクセス制御について学ぶ

ONTAP は、指定された認証ベースおよびファイルベースの制限に従って、ファイルアクセスを制御します。

クライアントがファイルにアクセスするためにストレージシステムに接続するとき、 ONTAP は 2 つのタスクを実行する必要があります。

- 認証

  ONTAP は、信頼できるソースで ID を検証して、クライアントを認証する必要があります。また、クライアントの認証タイプは、エクスポートポリシーの設定時にクライアントがデータにアクセスできるかどうかの判断に使用できる方法の 1 つです（ CIFS の場合は省略可能）。

- 許可

  ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに設定されている権限を比較し、提供するアクセスのタイプ（ある場合）を判別することで、ユーザを許可する必要があります。

ファイルアクセス制御を適切に管理するため、 ONTAP は、 NIS 、 LDAP 、および Active Directory サーバなどの外部サービスと通信します。CIFS または NFS を使用するストレージシステムのファイルアクセスを設定するには、 ONTAP の環境に応じて、サービスを適切に設定する必要があります。

ONTAP NAS SVM の認証ベースの制限について学習します

認証ベースの制限を使用すると、Storage Virtual Machine（SVM）に接続できるクライアントマシンおよびユーザを指定できます。

ONTAP は、 UNIX サーバおよび Windows サーバの両方からの Kerberos 認証をサポートします。

ONTAP NAS SVM のファイルベースの制限について学ぶ

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

どのストレージオブジェクトにも、最大 3 種類のセキュリティレイヤを含めることができます。

- エクスポート（NFS）および共有（SMB）セキュリティ

  エクスポートおよび共有セキュリティは、特定のNFSエクスポートまたはSMB共有へのクライアントアクセスに適用されます。管理Privilegesを持つユーザは、SMBクライアントおよびNFSクライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルとディレクトリのセキュリティ

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

  NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護セキュリティは表示されません。システム（WindowsまたはUNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。

- NTFS、UNIX、およびNFSv4の標準のファイルレベルセキュリティ

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

ONTAPによる**NFS**クライアント認証の処理

NASクライアントの**ONTAP**認証について学ぶ

NFSクライアントからSVM上のデータにアクセスするには、NFSクライアントが正しく認証されている必要があります。ONTAPは、UNIXクレデンシャルを設定されたネームサービスに照らしてチェックすることで、クライアントを認証します。

NFSクライアントがSVMに接続すると、ONTAPは、SVMのネームサービス設定に応じて複数のネームサービスをチェックすることで、そのユーザのUNIXクレデンシャルを取得します。ONTAPでは、ローカルUNIXアカウント、NISドメイン、およびLDAPドメインのクレデンシャルをチェックできます。ONTAPがユーザを正常に認証できるように、これらのうち少なくとも1つを設定する必要があります。複数のネームサービスと、ONTAPによる検索順序を指定できます。

UNIXのボリュームセキュリティ形式を使用する純粋なNFS環境では、この設定だけでNFSクライアントから接続しているユーザが認証され、適切なファイルアクセスが提供されます。

mixed、NTFS、またはunifiedのボリュームセキュリティ形式を使用している場合、ONTAPがUNIXユーザをWindowsドメインコントローラで認証するためにはSMBユーザ名を取得する必要があります。これには、ローカルのUNIXアカウントまたはLDAPドメインを使用して個 々 のユーザをマッピングするか、代わりにデフォルトのSMBユーザを使用します。ONTAPが検索するネームサービスの種類と検索順序を指定することも、デフォルトのSMBユーザを指定することもできます。

ONTAP がネームサービスを使用する方法を学ぶ

ONTAPは、ネームサービスを使用してユーザとクライアントに関する情報を取得します。ONTAPは、この情報を使用して、ストレージシステム上でデータにアクセスしたりストレージシステムを管理したりするユーザの認証や、混在環境でのユーザクレデンシャルのマッピングを行います。

ストレージシステムを設定する場合は、ONTAPが認証用のユーザクレデンシャルを取得するために使用するネームサービスを指定する必要があります。ONTAPは次のネームサービスをサポートしています。

- ローカルユーザ（ファイル）
- 外部NISドメイン（NIS）
- 外部LDAPドメイン（LDAP）

ネットワーク情報を検索するソースやソースの検索順序をSVMで設定するには、コマンドファミリーを使用し `vserver services name-service ns-switch`ます。これらのコマンドは、UNIXシステムのファイルと同等の機能を提供し `/etc/nsswitch.conf`ます。

NFS クライアントが SVM に接続すると、 ONTAP は指定されたネームサービスをチェックして、ユーザの UNIX クレデンシャルを取得します。ネームサービスが正しく設定されていて、ONTAPがUNIXクレデンシャルを取得できる場合、ONTAPはユーザの認証に成功します。

mixedセキュリティ形式の環境では、ONTAPによるユーザクレデンシャルのマッピングが必要になる場合があります。ONTAPでユーザクレデンシャルが適切にマッピングされるようにするには、環境のネームサービスを適切に設定する必要があります。

ONTAP は、 SVM 管理者アカウントの認証にもネームサービスを使用します。ネームサービススイッチを設定または変更する際にはこの点を念頭に置いて、 SVM 管理者アカウントの認証を誤って無効にしないようにする必要があります。SVM管理ユーザの詳細については、を参照してください"カンリシヤニンシヨウトRBAC"。

NFSクライアントから**ONTAP SMB**ファイルへのアクセスを許可する

ONTAP では、 NTFS （ Windows NT ファイルシステム）のセキュリティセマンティクスを利用して、 NTFS アクセス権によるファイルへのアクセス権が、 NFS クライアント上の UNIX ユーザにあるかどうかが判別されます。

ONTAPでは、ユーザのUNIXユーザID（UID）をSMBクレデンシャルに変換し、そのクレデンシャルを使用してユーザにファイルへのアクセス権があることを確認します。SMBクレデンシャルは、プライマリのSecurity Identifier（SID；セキュリティ識別子）（通常はユーザのWindowsユーザ名）と、ユーザが属しているWindowsグループに対応する1つ以上のグループSIDで構成されます。

ONTAPがUNIX UIDをSMBクレデンシャルに変換するのにかかる時間は、数十ミリ秒から数百ミリ秒です。これは、この処理にドメインコントローラへの問い合わせも含まれるためです。ONTAPはUIDをSMBクレデンシャルにマッピングし、クレデンシャルキャッシュにマッピングを入力して変換によって発生する検証時間を短縮します。

ONTAP NFS認証情報キャッシュの仕組み

NFS ユーザがストレージシステム上の NFS エクスポートへのアクセスを要求すると、

ONTAP は、ユーザの認証を行うために外部ネームサーバまたはローカルファイルからユーザクレデンシャルを取得する必要があります。ONTAPは、後で参照できるように、これらのクレデンシャルを内部クレデンシャルキャッシュに格納します。NFSクレデンシャルキャッシュの仕組みを理解することで、パフォーマンスやアクセスに関する潜在的な問題に対処できます。

クレデンシャルキャッシュがないと、 ONTAP ユーザは NFS ユーザからアクセスが要求されるたびにネームサービスを照会しなければなりません。多数のユーザがアクセスする使用頻度の高いストレージシステムでは、こうした状況がすぐに深刻なパフォーマンス上の問題につながり、不必要な遅延や、場合によっては NFS クライアントアクセスの拒否さえ引き起こす可能性があります。

クレデンシャルキャッシュがあれば、 ONTAP は取得したユーザクレデンシャルをあらかじめ決められた期間だけ格納しておき、同じ NFS クライアントから再び要求があっても迅速かつ簡単にアクセスすることができます。この方法には、次の利点があります。

- 外部ネームサーバ（ NIS や LDAP など）への要求の処理を減らすことで、ストレージシステムの負荷が軽減されます。
- 外部ネームサーバに送信する要求を減らすことで、外部ネームサーバの負荷が軽減されます。
- ユーザが認証される前に外部ソースからクレデンシャルを取得するための待機時間をなくすことで、ユーザアクセスを高速化します。

ONTAP は、受理されたクレデンシャルと拒否されたクレデンシャルの両方をクレデン受理されたクレデンシャルとは、ユーザが認証されてアクセス権を付与されたこと拒否されたクレデンシャルとは、ユーザが認証されずにアクセスが拒否されたことを意味します

デフォルトでは、ONTAPは受理されたクレデンシャルを24時間保存します。つまり、ユーザの初回認証後、ONTAPはそのユーザからのすべてのアクセス要求に対してキャッシュされたクレデンシャルを24時間使用します。24 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 ONTAP はキャッシュされたクレデンシャルを破棄し、適切なネームサービスソースから再びクレデンシャルを取得します。それまでの24時間にネームサーバ上でクレデンシャルが変更された場合、ONTAPは更新されたクレデンシャルをキャッシュして、次の24時間で使用できるようにします。

デフォルトでは、ONTAPは拒否されたクレデンシャルを2時間保存します。つまり、ユーザへのアクセスを最初に拒否したあと、ONTAPはそのユーザからのすべてのアクセス要求を2時間拒否し続けます。2 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 ONTAP は適切なネームサービスソースから再びクレデンシャルを取得します。過去2時間にネームサーバ上でクレデンシャルが変更された場合、ONTAPは次の2時間で使用できるように、更新されたクレデンシャルをキャッシュします。

NASネームスペースでのデータボリュームの作成と管理

指定されたジャンクションポイントを持つ ONTAP NAS ボリュームを作成する

ジャンクションポイントは、データボリュームの作成時に指定できます。作成したボリュームはジャンクションポイントに自動的にマウントされ、NASアクセス用の設定にすぐに使用できます。

開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量

またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

ジャンクションパスに次の文字は使用できません。 `* # " > < | ? \`

また、ジャンクションパスの長さは255文字以下にする必要があります。

手順

1. ジャンクションポイントを設定してボリュームを作成します。

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

ジャンクションパスはルート（/）で始まる必要があり、ディレクトリと結合されたボリュームの両方を含めることができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAP はStorage Virtual Machine（SVM）のルートボリュームと同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームに適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

ジャンクションパスでは大文字と小文字が区別されません。はと同じ `/eng`です。 `/ENG`CIFS共有を作成する場合、Windowsではジャンクションパスは大文字と小文字が区別されるかのように扱われます。たとえば、ジャンクションがの場合、 `/ENG`SMB共有のパスはではなくで `/eng`始まる必要があります `/ENG`。

データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

例

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

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

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

特定のジャンクションポイントなしで**ONTAP NAS**ボリュームを作成する

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にはマウントされず、NASアクセス用に設定することもできません。ボリュームに対してSMB共有またはNFSエクスポートを設定するには、ボリュームをマウントする必要があります。

開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. 次のコマンドを使用して、ジャンクションポイントが設定されていないボリュームを作成します。

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリュームと同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームに適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

2. ボリュームがジャンクションポイントなしで作成されたことを確認します。

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

例

次の例は、ジャンクションポイントにマウントされない「 sales 」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NASネームスペースで**ONTAP NFS**ボリュームをマウントまたはアンマウントする

Storage Virtual Machine（SVM）ボリュームに格納されたデータへのNASクライアントからのアクセスを設定するには、ボリュームがNASネームスペースにマウントされている必要があります。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームをアンマウントすることもできます。

タスクの内容

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、ジャンクションポイント内のすべてのデータにNASクライアントからアクセスできなくなります。

> ボリュームへのNASクライアントアクセスを中止するには、ボリュームをアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次の技術情報アーティクルを参照してください。
>
> "ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"

ボリュームをアンマウントしてオフラインにしても、ボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーと、ボリュームまたはディレクトリに作成されたSMB共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすると、NASクライアントは既存のエクスポートポリシーとSMB共有を使用してボリュームに格納されているデータにアクセスできます。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームのマウント	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

ボリュームのアンマウント	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例は、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ONTAP NASボリュームのマウントポイントとジャンクションポイントの情報を表示します。

Storage Virtual Machine（SVM）のマウントボリューム、およびボリュームがマウントされているジャンクションポイントに関する情報を表示できます。ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVMネームスペースを理解し、管理することができます。

ステップ

1. 必要な操作を実行します。

表示する項目	入力するコマンド
SVMのマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver` *`vserver_name`* `-junction`
SVMのマウントされたボリュームとマウントされていないボリュームに関する詳細情報	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`

SVMのマウントされたボリュームとマウントされていないボリュームに関する特定の情報	a. 必要に応じて、次のコマンドを使用してパラメータの有効なフィールドを表示できます `-fields`。
	`volume show -fields ?`
	b. パラメータを使用して、必要な情報を表示し `-fields`ます。
	`volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

例

次の例では、SVM vs1のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

次の例は、SVM vs2上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

セキュリティ形式の設定

セキュリティ形式がデータアクセスに与える影響

ONTAP NASのセキュリティスタイルについて学ぶ

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式によって、データに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データ アクセスの制御にONTAPで使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームでUNIXセキュリティ形式を使用している場合でも、ONTAPはマルチプロトコルに対応しているため、SMBクライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAPでは、UNIXクライアントのみが標準のツールを使用して変更できるUNIX権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
UNIX	NFS	NFSv3モードビット	UNIX	NFSとSMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
mixed	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
unified （ Infinite Volume のみ、ONTAP 9.4 以前のリリース）	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVolでは、UNIX、NTFS、およびmixedのセキュリティ形式がサポートされます。セキュリティ形式がmixedまたはunifiedの場合、ユーザはセキュリティ形式を個別に設定するため、権限を最後に変更したクライアントのタイプによって有効な権限が異なります。権限を最後に変更したクライアントがNFSv3クライアントの場合、権限はUNIX NFSv3モードビットになります。最後のクライアントがNFSv4クライアントの場合、権限はNFSv4 ACLになります。最後のクライアントがSMBクライアントの場合、権限はWindows NTFS ACLになります。

unifiedセキュリティ形式は、Infinite Volumeでのみ使用できます。Infinite Volumeは、ONTAP 9 .5以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

その `show-effective-permissions`パラメータを `vserver security file-directory`コマンドを使用すると、指定されたファイルまたはフォルダー パスで `Windows` または `UNIX` ユーザーに付与された有効な権限を表示できます。また、オプションのパラメータを `-share-name`使用すると、有効な共有権限を表示できます。の詳細については `vserver security file-directory show-effective-permissions`、を"ONTAPコマンド リファレンス"参照してください。

> ONTAPは、最初に一部のデフォルトのファイル権限を設定します。デフォルトでは、UNIX、mixed、およびunifiedのセキュリティ形式のボリュームにあるデータには、セキュリティ形式はUNIXになり、アクセス権のタイプはUNIXモードビット（特に指定がないかぎり0755）になります。これは、デフォルトのセキュリティ形式で許可されるようにクライアントによって設定されるまでの間です。デフォルトでは、NTFSセキュリティ形式のボリューム内のすべてのデータに対するセキュリティ形式はNTFSになり、すべてのユーザにフルコントロールを許可するACLが割り当てられます。

関連情報

- "ONTAPコマンド リファレンス"

ONTAP NFS FlexVol ボリュームのセキュリティスタイルについて学習します

セキュリティ形式は、 FlexVol （ルートボリュームとデータボリュームの両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

ONTAP NAS SVMで使用するセキュリティスタイルを決定する

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります。主な要因は、ファイルシステムを管理する管理者のタイプです。2番目の要因は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームでセキュリティ形式を設定する場合は、最適なセキュリティ形式を選択し、権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定には、次の考慮事項が役立ちます。

セキュリティ形式	以下の場合に選択
UNIX	• ファイルシステムはUNIX管理者によって管理されます。 • ユーザの大半がNFSクライアントである。 • データにアクセスするアプリケーションでは、UNIXユーザをサービスアカウントとして使用します。
NTFS	• ファイルシステムはWindows管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションでは、Windowsユーザをサービスアカウントとして使用します。
mixed	• ファイルシステムはUNIX管理者とWindows管理者の両方によって管理され、ユーザはNFSクライアントとSMBクライアントの両方で構成されます。

ONTAPの**NFS**セキュリティ形式の継承について

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAP NFS UNIX権限の保持について学ぶ

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

Windowsのセキュリティタブを使用して、**ONTAP NFS SVM**の**UNIX**権限を管理する

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 Windows クライアントのセキュリティタブを使用できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

  モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

ONTAP NFS SVMルートボリュームのセキュリティスタイルを設定する

Storage Virtual Machine（SVM）のルートボリューム上のデータに使用するアクセス権のタイプを決定するには、SVMルートボリュームのセキュリティ形式を設定します。

手順

1. セキュリティ形式を定義するには、コマンドで `-rootvolume-security-style`パラメータを使用し `vserver create`ます。

   ルートボリュームのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

2. 作成した SVM のルートボリュームセキュリティ形式を含む設定を表示して確認します。

   `vserver show -vserver vserver_name`

ONTAP NFS FlexVolボリュームのセキュリティスタイルを設定する

Storage Virtual Machine（SVM）のFlexVol上のデータに使用するアクセス権のタイプを決定するには、FlexVol volumeセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
まだ存在しません	`volume create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

   FlexVol volumeセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

   FlexVol volumeの作成時にセキュリティ形式を指定しない場合、ボリュームはルートボリュームのセキュリティ形式を継承します。

   コマンドまたは `volume modify`コマンドの詳細については `volume create`、を参照してください"論理ストレージ管理"。

2. 作成したFlexVol volumeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

   `volume show -volume volume_name -instance`

ONTAP NFS qtreeのセキュリティスタイルを設定する

qtree上のデータに使用するアクセス権のタイプを決定するには、qtreeボリュームのセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
まだ存在しません	`volume qtree create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume qtree modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

qtreeのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

コマンドまたは `volume qtree modify`コマンドの詳細については `volume qtree create`、を参照してください"論理ストレージ管理"。

2. 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。 `volume qtree show -qtree qtree_name -instance`

NFSを使用したファイルアクセスの設定

ONTAP SVM での **NFS** ファイルアクセスの設定について学習します

クライアントがNFSを使用してStorage Virtual Machine（SVM）上のファイルにアクセスできるようにするには、いくつかの手順を実行する必要があります。環境の現在の構成に応じて、追加の手順がいくつかあります。

クライアントがNFSを使用してSVMのファイルにアクセスできるようにするには、次のタスクを実行する必要があります。

1. SVMでNFSプロトコルを有効にします。

   クライアントからNFS経由のデータアクセスを許可するようにSVMを設定する必要があります。

2. SVMにNFSサーバを作成

   NFSサーバは、NFS経由でファイルを提供できるようにするSVM上の論理エンティティです。NFSサーバを作成し、許可するNFSプロトコルのバージョンを指定する必要があります。

3. SVMでエクスポートポリシーを設定します。

   エクスポートポリシーを設定して、クライアントがボリュームとqtreeを使用できるようにする必要があります。

4. ネットワークやストレージの環境に応じて、適切なセキュリティ設定やその他の設定でNFSサーバを構成します。

   この手順には、Kerberos、LDAP、NIS、ネームマッピング、およびローカルユーザの設定が含まれます。

エクスポート ポリシーを使用した**NFS**アクセスの保護

エクスポートポリシーが**ONTAP NFS**ボリュームまたは**qtree**へのクライアントアクセスを制御する方法

エクスポートポリシーには、各クライアントアクセス要求を処理する 1 つ以上の _ エクスポートルール _ が含まれています。このプロセスの結果、クライアントアクセスを許可するかどうか、およびアクセスのレベルが決まります。クライアントがデータにアクセスするためには、エクスポートルールを含むエクスポートポリシーがStorage Virtual Machine（SVM）上に存在する必要があります。

ボリュームまたは qtree へのクライアントアクセスを設定するには、各ボリュームまたは qtree にポリシーを 1 つ関連付けます。SVM には複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームまたは qtree を含む SVM に対して次の操作を実行できます。

- SVM のボリュームまたは qtree ごとに異なるエクスポートポリシーを割り当て、 SVM の各ボリュームまたは qtree へのクライアントアクセスを個別に制御する。
- SVM の複数のボリュームまたは qtree に同じエクスポートポリシーを割り当て、同一のクライアントアクセス制御を実行する。ボリュームまたは qtree ごとに新しいエクスポートポリシーを作成する必要はありません。

クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントがエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポートポリシーが空の場合、すべてのアクセスが暗黙的に拒否されます。

エクスポートポリシーは、 ONTAP を実行しているシステム上で動的に変更できます。

ONTAP NFS SVMのデフォルトのエクスポートポリシー

各 SVM には、ルールが含まれていないデフォルトのエクスポートポリシーが用意されています。SVM 上のデータにクライアントからアクセスできるようにするには、ルールを備えたエクスポートポリシーを用意する必要があります。SVM 内の各 FlexVol にエクスポートポリシーを関連付ける必要があります。

SVMを作成すると、SVMのルートボリュームに対してという名前のデフォルトのエクスポートポリシーがストレージシステムによって自動的に作成され `default`ます。SVM上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを1つ以上作成する必要があります。または、ルールを備えたカスタムのエクスポートポリシーを作成することもできます。デフォルトのエクスポートポリシーは、変更および名前変更は可能ですが、削除することはできません。

SVM 内に FlexVol ボリュームを作成すると、作成されたボリュームには、 SVM のルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。デフォルトでは、 SVM に作成した各ボリュームには、ルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。SVM 内のすべてのボリュームでデフォルトのエクスポートポリシーを使用することも、ボリュームごとに独自のエクスポートポリシーを作成することもできます。複数のボリュームを同じエクスポートポリシーに関連付けることができます。

ONTAP NFSエクスポートルールの仕組み

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポートルールでは、ボリュームへのクライアントアクセス要求が設定した特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順序で処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致した場合、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用してクライアントアクセス権限を決定するようにエクスポートルールを設定できます。

- クライアントが要求の送信に使用するファイルアクセスプロトコル（NFSv4やSMBなど）。

- クライアント識別子（ホスト名やIPアドレスなど）。

  フィールドの最大サイズ `-clientmatch`は4096文字です。

- クライアントが認証に使用するセキュリティタイプ（Kerberos v5、NTLM、AUTH_SYSなど）。

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

> ONTAP 9 .3以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にして、すべてのルール違反をエラールールリストに記録できます。 `vserver export-policy config-checker`コマンドを実行するとチェックが呼び出されて結果が表示され、設定を確認したり、誤ったルールをポリシーから削除したりできます。
>
> このコマンドで検証されるのは、エクスポート設定のホスト名、ネットグループ、匿名ユーザのみです。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv3プロトコルを使用して送信され、クライアントのIPアドレスは10.1.17.37です。

クライアントアクセスプロトコルが一致していても、クライアントのIPアドレスがエクスポートルールで指定されているサブネットとは異なるサブネットに属しています。そのため、クライアント一致は失敗し、このルールはこのクライアントには適用されません。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントのIPアドレスが指定したサブネットにあります。したがって、クライアント一致は成功し、このルールはこのクライアントに適用されます。セキュリティタイプに関係なく、クライアントは読み取り/書き込みアクセス権を取得します。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されます。

両方のクライアントでクライアントアクセスプロトコルとIPアドレスが一致している。読み取り専用パラメータでは、認証に使用したセキュリティタイプに関係なく、すべてのクライアントに読み取り専用アクセスが許可されます。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

エクスポートルールのアクセスパラメータに指定されていないセキュリティタイプをクライアントが使用している場合は、アクセスパラメータのオプションを使用して、クライアントへのアクセスを拒否するか、クライアントを匿名ユーザIDにマッピングするかを選択できます。 `none`

クライアントは、別のセキュリティタイプで認証されているか、まったく認証されていない（セキュリティタイプAUTH_NONE）という理由で、アクセスパラメータに指定されていないセキュリティタイプを使用している可能性があります。デフォルトでは、クライアントはそのレベルへのアクセスを自動的に拒否されます。ただし、アクセスパラメータにはオプションを追加できます `none`。このため、リストにないセキュリティ形式を使用するクライアントは、代わりに匿名ユーザIDにマッピングされます。パラメータは `-anon`、これらのクライアントに割り当てるユーザIDを決定します。パラメータに指定するユーザID `-anon`は、匿名ユーザに適していると思われる権限が設定されている有効なユーザである必要があります。

パラメータの有効な値 `-anon`の範囲は `0~ `65535`です。

割り当てられたユーザ**ID** `-anon`	クライアントアクセス要求の処理結果
`0- 65533`	クライアントアクセス要求は匿名ユーザIDにマッピングされ、このユーザに設定されている権限に応じてアクセスを取得します。
`65534`	クライアントアクセス要求はユーザnobodyにマッピングされ、このユーザに設定されている権限に応じてアクセスできます。これがデフォルトです。

割り当てられたユーザID -anon	クライアントアクセス要求の処理結果
65535	すべてのクライアントからのアクセス要求は、このIDにマッピングされ、セキュリティタイプがAUTH_NONEであると拒否されます。ユーザIDが0のクライアントからのアクセス要求は、このIDにマッピングされ、クライアントが他のセキュリティタイプを使用している場合は拒否されます。

オプションを使用する場合は none、最初に読み取り専用パラメータが処理されることを覚えておくことが重要です。リストにないセキュリティタイプを使用するクライアントのエクスポートルールを設定する際は、次のガイドラインを考慮してください。

読み取り専用インクルード none	読み取り/書き込みに含まれるもの none	リストにないセキュリティタイプを使用するクライアントのアクセス結果
いいえ	いいえ	拒否されました
いいえ	○	最初に読み取り専用が処理されるため拒否されました
○	いいえ	匿名として読み取り専用
○	○	匿名として読み取り/書き込み

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule sys,none
- -rwrule any
- -anon 70

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されます。

クライアント#3は、IPアドレスが10.1.16.234で、NFSv3プロトコルを使用してアクセス要求を送信し、認証を行わなかった（セキュリティタイプAUTH_NONE）。

3つのクライアントすべてで、クライアントアクセスプロトコルとIPアドレスが一致しています。読み取り専用パラメータでは、読み取り専用アクセスがAUTH_SYSで認証された、自身のユーザIDを持つクライアントに許可されています。読み取り専用パラメータは、ユーザIDが70の匿名ユーザとして、他のセキュリティタイプを使用して認証されたクライアントに読み取り専用アクセスを許可します。読み取り/書き込みパラメー

タでは、読み取り/書き込みアクセスがすべてのセキュリティタイプに許可されていますが、この場合は、読み取り専用ルールですでにフィルタされているクライアントにのみ適用されます。

したがって、クライアント#1とクライアント#3は、ユーザIDが70の匿名ユーザとしてのみ読み取り/書き込みアクセス権を取得します。クライアント#2は、自身のユーザIDを使用して読み取り/書き込みアクセス権を取得します。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されます。

クライアント#3は、IPアドレスが10.1.16.234で、NFSv3プロトコルを使用してアクセス要求を送信し、認証を行わなかった（セキュリティタイプAUTH_NONE）。

3つのクライアントすべてで、クライアントアクセスプロトコルとIPアドレスが一致しています。読み取り専用パラメータでは、読み取り専用アクセスがAUTH_SYSで認証された、自身のユーザIDを持つクライアントに許可されています。読み取り専用パラメータは、ユーザIDが70の匿名ユーザとして、他のセキュリティタイプを使用して認証されたクライアントに読み取り専用アクセスを許可します。読み取り/書き込みパラメータでは、読み取り/書き込みアクセスは匿名ユーザとしてのみ許可されます。

したがって、クライアント#1とクライアント#3は、ユーザIDが70の匿名ユーザとしてのみ読み取り/書き込みアクセス権を取得します。クライアント#2は、自身のユーザIDで読み取り専用アクセス権を取得しますが、読み取り/書き込みアクセスは拒否されます。

ONTAP セキュリティタイプが NFS クライアントのアクセスレベルを決定する方法

クライアントの認証に使用されるセキュリティタイプは、エクスポートルールで特別な役割を果たします。クライアントがボリュームまたは qtree にアクセスする際のレベルがセキュリティタイプによってどのように決定されるかについて理解しておく必要があります。

アクセスレベルには、次の 3 つがあります。

1. 読み取り専用
2. 読み取り/書き込み
3. superuser （ユーザ ID が 0 のクライアントの場合）

セキュリティタイプに基づくアクセスレベルはこの順序で評価されるため、エクスポートルールでアクセスレ

ベルパラメータを作成するときは、次のルールに従う必要があります。

クライアントに必要なアクセスレベル	クライアントのセキュリティタイプと一致する必要があるアクセスパラメータ
標準ユーザの読み取り専用	読み取り(`-rorule`専用)
標準ユーザの読み取り / 書き込み	読み取り専用(`-rorule`）および読み取り/書き込み(`-rwrule`)
スーパーユーザの読み取り専用	読み取り専用(`-rorule`）および `-superuser`
スーパーユーザの読み取り / 書き込み	読み取り専用(`-rorule`）(`-rwrule`および `-superuser`読み取り/書き込み

これら3つの各アクセスパラメータで有効なセキュリティタイプは次のとおりです。

- `any`
- `none`
- `never`

  このセキュリティタイプは、パラメータでは使用できません `-superuser`。

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

クライアントのセキュリティタイプを 3 つの各アクセスパラメータと照合したときの結果としては、次の 3 つが考えられます。

クライアントのセキュリティタイプ	クライアント
アクセスパラメータで指定されたタイプと一致する。	独自のユーザ ID を使用して、そのレベルのアクセス権を取得します。
指定したタイプと一致しないが、アクセスパラメータにオプションが指定されている `none`。	このレベルのアクセス権を取得しますが、パラメータで指定したユーザIDを持つ匿名ユーザとして取得します `-anon`。
指定したタイプと一致しないため、アクセスパラメータにオプションが指定されていません。 `none`	は、そのレベルのアクセス権を取得しません。これは、指定されていない場合でも常にを含むため、パラメータには適用され `-superuser`ません。 `none`

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されています。

クライアント#3は、IPアドレスが10.1.16.234、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信しますが、認証は行われていません（AUTH_NONE）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、セキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。読み取り/書き込みパラメータは、読み取り/書き込みアクセスを、AUTH_SYSまたはKerberos v5で認証された、自身のユーザIDを持つクライアントに許可します。superuserパラメータでは、Kerberos v5で認証されたユーザIDが0のクライアントにスーパーユーザアクセスを許可します。

したがって、クライアント #1 は、 3 つすべてのアクセスパラメータに一致するため、スーパーユーザの読み取り / 書き込みアクセス権を取得します。クライアント #2 は、読み取り / 書き込みアクセス権を取得しますが、スーパーユーザアクセス権は取得できません。クライアント #3 は、読み取り専用アクセス権を取得しますが、スーパーユーザアクセス権は取得できません。

ONTAP NFSスーパーユーザーアクセス要求の管理について学習します

エクスポートポリシーを設定する際には、ストレージシステムがユーザ ID が 0 のクライアントアクセス要求をスーパーユーザとして受信し、それに応じてエクスポートルールを設定する場合に必要な処理を考慮する必要があります。

UNIX の世界では、ユーザ ID 0 のユーザがスーパーユーザと呼ばれ、通常は root と呼ばれます。このユーザにはシステム上で無制限のアクセス権が与えられています。スーパーユーザ権限の使用は、システムやデータセキュリティの侵害などのいくつかの理由によってリスクを伴う可能性があります。

デフォルトでは、 ONTAP はユーザ ID が 0 のクライアントを匿名ユーザにマッピングします。ただし、エクスポートルールでパラメータを指定すると、ユーザIDが0のクライアントの処理方法をセキュリティタイプに応じて決定できます - `superuser`。パラメータに有効なオプションは次のとおりです `-superuser`。

- `any`
- `none`

  これは、パラメータを指定しない場合のデフォルト設定 `-superuser`です。

- `krb5`

- ntlm
- sys

ユーザIDが0のクライアントは、パラメータの設定に応じて2つの方法で処理されます。 -superuser

`-superuser`パラメータとクライアントのセキュリティタイプ	クライアント
一致	ユーザ ID 0 でスーパーユーザアクセス権を取得します。
一致しません	パラメータで指定したユーザIDと、割り当てられた権限を持つ匿名ユーザとしてアクセスを取得します -anon。これは、読み取り専用パラメータと読み取り/書き込みパラメータのどちらでオプションが指定されているかに関係あり `none`ません。

クライアントがNTFSセキュリティ形式のボリュームにアクセスするためにユーザID 0を提示し、パラメータがに設定されている none`場合 `-superuser、ONTAPは匿名ユーザのネームマッピングを使用して適切なクレデンシャルを取得します。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule krb5,ntlm
- -anon 127

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが746で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されています。

両方のクライアントでクライアントアクセスプロトコルとIPアドレスが一致している。読み取り専用パラメータでは、認証に使用したセキュリティタイプに関係なく、すべてのクライアントに読み取り専用アクセスが許可されます。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。

クライアント #2 は、スーパーユーザアクセス権を取得できません。パラメータが指定されていないため、代わりに匿名にマッピングされ `-superuser`ます。つまり、デフォルトで `none`ユーザID 0が匿名にマッピングされ、自動的にマッピングされます。また、クライアント #2 はセキュリティタイプが読み取り / 書き込みパラメータと一致しなかったため、読み取り専用アクセス権のみを取得します。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されています。

両方のクライアントでクライアントアクセスプロトコルとIPアドレスが一致している。読み取り専用パラメータでは、認証に使用したセキュリティタイプに関係なく、すべてのクライアントに読み取り専用アクセスが許可されます。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

このエクスポートルールでは、ユーザ ID が 0 のクライアントにスーパーユーザアクセスが許可されています。クライアント#1は、読み取り専用パラメータとパラメータのユーザIDおよびセキュリティタイプと一致しているため、スーパーユーザアクセスを取得します。 `-superuser`クライアント#2のセキュリティタイプが読み取り/書き込みパラメータまたはパラメータと一致しないため、読み取り/書き込みアクセス権もスーパーユーザアクセス権も取得されません。 `-superuser`代わりに、クライアント #2 は匿名ユーザにマッピングされます。この場合、ユーザ ID は 0 です。

ONTAP NFSエクスポートポリシーキャッシュについて学ぶ

システムパフォーマンスを向上するために、 ONTAP はローカルキャッシュを使用してホスト名やネットグループなどの情報を格納します。これにより、 ONTAP は外部ソースから情報を取得するよりも迅速にエクスポートポリシールールを処理できます。キャッシュとは何か、またキャッシュによって何が行われるのかを理解すると、クライアントアクセスに関する問題のトラブルシューティングに役立ちます。

NFS エクスポートへのクライアントアクセスを制御するには、エクスポートポリシーを設定します。各エクスポートポリシーにはルールが含まれており、各ルールにはアクセスを要求しているクライアントに対するマッチングを行うパラメータが含まれています。これらのパラメータの一部では、ドメイン名、ホスト名、ネットグループなどのオブジェクトを解決するために ONTAP が DNS サーバや NIS サーバのような外部ソースと通信する必要があります。

外部ソースとの通信には少し時間がかかります。パフォーマンスを向上させるために、 ONTAP は、各ノード上の複数のキャッシュに情報をローカルに格納して、エクスポートポリシールールオブジェクトの解決にかかる時間を短縮します。

キャッシュ名	保存される情報のタイプ
アクセス	対応するエクスポートポリシーへのクライアントのマッピング

キャッシュ名	保存される情報のタイプ
名前	対応する UNIX ユーザ ID への UNIX ユーザ名のマッピング
ID	対応する UNIX ユーザ ID および拡張された UNIX グループ ID への UNIX ユーザ ID のマッピング
ホスト	対応する IP アドレスへのホスト名のマッピング
ネットグループ	メンバーの対応する IP アドレスへのネットグループのマッピング
showmount	SVM ネームスペースからエクスポートされたディレクトリのリスト

ONTAP が外部ネームサーバ上の情報を取得してローカルに格納したあとに、環境内の外部ネームサーバ上の情報を変更すると、キャッシュ内の情報が古くなる可能性があります。ONTAP は一定期間の経過後に自動的にキャッシュを更新しますが、有効期限や更新の時期およびアルゴリズムはキャッシュごとに異なります。

キャッシュに古くなった情報が含まれる理由としてもう 1 つ考えられるのは、 ONTAP がキャッシュされた情報の更新を試みたにもかかわらずネームサーバと通信しようとしてエラーが発生した場合です。この場合、ONTAP は、クライアントの中断を避けるために現在ローカルキャッシュに格納されている情報を引き続き使用します。

その結果、成功することが想定されるクライアントアクセス要求が失敗し、エラーとなることが想定されるクライアントアクセス要求が成功する可能性があります。クライアントアクセスに関するこのような問題のトラブルシューティング時には、エクスポートポリシーキャッシュの一部を表示したり、手動でフラッシュしたりできます。

ONTAP NFSアクセスキャッシュについて学ぶ

ONTAP は、アクセスキャッシュを使用して、ボリュームまたは qtree へのクライアントアクセス処理に対するエクスポートポリシールール評価の結果を格納します。これにより、クライアントから I/O 要求が送信されるたびにエクスポートポリシールール評価の処理を行う場合よりも、アクセスキャッシュから情報をはるかに短時間で取得できるため、パフォーマンスが向上します。

NFS クライアントがボリュームまたは qtree 上のデータにアクセスするための I/O 要求を送信するたびに、ONTAP はそれぞれの I/O 要求を評価して、その I/O 要求を許可するか拒否するかを決定する必要があります。この評価には、そのボリュームまたは qtree に関連付けられているすべてのエクスポートポリシールールのチェックが伴います。ボリュームまたは qtree へのパスが 1 つ以上のジャンクションポイントと交差している場合は、そのパスに付随する複数のエクスポートポリシーに対してこのチェックの実行が必要になる可能性があります。

なお、この評価は、最初のマウント要求についてだけでなく、読み取り、書き込み、リスト、コピーなどの処理を行う NFS クライアントから送信されたすべての I/O 要求について行われます。

ONTAP が適用可能なエクスポートポリシールールを特定して要求を許可するか拒否するかを決定すると、ONTAP はその情報を格納するためのエントリをアクセスキャッシュ内に作成します。

NFS クライアントが I/O 要求を送信すると、 ONTAP は、そのクライアントの IP アドレス、 SVM の ID 、ターゲットボリュームまたは qtree に関連付けられているエクスポートポリシーを記録したうえで、まずアクセスキャッシュをチェックして一致するエントリがないか確認します。一致するエントリがアクセスキャッシュ内に存在する場合、 ONTAP はそこに格納されている情報を使用して、 I/O 要求を許可または拒否します。一致するエントリが存在しない場合、 ONTAP は先ほど述べたすべての適用可能なポリシールールを評価する通常の処理を行います。

アクティブに使用されていないアクセスキャッシュエントリは更新されません。これにより、外部ネームサーバとの無駄な通信が削減されます。

アクセスキャッシュからの情報の取得は、 I/O 要求のたびにエクスポートポリシールールを評価する全体的な処理よりもずっと高速です。そのため、アクセスキャッシュを使用すると、クライアントアクセスチェックのオーバーヘッドが軽減され、パフォーマンスが大幅に向上します。

ONTAP NFSアクセスキャッシュパラメータについて学ぶ

アクセスキャッシュ内のエントリの更新期間は、いくつかのパラメータで制御されます。これらのパラメータの仕組みを理解しておくと、パラメータを変更してアクセスキャッシュを調整し、パフォーマンスと格納される情報の最新度のバランスを取ることができます。

アクセスキャッシュには、ボリュームまたはqtreeにアクセスするクライアントに適用される1つ以上のエクスポートルールで構成されるエントリが格納されます。これらのエントリは、一定期間格納されたあと、更新されます。更新時間はアクセスキャッシュパラメータによって決まり、アクセスキャッシュエントリのタイプによって異なります。

アクセスキャッシュパラメータは、個 々 のSVMに対して指定できます。これにより、SVMのアクセス要件に応じてパラメータを変更できます。アクティブに使用されていないアクセスキャッシュエントリは更新されないため、外部ネームサーバとの不要で無駄な通信が削減されます。

アクセスキャッシュエントリタイプ	説明	更新期間（秒）
正のエントリ	クライアントへのアクセス拒否が発生していないアクセスキャッシュエントリ。	最小：300 最大値：86、400 デフォルト：3、600
負のエントリ	クライアントへのアクセス拒否の原因となったアクセスキャッシュエントリ。	最小：60 最大値：86、400 デフォルト：3、600

例

NFSクライアントがクラスタ上のボリュームへのアクセスを試みます。ONTAPは、クライアントをエクスポートポリシールールと照合し、エクスポートポリシールールの設定に基づいてアクセスを許可していると判断します。ONTAPはエクスポートポリシールールを正のエントリとしてアクセスキャッシュに格納します。デフォルトでは、 ONTAP は、この正のエントリを 1 時間（ 3 、 600 秒）アクセスキャッシュ内に保持したあと、情報を最新の状態にするためにこのエントリを自動的に更新します。

アクセスキャッシュが不必要にいっぱいになるのを防ぐために、クライアントアクセスの決定に一定期間使用されていない既存のアクセスキャッシュエントリを消去するパラメータが追加されています。 `-harvest-timeout`このパラメータの有効範囲は60~2、592、000秒で、デフォルト設定は86、400秒です。

ONTAP NFS qtreeからエクスポートポリシーを削除する

qtree に割り当てられている特定のエクスポートポリシーが不要になった場合は、代わりに格納先ボリュームのエクスポートポリシーを継承するように qtree を変更することで、エクスポートポリシーを削除できます。これを行うには `volume qtree modify`、コマンドでパラメータと空の名前文字列（""）を指定し `-export-policy`ます。

手順

1. qtreeからエクスポートポリシーを削除するには、次のコマンドを入力します。

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. qtreeが適切に変更されたことを確認します。

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

qtree ファイル操作の ONTAP NFS qtree ID を検証する

ONTAP では、オプションで qtree ID の検証を追加で実行できます。この検証により、クライアントのファイル処理要求で有効な qtree ID が使用されるとともに、クライアントによるファイルの移動が同じ qtree 内でのみ行えるようになります。この検証を有効または無効にするには、パラメータを変更し `-validate-qtree-export`ます。このパラメータはデフォルトで有効になっています。

タスクの内容

このパラメータは、 Storage Virtual Machine （ SVM ）上の 1 つ以上の qtree にエクスポートポリシーを直接割り当てている場合にのみ有効です。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

検証する **qtree ID** の状態	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`

検証する **qtree ID** の状態	入力するコマンド
無効にする	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP NFS FlexVol ボリュームのエクスポート ポリシーの制限とネストされたジャンクション

ネストされたジャンクションでは制限の少ないポリシーを設定し、上位のジャンクションではより制限の厳しいポリシーを設定するようにエクスポートポリシーを設定した場合、下位のジャンクションへのアクセスが失敗する可能性があります。

上位レベルのジャンクションには下位レベルのジャンクションよりも制限の少ないエクスポートポリシーを設定する必要があります。

NFSでの**Kerberos**使用によるセキュリティ強化

ONTAP NFS の **Kerberos** サポート

Kerberosは、クライアント/サーバアプリケーションに強力で安全な認証を提供します。認証は、サーバに対するユーザIDとプロセスIDの検証を提供します。ONTAP環境では、KerberosでStorage Virtual Machine（SVM）とNFSクライアント間の認証を実行できます。

ONTAP 9では、次のKerberos機能がサポートされます。

- 整合性チェック機能を備えたKerberos 5認証（krb5i）

  krb5iは、チェックサムを使用して、クライアントとサーバ間で転送される各NFSメッセージの整合性を検証します。これは、セキュリティ上の理由（データが改ざんされていないことの確認など）とデータ整合性上の理由（信頼性の低いネットワークでNFSを使用する場合のデータ破損の防止など）の両方で役立ちます。

- プライバシーチェックを使用したKerberos 5認証（krb5p）

  krb5pはチェックサムを使用して、クライアントとサーバ間のすべてのトラフィックを暗号化します。これはより安全であり、より多くの負荷が発生します。

- 128ビットおよび256ビットのAES暗号化

  Advanced Encryption Standard（AES）は、電子データを保護するための暗号化アルゴリズムです。ONTAPでは、セキュリティを強化するために、128ビットキーによるAES（AES-128）と256ビットキーによるAES（AES-256）がKerberosでサポートされます。

- SVMレベルのKerberos Realm設定

SVM管理者は、Kerberos Realm設定をSVMレベルで作成できるようになりました。つまり、SVM管理者はKerberos Realmの設定に関してクラスタ管理者に頼る必要がなくなり、個 々 のKerberos Realm設定をマルチテナンシー環境で作成できます。

ONTAP NFSでKerberosを設定するための要件

NFSでKerberosを使用するようにシステムで設定する前に、ネットワークおよびストレージの環境内の特定の項目が適切に設定されていることを確認する必要があります。

> 環境を設定する手順は、使用しているクライアントオペレーティングシステム、ドメインコントローラ、Kerberos、DNSなどのバージョンとタイプによって異なります。これらすべての変数を文書化することは、このドキュメントの範囲外です。詳細については、各コンポーネントのそれぞれのドキュメントを参照してください。
>
> Windows Server 2008 R2のActive DirectoryおよびLinuxホストを使用する環境でのNFSv3およびNFSv4でのONTAPおよびKerberos 5のセットアップ方法の詳細な例については、テクニカルレポート4073を参照してください。

最初に次の項目を設定する必要があります。

ネットワーク環境の要件

- Kerberos

  Windows Active DirectoryベースのKerberosやMIT Kerberosなど、Key Distribution Center（KDC；キー配布センター）を使用してKerberosを設定しておく必要があります。

  NFSサーバは、マシンプリンシパルのプライマリコンポーネントとしてを使用する必要があります `nfs`。

- ディレクトリサービス

  Active DirectoryやOpenLDAPなど、SSL/TLS経由のLDAPを使用するように設定されたセキュアなディレクトリサービスを環境で使用する必要があります。

- NTP

  NTPを実行している稼働中のタイムサーバが必要です。これは、時間のずれによるKerberos認証の失敗を防ぐために必要です。

- ドメイン名解決（DNS）

  各UNIXクライアントおよび各SVM LIFについて、KDCのフォワードルックアップゾーンとリバースルックアップゾーンに適切なサービスレコード（SRV）が登録されている必要があります。すべての参加者は、DNSを介して適切に解決できる必要があります。

- ユーザアカウント

  各クライアントには、Kerberos Realmのユーザアカウントが必要です。NFS サーバでは ' マシン・プリンシパルの主要コンポーネントとして NFS' を使用する必要があります

NFSクライアントの要件

- NFS

  NFSv3またはNFSv4を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。

  クライアントがRFC1964およびRFC2203をサポートしている必要があります。

- Kerberos

  Kerberos認証を使用するように各クライアントが適切に設定されている必要があります。詳細は次のとおりです。

  - TGS 通信の暗号化が有効です。

    最も強力なセキュリティを実現するAES-256。

  - TGT 通信に対する最も安全な暗号化タイプが有効です。
  - Kerberos Realm とドメインを正しく設定します。
  - GSSはイネーブルです。

    マシンのクレデンシャルを使用する場合：

  - パラメータを指定し `-n`てを実行しないで `gssd`ください。
  - をrootユーザとして実行しない `kinit`でください。

- 各クライアントは、最新の更新されたオペレーティングシステムバージョンを使用する必要があります。

  これにより、Kerberosを使用したAES暗号化に最高の互換性と信頼性が提供されます。

- DNS

  正しい名前解決のためにDNSを使用するように各クライアントが適切に設定されている必要があります。

- NTP

  各クライアントがNTPサーバと同期している必要があります。

- ホストおよびドメインの情報

  各クライアントの `/etc/hosts`ファイルと `/etc/resolv.conf`ファイルに正しいホスト名とDNS情報が格納されている必要があります。

- keytabファイル

  各クライアントには、KDCのkeytabファイルが必要です。Realmは大文字で指定する必要があります。セキュリティを最大限に高めるには、暗号化タイプをAES-256にする必要があります。

- オプション：パフォーマンスを最大限に高めるには、ローカルエリアネットワークとの通信用とストレージネットワークとの通信用に少なくとも2つのネットワークインターフェイスを用意する必要があります。

ストレージシステムの要件

- NFSライセンス

  ストレージシステムに有効なNFSライセンスがインストールされている必要があります。

- CIFSライセンス

  CIFSライセンスはオプションです。マルチプロトコルのネームマッピングを使用する場合にWindowsクレデンシャルを確認するためにのみ必要です。厳密なUNIXのみの環境では必要ありません。

- SVM

  システムでSVMを少なくとも1つ設定しておく必要があります。

- SVMでのDNS

  各SVMでDNSを設定しておく必要があります。

- NFSサーバ

  SVMでNFSを設定しておく必要があります。

- AES暗号化

  最高レベルのセキュリティを確保するには、KerberosでAES-256暗号化のみを許可するようにNFSサーバを設定する必要があります。

- SMB サーバ

  マルチプロトコル環境の場合は、SVMでSMBを設定しておく必要があります。SMBサーバはマルチプロトコルのネームマッピングに必要です。

- ボリューム

  SVMで使用するルートボリュームと少なくとも1つのデータボリュームを設定しておく必要があります。

- ルートボリューム

  SVMのルートボリュームを次のように設定しておく必要があります。

名前	設定
セキュリティ形式	UNIX
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	777

ルートボリュームとは異なり、データボリュームにはどちらのセキュリティ形式も使用できます。

- UNIXグループ

  SVMで次のUNIXグループを設定しておく必要があります。

グループ名	グループ**ID**
デーモン	1
root	0
pcuser	65534（SVMを作成するとONTAPによって自動的に作成されます）

- UNIXユーザ

  SVMで次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザ**ID**	プライマリグループ**ID**	コメント
NFS	500	0	GSS INITフェーズで必要 NFSクライアントユーザSPNの最初のコンポーネントがユーザとして使用されます。
pcuser	65534	65534	NFSトCIFSノマルチフロトコルノシヨウニヒツヨウ SVMを作成すると、ONTAPで自動的に作成されてpcuserグループに追加されます。
root	0	0	マウントに必要

  NFSクライアントユーザのSPNに対するKerberos-UNIXネームマッピングがある場合は、nfsユーザは必要ありません。

- エクスポートポリシーおよびルール

  ルートボリューム、データボリューム、およびqtreeに対するエクスポートポリシーと必要なエクスポートルールを設定しておく必要があります。SVMのすべてのボリュームへのアクセスにKerberosを使用する場合は、ルートボリュームのエクスポートルールオプション、 `-rwrule`、 `-superuser`、を、 `krb5i`または `krb5p`に `krb5`設定でき `-rorule`ます。

- Kerberos-UNIXネームマッピング

NFSクライアントユーザSPNによって識別されたユーザにroot権限を付与する場合は、rootへのネームマッピングを作成する必要があります。

関連情報

"NetAppテクニカルレポート4073：『Secure Unified Authentication』"

"NetApp Interoperability Matrix Tool"

"システム管理"

"論理ストレージ管理"

NFSv4のONTAPユーザーIDドメインを指定する

ユーザIDドメインを指定するには、オプションを設定し `-v4-id-domain`ます。

タスクの内容

NFSv4 ユーザ ID のマッピングにデフォルトで使用されるドメインは、 NIS ドメインが設定されている場合は NIS ドメインになります。 ONTAPNISドメインが設定されていない場合は、DNSドメインが使用されます。たとえば、複数のユーザIDドメインがある場合などに、ユーザIDドメインの設定が必要になることがあります。ドメイン名は、ドメインコントローラのドメイン設定と一致している必要があります。NFSv3の場合は必要ありません。

ステップ

1. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

ネームサービスを設定する

ONTAP NFSネームサービススイッチ設定の詳細

ONTAPでは、UNIXシステムのファイルに相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf`。このテーブルを環境に合わせて適切に設定できるように、このテーブルの機能とONTAPでの使用方法を理解しておく必要があります。

ONTAPネームサービススイッチテーブルは、ONTAPが特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順序で参照するかを決定します。ネームサービススイッチテーブルは、SVMごとにONTAPで管理されます。

データベースタイプ

このテーブルには、次のデータベースタイプごとにネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名からIPアドレスへの変換	フアイル、DNS

データベースタイプ	ネームサービスソースの用途	有効なソース
グループ	ユーザグループ情報の検索	フアイル、NIS、LDAP
パスワード	ユーザ情報の検索	フアイル、NIS、LDAP
ネットグループ	ネットグループ情報の検索	フアイル、NIS、LDAP
namemap	ユーザ名のマッピング	フアイル、LDAP

ソースタイプ

ソースによって、適切な情報の取得に使用するネームサービスソースが指定されます。

ソースタイプ	情報の検索先	使用するコマンド

ファイル	ローカルソースファイル	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	SVMのNISドメイン設定で指定された外部のNISサーバ	`vserver services name-service nis-domain`
LDAP	SVMのLDAPクライアント設定で指定された外部のLDAPサーバ	`vserver services name-service ldap`
DNS	SVMのDNS設定で指定された外部のDNSサーバ	`vserver services name-service dns`

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合でも、NISまたはLDAP認証が失敗した場合に備えて、ローカルユーザをフォールバックとして含めて設定しておく必要があります `files`。

外部ソースへのアクセスに使用するプロトコル

ONTAPでは、外部ソースのサーバにアクセスするために、次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP

外部のネームサービスソース	アクセスに使用するプロトコル
DNS	UDP
LDAP	TCP

例

次の例は、SVM svm_1のネームサービススイッチ設定を表示します。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

ホストのIPアドレスを検索するために、ONTAPは最初にローカルソースファイルを参照します。クエリから結果が返されない場合は、次にDNSサーバがチェックされます。

ユーザーまたはグループ情報を検索するために、ONTAPはローカルソースファイルのみを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報を検索するために、ONTAPは最初に外部NISサーバを参照します。クエリから結果が返されない場合は、次にローカルネットグループファイルがチェックされます。

SVM svm_1のテーブルには、ネームマッピング用のネームサービスエントリはありません。したがって、ONTAPはデフォルトでローカルソースファイルのみを参照します。

関連情報

"NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

LDAPを使用

ONTAP NFS SVMのLDAPについて学ぶ

LDAP（Lightweight Directory Access Protocol）サーバを使用すると、ユーザ情報を一元的に管理できます。ユーザデータベースをLDAPサーバに格納する場合は、既存のLDAPデータベースのユーザ情報を検索するようにストレージシステムを設定できます。

- ONTAP用にLDAPを設定する前に、サイト環境がLDAPサーバとクライアントの設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAPサーバのドメイン名がLDAPクライアントのエントリと一致している必要があります。

- LDAPサーバでサポートされるLDAPユーザパスワードのハッシュタイプには、ONTAPでサポートされるハッシュタイプが含まれている必要があります。
  - Crypt（すべてのタイプ）およびSHA-1（SHA、SSHA）。
  - ONTAP 9 .8以降では、SHA-2ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384、およびSSHA-512）もサポートされます。
- LDAPサーバでセッションセキュリティ対策が必要な場合は、LDAPクライアントで設定する必要があります。

  次のセッションセキュリティオプションを使用できます。

  - LDAP署名（データ整合性チェックを提供）およびLDAP署名と封印（データ整合性チェックと暗号化を提供）
  - START TLS
  - LDAPS （ LDAP over TLS または SSL ）
- 署名および封印されたLDAPクエリを有効にするには、次のサービスを設定する必要があります。
  - LDAPサーバは、GSSAPI（Kerberos）SASLメカニズムをサポートしている必要があります。
  - LDAPサーバには、DNS A/AAAAレコードと、DNSサーバで設定されたPTRレコードが必要です。
  - Kerberosサーバには、DNSサーバ上にSRVレコードが存在する必要があります。
- START TLSまたはLDAPSを有効にするには、次の点を考慮する必要があります。
  - NetAppでは、LDAPSではなくStart TLSを使用することを推奨します。
  - ONTAP 9.5以降でLDAPSを使用する場合は、TLS用またはSSL用にLDAPサーバが有効になっている必要があります。SSL はONTAP 9.4 - 9.0 ではサポートされていません。
  - 証明書サーバがドメインで設定済みである必要があります。
- LDAPリファーラル追跡を有効にするには（ONTAP 9 .5以降で）、次の条件を満たす必要があります。
  - 両方のドメインに次のいずれかの信頼関係を設定する必要があります。
    - 双方向
    - 一方向（プライマリがリファーラルドメインを信頼する場合）
    - 親子
  - 参照されるすべてのサーバ名を解決するようにDNSを設定する必要があります。
  - trueに設定した場合、認証するドメインパスワードは同じである必要があります `--bind-as-cifs-server`。

次の設定はLDAPリファーラル追跡ではサポートされていません。

- すべてのONTAPバージョン：
- 管理 SVM 上の LDAP クライアント
- ONTAP 9.8 以前では（ 9.9.1 以降でサポートされています）：
- LDAPの署名と封印（ `-session-security`オプション）
- 暗号化されたTLS接続（ `-use-start-tls`オプション）
- LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap`オプション）

- ONTAP 9 .11.1以降では、"ONTAP NFS SVM の nsswitch 認証には LDAP 高速バインドを使用します。"
- SVMでLDAPクライアントを設定するときは、LDAPスキーマを入力する必要があります。

  ほとんどの場合、デフォルトのONTAPスキーマのいずれかが適切です。ただし、環境で使用するLDAPスキーマがこれらと異なる場合は、LDAPクライアントを作成する前に、ONTAP用の新しいLDAPクライアントスキーマを作成する必要があります。環境の要件については、LDAP管理者にお問い合わせください。

- ホスト名解決にLDAPを使用することはサポートされていません。

詳細については、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

ONTAP NFS SVMの**LDAP**署名とシーリングについて学ぶ

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへのクエリに対してLDAPセッションセキュリティを有効にすることができます。Storage Virtual Machine（SVM）のNFSサーバセキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、シークレットキーテクノロジを使用してLDAPペイロードデータの整合性を確認します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。LDAPトラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトは.testです `none`。

SMBトラフィックでのLDAPの署名と封印は、コマンドのオプションを `vserver cifs security modify`使用して`SVM`で有効にします `-session-security-for-ad-ldap`。

ONTAP NFS SVMの**LDAPS**について学ぶ

ONTAPでのLDAP通信の保護方法に関する用語や概念を理解しておく必要があります。ONTAPでは、Active Directory統合LDAPサーバ間またはUNIXベースのLDAPサーバ間の認証されたセッションを設定するために、START TLSまたはLDAPSを使用できます。

用語

ONTAPでのLDAPSを使用したLDAP通信の保護方法について理解しておくべき用語があります。

- * LDAP *

  （Lightweight Directory Access Protocol）情報ディレクトリにアクセスして管理するためのプロトコル。LDAPは、ユーザ、グループ、ネットグループなどのオブジェクトを格納するための情報ディレクトリとして使用されます。LDAPは、これらのオブジェクトを管理し、LDAPクライアントからのLDAP要求を満たすディレクトリサービスも提供します。

- **SSL**

  (Secure Sockets Layer)インターネットを介して情報を安全に送信するために開発されたプロトコルです。SSLはONTAP 9以降でサポートされていますが、TLSの導入に伴い廃止されています。

- * tls *

  （Transport Layer Security）IETF標準の追跡プロトコルで、以前のSSL仕様に基づいています。SSLの後継です。TLSはONTAP 9 .5以降でサポートされています。

- * LDAPS （ LDAP over SSL または TLS ） *

  TLSまたはSSLを使用してLDAPクライアントとLDAPサーバの間の通信を保護するプロトコル。「*ldap over SSL*」と「*ldap over TLS*」は同じ意味で使用されることがあります。LDAPSはONTAP 9 .5以降でサポートされています。

  - ONTAP 9.8～9.5では、LDAPSはポート636でのみ有効にできます。そのためには、 `-use-ldaps-for-ad-ldap`パラメータを `vserver cifs security modify`指示。
  - ONTAP 9.9.1以降では、任意のポートでLDAPSを有効にできますが、デフォルトはポート636です。そのためには、パラメータをに `true`設定し `-ldaps-enabled`、必要なパラメータを指定します `-port`。の詳細については `vserver services name-service ldap client create`、を"ONTAPコマンド リファレンス"参照してください。

  NetAppでは、LDAPSではなくStart TLSを使用することを推奨します。

- * TLS を開始 *

  （ *START_TLS*,*STARTTLS* 、 *_StartTLS* とも呼ばれます）。 TLS プロトコルを使用してセキュアな通信を提供するメカニズムです。

  ONTAPでは、LDAP通信を保護するためにSTARTTLSを使用し、デフォルトのLDAPポート（389）を使用してLDAPサーバと通信します。LDAPサーバは、LDAPポート389経由の接続を許可するように設定する必要があります。そうしないと、SVMからLDAPサーバへのLDAP TLS接続が失敗します。

ONTAPでの**LDAPS**の使用方法

ONTAPはTLSサーバ認証をサポートしています。これにより、SVM LDAPクライアントは、バインド処理時にLDAPサーバのIDを確認できます。TLS対応LDAPクライアントでは、公開鍵暗号化の標準的な技術を使用して、サーバの証明書と公開IDが有効であり、クライアントの信頼できるCAのリストに記載されている認証局（CA）によって発行されたものであることを確認できます。

LDAPでは、TLSを使用した通信の暗号化でSTARTTLSがサポートされます。STARTTLSは標準のLDAPポート（389）経由でプレーンテキスト接続として開始され、その後TLS接続にアップグレードされます。

ONTAPは次の機能をサポートします。

- Active Directory統合LDAPサーバとSVMの間のSMB関連トラフィックに対するLDAPSの使用
- ネームマッピングやその他のUNIX情報のLDAPトラフィックに対するLDAPSの使用

  Active Directory統合LDAPサーバまたはUNIXベースのLDAPサーバのいずれかを使用して、LDAPネームマッピングおよびその他のUNIX情報（ユーザ、グループ、ネットグループなど）の情報を格納できます。

- シコシヨメイルウトCAシヨウメイシヨ

  Active Directory統合LDAPを使用している場合、Windows Server証明書サービスがドメインにインストールされているときに自己署名ルート証明書が生成されます。UNIXベースのLDAPサーバをLDAPネームマッピングに使用している場合は、そのLDAPアプリケーションに適した方法で自己署名ルート証明書が生成されて保存されます。

デフォルトでは、LDAPSは無効になっています。

ONTAP NFS SVMのLDAP RFC2307bisサポートを有効にする

LDAPを使用する必要があり、ネストされたグループメンバーシップを使用するための追加機能が必要な場合は、ONTAPを設定してLDAPのRFC2307bisサポートを有効にすることができます。

開始する前に

デフォルトのLDAPクライアントスキーマのいずれかのコピーを作成しておく必要があります。

タスクの内容

LDAPクライアントスキーマでは、グループオブジェクトはmemberUid属性を使用します。この属性には複数の値を含めることができ、そのグループに属するユーザの名前がリストされます。RFC2307bis対応のLDAPクライアントスキーマでは、グループオブジェクトでuniqueMember属性が使用されます。この属性には、LDAPディレクトリ内の別のオブジェクトの完全な識別名（DN）を含めることができます。これにより、グループに他のグループをメンバーとして追加できるため、ネストされたグループを使用できます。

ユーザは、ネストされたグループを含めて256を超えるグループのメンバーになることはできません。ONTAPでは、この256グループ制限を超えるグループは無視されます。

デフォルトでは、RFC2307bisサポートは無効になっています。

> MS-AD-BISスキーマを使用してLDAPクライアントを作成すると、ONTAPでRFC2307bisサポートが自動的に有効になります。

詳細については、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. コピーしたRFC2307 LDAPクライアントスキーマを変更して、RFC2307bisのサポートを有効にします。

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   ```

```
-schema schema-name -enable-rfc2307bis true
```

3. LDAPサーバでサポートされているオブジェクトクラスに一致するようにスキーマを変更します。

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -group-of-unique-names-object-class object_class
```

4. LDAPサーバでサポートされている属性名に一致するようにスキーマを変更します。

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -unique-member-attribute attribute_name
```

5. admin権限レベルに戻ります。

```
set -privilege admin
```

LDAPディレクトリ検索のための**ONTAP NFS**設定オプション

環境に最も適した方法でLDAPサーバに接続するようにONTAP LDAPクライアントを設定することで、ユーザ、グループ、ネットグループ情報を含むLDAPディレクトリ検索を最適化できます。デフォルトのLDAPベースと範囲の検索値で十分な状況と、カスタム値の方が適切な場合に指定するパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報に対するLDAPクライアント検索オプションは、LDAPクエリの失敗、ひいてはストレージシステムへのクライアントアクセスの失敗を回避するのに役立ちます。また、クライアントのパフォーマンスの問題を回避するために、検索を可能な限り効率的に行うこともできます。

デフォルトのベースおよび範囲検索値

LDAPベースは、LDAPクライアントがLDAPクエリの実行に使用するデフォルトのベースDNです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベースDNを使用して実行されます。このオプションは、LDAPディレクトリが比較的小さく、関連するすべてのエントリが同じDN内にある場合に適しています。

カスタムベースDNを指定しない場合、デフォルトはです `root`。つまり、各クエリでディレクトリ全体が検索されます。これにより、LDAPクエリが成功する可能性は最大になりますが、非効率的になり、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

LDAPベーススコープは、LDAPクライアントがLDAPクエリの実行に使用するデフォルトの検索スコープです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベーススコープを使用して実行されます。LDAPクエリーで、名前付きエントリのみを検索するか、DNの1レベル下のエントリを検索するか、DNの下のサブツリー全体を検索するかを決定します。

カスタムベーススコープを指定しない場合、デフォルトはです `subtree`。つまり、各クエリはDNの下のサブツリー全体を検索します。これにより、LDAPクエリが成功する可能性は最大になりますが、非効率的になり、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

カスタムベースおよびスコープ検索値

必要に応じて、ユーザ、グループ、およびネットグループ検索で、別々のベースおよびスコープ値を指定できます。この方法で検索ベースとクエリの範囲を制限すると、検索がLDAPディレクトリのより小さなサブセクションに制限されるため、パフォーマンスが大幅に向上します。

カスタムベースと範囲の値を指定すると、ユーザ、グループ、およびネットグループ検索の一般的なデフォルトの検索ベースと範囲が上書きされます。カスタムのベース値と範囲値を指定するパラメータは、advanced 権限レベルで使用できます。

LDAP クライアントパラメータ	カスタム指定要素
`-base-dn`	すべてのLDAP検索のベースDN。必要に応じて複数の値を入力できます（たとえば、ONTAP 9.5以降のリリースでLDAPリファーラル追跡が有効になっている場合など）。
`-base-scope`	すべての LDAP 検索の基本スコープ。
`-user-dn`	すべてのLDAPユーザー検索のベースDN。このパラメータはユーザー名マッピング検索にも適用されます。
`-user-scope`	すべてのLDAPユーザー検索の基本スコープ。このパラメータはユーザー名マッピング検索にも適用されます。
`-group-dn`	すべての LDAP グループ検索のベース DN。
`-group-scope`	すべての LDAP グループ検索の基本スコープ。
`-netgroup-dn`	すべての LDAP ネットグループ検索のベース DN。
`-netgroup-scope`	すべての LDAP ネットグループ検索の基本スコープ。

複数のカスタムベース**DN**値

LDAPディレクトリ構造がより複雑な場合は、特定の情報についてLDAPディレクトリの複数の部分を検索するために、複数のベースDNを指定する必要がある場合があります。ユーザ、グループ、およびネットグループDNの各パラメータに複数のDNを指定するには、各パラメータをセミコロン（;）で区切り、DN検索リスト全体を二重引用符（"）で囲みます。DNにセミコロンが含まれている場合は、DN内のセミコロンの直前にエスケープ文字（\）を追加する必要があります。

スコープは、対応するパラメータに指定されたDNSのリスト全体に適用されることに注意してください。たとえば、ユーザスコープに3つの異なるユーザDNとサブツリーのリストを指定すると、LDAPユーザ検索では、指定された3つのDNのそれぞれについてサブツリー全体が検索されます。

また、 ONTAP 9.5 以降では、 LDAP_referral_c追いかけ _ を指定することもできます。これにより、プライマリ LDAP サーバから LDAP リファーラル応答が返されなかった場合に、 ONTAP LDAP クライアントがその他の LDAP サーバへのルックアップ要求を参照することができます。クライアントは、そのリファーラルデータを使用して、リファーラルデータに記載されたターゲットオブジェクトをサーバから読み出します。参照されたLDAPサーバにあるオブジェクトを検索するには、参照されたオブジェクトのベースDNをLDAPクライアント設定の一部としてベースDNに追加します。ただし、参照されたオブジェクトが検索されるのは、LDAPクライアントの作成時または変更時にリファーラル追跡が有効（オプションを使用）になっている場合のみです `-referral-enabled true`。

カスタム**LDAP**検索フィルタ

LDAP設定オプションパラメータを使用して、カスタム検索フィルタを作成できます。パラメータは、 `-group-membership-filter`LDAPサーバからグループメンバーシップを検索するときに使用する検索フィルタを指定します。

有効なフィルタの例を次に示します。

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

詳細については、をご覧ください "ONTAPでLDAPを設定する方法"。

ONTAP NFS SVMの**LDAP**ディレクトリネットグループ別ホスト検索のパフォーマンスを向上

LDAP環境がホスト単位のネットグループ検索を許可するように設定されている場合は、この機能を利用するようにONTAPを設定し、ホスト単位のネットグループ検索を実行できます。これにより、ネットグループ検索にかかる時間が大幅に短縮され、ネットグループ検索時のレイテンシによるNFSクライアントアクセスの問題が軽減されます。

開始する前に

LDAPディレクトリにマップが含まれている必要があり `netgroup.byhost`ます。

DNSサーバには、NFSクライアントのフォワード（A）ルックアップレコードとリバース（PTR）ルックアップレコードの両方が含まれている必要があります。

ネットグループでIPv6アドレスを指定する場合は、常にRFC 5952で指定されているとおりに各アドレスを短縮および圧縮する必要があります。

タスクの内容

NISサーバは、 `netgroup.byuser`、および `netgroup.byhost`という3つの独立したマップにネットグループ情報を格納します `netgroup`。マップと `netgroup.byhost`マップの目的は `netgroup.byuser`、ネットグループの検索速度を上げることです。ONTAPでは、マウントの応答時間を短縮するために、NISサーバ上でホスト単位のネットグループ検索を実行できます。

デフォルトでは、LDAPディレクトリにはNISサーバのようなマップがありません `netgroup.byhost`。ただし、サードパーティのツールを使用すれば、NISマップをLDAPディレクトリにインポートして、ホスト単位の高速ネットグループ検索を有効にすることができます `netgroup.byhost`。ホスト単位のネットグループ検索を許可するようにLDAP環境を設定している場合は、ONTAP LDAPクライアントにマップ名、DN、および検索範囲を設定して、ホスト単位のネットグループ検索を高速化できます `netgroup.byhost`。

ホスト単位のネットグループ検索の結果をより速く受け取ることで、ONTAPクライアントがエクスポートへのアクセスを要求したときに、エクスポートルールをより迅速に処理できるようになります。これにより、ネットグループ検索のレイテンシの問題が原因でアクセスが遅延する可能性が低くなります。

手順

1. LDAPディレクトリにインポートしたNISマップの完全な識別名を取得します `netgroup.byhost`。

   マップDNは、インポートに使用したサードパーティツールによって異なります。最高のパフォーマンスを得るには、正確なマップDNを指定する必要があります。

2. 権限レベルをadvancedに設定します。 `set -privilege advanced`
3. Storage Virtual Machine（SVM）のLDAPクライアント設定でホスト単位のネットグループ検索を有効にします。 `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled{true false}` LDAPディレクトリのホスト単位のネットグループ検索を有効または無効にします。デフォルトはです `false`。

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name`LDAPディレクトリ内のマップの識別名を指定します `netgroup.byhost`。この値は、ホスト単位のネットグループ検索のベースDNを上書きします。このパラメータを指定しない場合、ONTAPは代わりにベースDNを使用します。

   `-netgroup-byhost-scope{base|onelevel subtree}` は、ホスト単位のネットグループ検索の検索範囲を指定します。このパラメータを指定しない場合のデフォルトのはです `subtree`。

   LDAPクライアント設定がまだ存在しない場合は、コマンドを使用して新しいLDAPクライアント設定を作成するときにこれらのパラメータを指定することで、ホスト単位のネットグループ検索を有効にできます `vserver services name-service ldap client create`。

   。 `-ldap-servers` LDAP サーバーのホスト名または IP アドレスを指定するフィールド。
4. admin権限レベルに戻ります。 `set -privilege admin`

例

次のコマンドは、「'ldap_corp'」という既存のLDAPクライアント設定を変更し、「'nisMapName="netgroup.byhost"、dc=corp、dc=example、dc=com`」というマップとデフォルトの検索範囲を `subtree`使用して、ホスト単位のネットグループ検索を有効にし `netgroup.byhost`ます。

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

終了後

`netgroup.byhost`ディレクトリ内のマップと `netgroup`マップは、クライアントアクセスに関する問題を回避するために、常に同期されている必要があります。

関連情報

"IETF RFC 5952 ：『 A Recommendation for IPv6 Address Text Representation 』"

ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する

ONTAP 9.11.1以降では、ldap_fast bind_fルキノ ウ（_コンカレントbind_とも呼ばれます）を利用して、クライアント認証要求を迅速かつ簡単に行うことができます。この機

能を使用するには、LDAPサーバが高速バインド機能をサポートしている必要があります。

タスクの内容

高速バインドを使用しない場合、ONTAPはLDAP簡易バインドを使用してLDAPサーバで管理者ユーザを認証します。この認証方式では、ONTAPはユーザ名またはグループ名をLDAPサーバに送信し、保存されているハッシュパスワードを受信して、サーバハッシュコードとユーザパスワードからローカルに生成されたハッシュパスコードを比較します。これらが同一の場合、ONTAPはログイン権限を付与します。

高速バインド機能を使用すると、ONTAPはユーザクレデンシャル（ユーザ名とパスワード）のみをセキュアな接続経由でLDAPサーバに送信します。LDAPサーバはこれらのクレデンシャルを検証し、ONTAPにログイン権限を付与するように指示します。

高速バインドの利点の1つは、パスワードのハッシュはLDAPサーバによって実行されるため、LDAPサーバがサポートする新しいハッシュアルゴリズムをONTAPでサポートする必要がないことです。

"高速バインドの使用方法について説明します。"

LDAP高速バインドには、既存のLDAPクライアント設定を使用できます。ただし、LDAPクライアントをTLSまたはLDAPS用に設定することを強く推奨します。設定しないと、パスワードはプレーンテキストでネットワーク経由で送信されます。

ONTAP環境でLDAP高速バインドを有効にするには、次の要件を満たす必要があります。

- ONTAP管理者ユーザは、高速バインドをサポートするLDAPサーバで設定する必要があります。
- ネームサービススイッチ（nsswitch）データベースでLDAP用にONTAP SVMが設定されている必要があります。
- 高速バインドを使用したnsswitch認証用に、ONTAP管理者のユーザおよびグループのアカウントを設定する必要があります。

手順

1. LDAPサーバでLDAP高速バインドがサポートされていることをLDAP管理者に確認します。
2. ONTAP管理者ユーザクレデンシャルがLDAPサーバに設定されていることを確認します。
3. 管理SVMまたはデータSVMにLDAP高速バインドが正しく設定されていることを確認します。

    a. LDAP高速バインドサーバがLDAPクライアント設定に表示されていることを確認するには、次のように入力します。

    ```
    vserver services name-service ldap client show
    ```

    "LDAPクライアント設定について説明します。"

    b. がnsswitchデータベースに設定されているソースの1つである `passwd` ことを確認するには `ldap`、次のように入力します。

    ```
    vserver services name-service ns-switch show
    ```

    "nsswitchの設定について説明します。"

4. 管理者ユーザがnsswitchで認証されていること、およびLDAP高速バインド認証がアカウントで有効にな

っていることを確認します。

- 既存のユーザの場合は、次のパラメータ設定を入力し `security login modify`て確認します。

```
-authentication-method nsswitch

-is-ldap-fastbind true
```

の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

- 新しい管理者ユーザについては、を参照してください"LDAPまたはNIS ONTAPアカウントアクセスの有効化"。

ONTAP NFS SVMのLDAP統計を表示する

ストレージ システム上のストレージ仮想マシン (SVM) の LDAP 統計を表示して、パフォーマンスを監視し、問題を診断できます。

開始する前に

- SVM で LDAP クライアントを設定しておく必要があります。
- データを表示できる LDAP オブジェクトを特定しておく必要があります。

ステップ

1. カウンタオブジェクトのパフォーマンスデータを表示します。

```
statistics show
```

例

次の例は、* smpl_1 *という名前のサンプルについて、avg_processor_busyカウンタとcpu_busyカウンタの統計を表示します。

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

関連情報

- "statistics show"
- "statistics start"
- "statistics stop"

ネームマッピングの設定

ONTAP NAS SVMの名前マッピング構成について学習します

ONTAPでは、ネームマッピングを使用して、SMB IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをSMB IDにマッピングします。この情報は、NFSクライアントとSMBクライアントのどちらから接続しているかに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要です。

ネームマッピングを使用する必要がない例外が2つあります。

- 純粋なUNIX環境を構成し、ボリューム上でSMBアクセスまたはNTFSセキュリティ形式を使用する予定がない場合。
- 代わりにデフォルトユーザを使用するように設定します。

  このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。

ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できないことに注意してください。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、salesという

語で開始または終了するすべてのADユーザを、特定のUNIXユーザおよびそのユーザのUIDにマッピングできます。

ONTAP NAS SVMの名前マッピングについて学ぶ

ONTAPでユーザのクレデンシャルをマッピングする必要がある場合は、まずローカルのネームマッピングデータベースとLDAPサーバで既存のマッピングの有無を確認します。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVMのネームサービスの設定で決まります。

- WindowsからUNIXへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPは小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。見つからない場合は、デフォルトのUNIXユーザを使用します（設定済みの場合）。デフォルトのUNIXユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIXからWindowsへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPはSMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合は、デフォルトのSMBユーザを使用します（設定済みの場合）。デフォルトのSMBユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトで指定されたデフォルトのUNIXユーザにマッピングされます。デフォルトのUNIXユーザが指定されていない場合、マシンアカウントのマッピングは失敗します。

- ONTAP 9 .5以降では、マシンアカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9 .4以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントのネームマッピングが定義されていても、それらのマッピングは無視されます。

ONTAP NAS SVM 上の UNIX から Windows へのユーザー名マッピングのマルチドメイン検索

ONTAPは、UNIXユーザをWindowsユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性がUNIXユーザからWindowsユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性がONTAPとどのように連携するかを理解しておく必要があります。SMBサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、SVMのSMBサーバが属しているドメインです。

- _ 双方向の信頼 _

双方向の信頼では、両方のドメインが相互に信頼されます。SMBサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

UNIXユーザからWindowsユーザへのネームマッピング検索は、ホームドメインともう一方のドメイン間で双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼 _

  アウトバウンドの信頼では、ホームドメインはもう一方のドメインを信頼します。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属するユーザを認証および許可できます。

  ホームドメインとアウトバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

- インバウンドの信頼 _

  インバウンドの信頼では、もう一方のドメインがSMBサーバのホームドメインを信頼します。この場合、ホームドメインはインバウンドの信頼できるドメインに属するユーザを認証または許可できません。

  ホームドメインとインバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

ワイルドカード（*）を使用したネームマッピング用のマルチドメイン検索の設定方法

マルチドメインネームマッピングの検索は、Windowsユーザ名のドメインセクションにワイルドカードを使用することで簡単に実行できます。次の表に、ネームマッピングエントリのドメイン部分でワイルドカードを使用してマルチドメイン検索を有効にする方法を示します。

パターン	交換	結果
root	｛Asterisk｝　｛backslash｝　｛backslash｝　管理者	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。

パターン	交換	結果
*	｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝	有効なUNIXユーザが対応するWindowsユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。 パターン ｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝ は、UNIX から Windows へのネームマッピングでのみ有効で、反対方向では無効です。

マルチドメインの名前検索の実行方法

マルチドメイン名の検索に使用する信頼できるドメインのリストを決定するには、次の2つの方法のいずれかを選択します。

- ONTAPによってコンパイルされた自動検出双方向信頼リストを使用する
- コンパイルした信頼できるドメインの優先リストを使用する

ユーザ名のドメインセクションにワイルドカードを使用してUNIXユーザがWindowsユーザにマッピングされている場合、Windowsユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピングされたWindowsユーザはこの検索リストでのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係が確立されたすべてのドメインでWindowsユーザの検索が行われます。
- ホームドメインに双方向の信頼関係が確立されたドメインがない場合は、ホームドメインでユーザの検索が行われます。

UNIXユーザがユーザ名にドメインセクションのないWindowsユーザにマッピングされている場合、ホームドメインでWindowsユーザの検索が行われます。

ONTAP NAS SVMの名前マッピング変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIXプログラムのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed`。

コマンドを使用すると、ネームマッピングを作成できます `vserver name-mapping create`。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

タスクの内容

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> および `-replacement`ステートメントは、 `-pattern`正規表現として記述できます。また、ステートメントを使用して、`null`の置換文字列（スペース文字）を使用してユーザへのマッピングを明示的に拒否する `" "`こともできます `-replacement`。の詳細については `vserver name-mapping create`、を"ONTAPコマンド リファレンス"参照してください。

Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、 vs1 という名前の SVM 上にネームマッピングを作成します。このマッピングは、UNIXからWindowsへのマッピングで、優先順位リストの1番目にあります。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン ENG 内のすべての CIFS ユーザが、 SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

ONTAP NAS SVMのデフォルトユーザーを設定する

ユーザに対する他のマッピング試行がすべて失敗した場合や、UNIXとWindowsの間で個々 のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。または、マッピングされていないユーザの認証を失敗させる場合は、デフォルトユーザを設定しないでください。

タスクの内容

CIFS認証で、各Windowsユーザを個 々 のUNIXユーザにマッピングしない場合は、代わりにデフォルトのUNIXユーザを指定できます。

NFS認証で、各UNIXユーザを個 々 のWindowsユーザにマッピングしない場合は、代わりにデフォルトのWindowsユーザを指定できます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトのUNIXユーザを設定する	`vserver cifs options modify -default-unix-user user_name`
デフォルトのWindowsユーザを設定する	`vserver nfs modify -default-win-user user_name`

NFSネームマッピングを管理するためのONTAPコマンド

ONTAPには、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
名前マッピングを作成する	`vserver name-mapping create`
特定の位置に名前マッピングを挿入する	`vserver name-mapping insert`
表示名のマッピング	`vserver name-mapping show`

2つのネームマッピングの位置を交換する注：ネームマッピングがIP修飾子エントリで設定されている場合はスワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`
ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

の詳細については `vserver name-mapping`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SVMのWindows NFSクライアントのアクセスを有効にする

ONTAPは、Windows NFSv3クライアントからのファイルアクセスをサポートしています。つまり、NFSv3をサポートするWindowsオペレーティングシステムを実行しているクライアントは、クラスタのNFSv3エクスポートのファイルにアクセスできます。この機能を正しく使用するには、Storage Virtual Machine（SVM）を適切に設定し、一定の要件と制限事項に注意する必要があります。

タスクの内容

デフォルトでは、Windows NFSv3クライアントのサポートは無効になっています。

開始する前に

SVMでNFSv3が有効になっている必要があります。

手順

1. Windows NFSv3クライアントのサポートを有効にします。

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Windows NFSv3クライアントをサポートするすべてのSVMで、パラメータと `-v3-connection-drop`パラメータを無効にし `-enable-ejukebox`ます。

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   これで、Windows NFSv3クライアントでストレージシステムにエクスポートをマウントできるようになります。

3. オプションを指定して、各Windows NFSv3クライアントがハードマウントを使用するようにします `-o mtype=hard`。

   これは、マウントの信頼性を確保するために必要です。

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

ONTAP SVMのNFSクライアントでのエクスポートの表示を有効にする

NFSクライアントでは、コマンドを使用して、ONTAP NFSサーバから使用可能なエクスポートのリストを表示できます `showmount -e`。これは、ユーザがマウントするファイルシステムを確認するのに役立ちます。

ONTAPでは、NFS クライアントがデフォルトでエクスポート リストを表示できます。以前のリリースでは、`showmount`コマンドのオプションを `vserver nfs modify`明示的に有効にする必要がありました。エクスポートリストを表示するには、 SVM で NFSv3 が有効になっている必要があります。

例

次のコマンドは、 vs1 という SVM に対して showmount を実行します。

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1     enabled
```

次のコマンドは、 IP アドレスが 10.63.21.9 の NFS サーバ上のエクスポートのリストを表示します。

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

NFSを使用したファイルアクセスの管理

ONTAP SVM の **NFSv3** を有効または無効にする

NFSv3を有効または無効にするには、オプションを変更し `-v3`ます。これにより、NFSv3プロトコルを使用してクライアントがファイルにアクセスできるようになります。デフォルトでは、NFSv3が有効になっています。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv3を有効にする	`vserver nfs modify -vserver vserver_name -v3 enabled`

NFSv3を無効にする	`vserver nfs modify -vserver vserver_name -v3 disabled`

ONTAP SVM の **NFSv4.0** を有効または無効にする

NFSv4.0を有効または無効にするには、オプションを変更し`-v4.0`ます。これにより、NFSv4.0プロトコルを使用してクライアントがファイルにアクセスできるようになります。ONTAP 9.9.1では、NFSv4.0はデフォルトで有効になっています。以前のリリースでは、デフォルトで無効になっていました。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.0を有効にする	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
NFSv4.0を無効にする	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

ONTAP SVM の **NFSv4.1** を有効または無効にする

NFSv4.1を有効または無効にするには、オプションを変更し`-v4.1`ます。これにより、NFSv4.1プロトコルを使用してクライアントがファイルにアクセスできるようになります。ONTAP 9.9.1では、NFSv4.1がデフォルトで有効になります。以前のリリースでは、デフォルトで無効になっていました。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.1を有効にする	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
NFSv4.1を無効にする	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

ONTAP NFSv4 ストアプールの制限を管理する

ONTAP 9 .13以降では、管理者がクライアントあたりのストレージプールのリソース制限に達したときに、NFSv4サーバがNFSv4クライアントに対するリソースを拒否するように設定できます。クライアントがNFSv4ストレージプールリソースを大量に消費する

と、NFSv4ストレージプールリソースが使用できないために他のNFSv4クライアントがブロックされる可能性があります。

この機能を有効にすると、各クライアントによるアクティブなストレージプールリソース消費量を表示することもできます。これにより、システムリソースを使い果たしているクライアントを識別しやすくなり、クライアントごとのリソース制限を課すことができます。

消費されたストレージプールリソースの表示

`vserver nfs storepool show`コマンドは、消費された`storepool`リソースの数を表示します。ストレージプールは、NFSv4クライアントが使用するリソースのプールです。

ステップ

1. 管理者は、コマンドを実行して `vserver nfs storepool show`NFSv4クライアントのストレージプール情報を表示します。

例

次の例は、NFSv4クライアントのストレージプール情報を表示します。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

ストレージプールの制限制御を有効または無効にする

管理者は、次のコマンドを使用して、ストレージプールの制限制御を有効または無効にできます。

ステップ

1. 管理者は、次のいずれかの操作を実行します。

状況	入力するコマンド
ストレージプール制限の制御を有効にする	`vserver nfs storepool config modify -limit-enforce enabled`
ストレージプール制限制御を無効にする	`vserver nfs storepool config modify -limit-enforce disabled`

ブロックされたクライアントのリストを表示する

ストレージプール制限が有効になっている場合、管理者は、クライアントごとのリソースしきい値に達したときにブロックされたクライアントを確認できます。管理者は次のコマンドを使用して、ブロックされたクライアントとしてマークされているクライアントを確認できます。

手順

1. コマンドを使用して `vserver nfs storepool blocked-client show`、NFSv4のブロックされたクライアントリストを表示します。

ブロックされたクライアントリストからクライアントを削除する

クライアントあたりのしきい値に達したクライアントは切断され、ブロッククライアントキャッシュに追加されます。管理者は次のコマンドを使用して、ブロッククライアントキャッシュからクライアントを削除できます。これにより、クライアントはONTAP NFSv4サーバに接続できるようになります。

手順

1. コマンドを使用して `vserver nfs storepool blocked-client flush -client-ip <ip address>`、storepool blockedクライアントキャッシュをフラッシュします。
2. コマンドを使用し `vserver nfs storepool blocked-client show`て、クライアントがブロッククライアントキャッシュから削除されたことを確認します。

例

この例では、IPアドレスが「10.2.1.1」のブロックされたクライアントがすべてのノードからフラッシュされています。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

ONTAP SVM の pNFS を有効または無効にする

pNFSを使用すると、NFSクライアントがストレージデバイスに対する読み取り/書き込み処理を直接かつ並行して実行できるようになり、潜在的なボトルネックとしてNFSサーバがバイパスされるため、パフォーマンスが向上します。pNFS（Parallel NFS）を有効または無効にするには、オプションを変更します `-v4.1-pnfs`。

ONTAPのリリース	pNFSのデフォルト
9.8以降	無効
9.7以前	有効

開始する前に

pNFSを使用するには、NFSv4.1のサポートが必要です。

pNFSを有効にする場合は、まずNFSリファーラルを無効にする必要があります。両方を同時に有効にすることはできません。

SVMでpNFSとKerberosを併用する場合は、SVM上のすべてのLIFでKerberosを有効にする必要があります。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
pNFSを有効にする	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
pNFSを無効にする	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

関連情報

- NFSトランキングの概要

ONTAP SVM の TCP および UDP 経由の NFS アクセスを制御する

TCPおよびUDP経由のStorage Virtual Machine（SVM）へのNFSアクセスを有効または無効にするには、パラメータと `-udp`パラメータをそれぞれ変更し `-tcp`ます。これにより、環境内でNFSクライアントがTCPまたはUDP経由でデータにアクセスできるかどうかを制御できます。

タスクの内容

これらのパラメータはNFSにのみ適用されます。補助プロトコルには影響しません。たとえば、NFS over TCPを無効にしても、TCP経由のマウント処理は引き続き成功します。TCPまたはUDPトラフィックを完全にブロックするには、エクスポートポリシールールを使用します。

コマンドが失敗しないように、NFSに対してTCPを無効にする前にSnapDiff RPCサーバをオフにする必要があります。TCPを無効にするには、コマンドを使用し `vserver snapdiff-rpc-server off -vserver vserver name`ます。

ステップ

1. 次のいずれかを実行します。

設定する NFS アクセスの状態	入力するコマンド
TCP経由で有効化	`vserver nfs modify -vserver vserver_name -tcp enabled`
TCP経由で無効化	`vserver nfs modify -vserver vserver_name -tcp disabled`
UDP経由で有効化	`vserver nfs modify -vserver vserver_name -udp enabled`
UDP 経由で無効にしました	`vserver nfs modify -vserver vserver_name -udp disabled`

ONTAP SVMの予約されていないポートからの**NFS**要求を制御する

オプションを有効にすると、非予約ポートからのNFSマウント要求を拒否できます `-mount-rootonly`。非予約ポートからのすべてのNFS要求を拒否するには、オプションを有効にし `-nfs-rootonly`ます。

タスクの内容

デフォルトでは、オプション `-mount-rootonly`はです `enabled`。

デフォルトでは、オプション `-nfs-rootonly`はです `disabled`。

これらのオプションはNULLプロシージャには適用されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
非予約ポートからのNFSマウント要求を許可する	`vserver nfs modify -vserver vserver_name -mount-rootonly disabled`
非予約ポートからのNFSマウント要求を拒否する	`vserver nfs modify -vserver vserver_name -mount-rootonly enabled`
非予約ポートからのすべてのNFS要求を許可する	`vserver nfs modify -vserver vserver_name -nfs-rootonly disabled`

非予約ポートからのすべてのNFS要求を拒否する	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

不明な**UNIX**ユーザーによる**ONTAP NTFS**ボリュームまたは**qtree**への**NFS**アクセスを処理する

ONTAPは、NTFSセキュリティ形式のボリュームまたはqtreeへの接続を試みるUNIXユーザを識別できない場合、そのユーザをWindowsユーザに明示的にマッピングできません。セキュリティを強化するためにこのようなユーザに対してアクセスを拒否するようにを設定することも、デフォルトのWindowsユーザにマッピングしてすべてのユーザに最小限のアクセスレベルを保証するようにONTAPを設定することもできます。

開始する前に

このオプションを有効にする場合は、デフォルトのWindowsユーザを設定する必要があります。

タスクの内容

UNIXユーザがNTFSセキュリティ形式のボリュームまたはqtreeにアクセスしようとする場合、そのUNIXユーザは、ONTAPがNTFSアクセス権を適切に評価できるように、まずWindowsユーザにマッピングされている必要があります。ただし、ONTAPは、設定されているユーザ情報ネームサービスソースでUNIXユーザの名前を検索できない場合、特定のWindowsユーザにUNIXユーザを明示的にマッピングすることはできません。このような不明なUNIXユーザの処理方法は、次の方法で決定できます。

- 不明なUNIXユーザへのアクセスを拒否します。

  これにより、NTFSボリュームまたはqtreeにアクセスするすべてのUNIXユーザに明示的なマッピングを要求することで、より厳格なセキュリティが適用されます。

- 不明なUNIXユーザをデフォルトのWindowsユーザにマッピングします。

  これにより、セキュリティは低下しますが、すべてのユーザがデフォルトのWindowsユーザを介してNTFSボリュームまたはqtreeへの最小限のレベルのアクセス権を取得できるようになるため、利便性が向上します。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

不明な UNIX ユーザへのデフォルトの Windows ユーザのマッピング	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
無効にする	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. admin権限レベルに戻ります。

```
set -privilege admin
```

予約されていないポートに **ONTAP NFS** エクスポートをマウントするクライアントに関する考慮事項

この `-mount-rootonly`オプションは、非予約ポートを使用してNFSエクスポートをマウントするクライアントをサポートする必要があるストレージシステムでは、ユーザがrootとしてログインしている場合でも無効にする必要があります。Hummingbird クライアントや Solaris NFS / IPv6 クライアントがこれに該当します。

この `-mount-rootonly`オプションを有効にすると、ONTAPでは、非予約ポート（1、023より大きいポート）を使用するNFSクライアントにNFSエクスポートのマウントを許可しません。

ONTAP NFS SVMのドメインを検証することで、ネットグループに対するより厳格なアクセスチェックを実行します。

デフォルトでは、 ONTAP はネットグループに対するクライアントアクセスを評価する際に追加の検証を実行します。この追加チェックにより、クライアントのドメインが Storage Virtual Machine （ SVM ）のドメイン設定に一致していることが確認されます。一致しない場合、 ONTAP はクライアントアクセスを拒否します。

タスクの内容

ONTAP は、クライアントアクセス用のエクスポートポリシールールおよびネットグループが含まれているエクスポートポリシールールを評価する際に、クライアントの IP アドレスがそのネットグループに属しているかどうかを ONTAP が確認する必要があります。そのために、 ONTAP は、 DNS を使用してクライアントの IP アドレスをホスト名に変換し、 Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を取得します。

ネットグループファイルにホストの短い名前のみがリストされていて、そのホストの短い名前が複数のドメインに存在している場合は、異なるドメインのクライアントがこのチェックなしでアクセス権を取得することが可能です。

この問題を回避するために、 ONTAP は、ホストについて DNS から返されたドメインを SVM 用に設定されている DNS ドメイン名のリストと比較します。一致した場合は、アクセスが許可されます。一致しない場合、アクセスは拒否されます。

この検証はデフォルトで有効になっています。これを管理するには、advanced権限レベルで使用できるパラメータを変更し `-netgroup-dns-domain-search`ます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 必要な操作を実行します。

ネットグループのドメイン検証の設定	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
無効にする	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. 権限レベルをadminに設定します。

   ```
   set -privilege admin
   ```

ONTAP SVMのNFSv3サービスに使用されるポートを変更する

ストレージシステム上のNFSサーバは、マウントデーモンやNetwork Lock Managerなどのサービスを使用して、特定のデフォルトネットワークポートを介してNFSクライアントと通信します。ほとんどのNFS環境ではデフォルトポートは正しく機能し、変更は必要ありませんが、NFSv3環境で別のNFSネットワークポートを使用する場合は変更できます。

開始する前に

ストレージシステムでNFSポートを変更するには、すべてのNFSクライアントがシステムに再接続する必要があるため、変更を行う前にこの情報をユーザに伝えておく必要があります。

タスクの内容

NFSマウントデーモン、Network Lock Manager（NLM；ネットワークロックマネージャ）、Network Status Monitor（ネットワークステータスモニタ）、およびNFSクォータデーモンの各サービスで使用されるポートをStorage Virtual Machine（SVM）ごとに設定できます。ポート番号の変更は、TCPとUDPの両方でデータにアクセスするNFSクライアントに影響します。

NFSv4およびNFSv4.1のポートは変更できません。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. NFSへのアクセスを無効にします。

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. 特定のNFSサービスのNFSポートを設定します。

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFS ポートのパラメータ	説明	デフォルトポート
`-mountd-port`	NFSマウントデーモン	635
`-nlm-port`	ネットワークロックマネージャ	4045
`-nsm-port`	ネットワークステータスモニタ	4046
`-rquotad-port`	NFSクォータデーモン	4049

デフォルトのポート以外に、使用できるポート番号の範囲は1024~65535です。各NFSサービスは一意のポートを使用する必要があります。

4. NFSへのアクセスを有効にします。

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. コマンドを使用し `network connections listening show`て、ポート番号の変更を確認します。

   の詳細については `network connections listening show`、を"ONTAPコマンド リファレンス"参照してください。

6. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次のコマンドは、vs1というSVMでNFSマウントデーモンのポートを1113に設定します。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

NFSサーバの管理用**ONTAP**コマンド

ONTAPには、NFSサーバを管理するためのコマンドが用意されています。

状況	使用するコマンド
NFSサーバを作成する	`vserver nfs create`
NFSサーバを表示する	`vserver nfs show`
NFSサーバを変更する	`vserver nfs modify`
NFSサーバを削除する	`vserver nfs delete`

NFSv3マウントポイントのディレクトリの一覧を非表示にする `.snapshot` このオプションを有効にしても、ディレクトリへの明示的なアクセス `.snapshot`は許可されます。	`vserver nfs`enabledオプションを指定したコマンド `-v3-hide-snapshot`

の詳細については `vserver nfs`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP NAS SVM のネームサービスの問題のトラブルシューティング

ネームサービスの問題でクライアントでアクセスエラーが発生した場合は、コマンドファミリーを使用してさまざまなネームサービス検索を手動で実行し、検索の詳細や結果を調べてトラブルシューティングに役立てることができます `vserver services name-service getxxbyyy`。

タスクの内容

- 各コマンドでは、次の情報を指定できます。
  - 検索を実行するノードまたは Storage Virtual Machine （ SVM ）の名前。

    これにより、特定のノードまたはSVMでネームサービス検索をテストして、ネームサービス設定の問題の可能性を絞り込むことができます。
  - 検索に使用されるソースを表示するかどうか。

    これにより、正しいソースが使用されているかどうかを確認できます。
- ONTAPは、設定されているネームサービススイッチの順序に基づいて、検索を実行するためのサービスを選択します。
- これらのコマンドはadvanced権限レベルで使用できます。

手順

1. 次のいずれかを実行します。

取得する情報	使用するコマンド
ホスト名のIPアドレス	`vserver services name-service getxxbyyy getaddrinfo vserver services name-service getxxbyyy gethostbyname` （IPv4アドレスのみ）
グループのメンバー（グループID別）	`vserver services name-service getxxbyyy getgrbygid`

グループのメンバー（グループ名別）	`vserver services name-service getxxbyyy getgrbyname`
ユーザが属しているグループのリスト	`vserver services name-service getxxbyyy getgrlist`
IPアドレスのホスト名	`vserver services name-service getxxbyyy getnameinfo vserver services name-service getxxbyyy gethostbyaddr` （IPv4アドレスのみ）
ユーザ情報（ユーザ名別）	`vserver services name-service getxxbyyy getpwbyname`パラメータをに `true`指定すると、RBACユーザの名前解決をテストできます `-use-rbac`。
ユーザ情報（ユーザID別）	`vserver services name-service getxxbyyy getpwbyuid`パラメータをに `true`指定すると、RBACユーザの名前解決をテストできます `-use-rbac`。
クライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrp`
ホスト単位のネットグループ検索を使用したクライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrpbyhost`

次の例は、ホストacast1.eng.example.comのIPアドレスの取得を試みることでSVM vs1のDNSルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

次の例は、501768というUIDを持つユーザのユーザ情報の取得を試みることでSVM vs1のNIS検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

次の例は、ldap1という名前のユーザのユーザ情報の取得を試みることでSVM vs1のLDAP検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

次の例は、クライアントdnshost0がネットグループlnetgroup136のメンバーであるかどうかを調べることでSVM vs1のネットグループ検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 実行したテストの結果を分析し、必要な措置を取ります。

状況	を確認します
ホスト名またはIPアドレスの検索に失敗したか、正しくない結果が返されました	DNS構成
ルックアップで不正なソースが照会されました	ネームサービススイッチの設定

状況	を確認します
ユーザまたはグループの検索に失敗したか、正しくない結果が得られた	• ネームサービススイッチの設定 • ソースの設定（ローカルファイル、NISドメイン、LDAPクライアント） • ネットワーク設定（LIFやルートなど）
ホスト名の検索に失敗するかタイムアウトし、DNSの短縮名（host1など）がDNSサーバで解決されない	Top-Level Domain（TLD；最上位レベルドメイン）クエリのDNS設定。TLDクエリを無効にするには、コマンドのオプションを `vserver services name-service dns modify`使用し `-is-tld-query-enabled false`ます。

関連情報

"NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

ONTAP NAS SVMのネームサービス接続を確認する

DNSおよびLightweight Directory Access Protocol（LDAP）ネームサーバがONTAPに接続されているかどうかを確認できます。これらのコマンドは管理者権限レベルで使用できます。

タスクの内容

ネームサービス設定チェックを使用して、必要に応じてDNSまたはLDAPのネームサービス設定が有効かどうかを確認できます。この検証チェックは、コマンドラインまたはSystem Managerで開始できます。

DNS構成では、すべてのサーバがテストされ、構成が有効であるとみなされるためにはすべてのサーバが動作している必要があります。LDAP設定の場合、いずれかのサーバが稼働していれば設定は有効です。ネームサービスコマンドは、フィールドがtrue（デフォルトはfalse）でないかぎり設定チェックを適用します `skip-config-validation`。

ステップ

1. 該当するコマンドを使用して、ネームサービスの設定を確認します。設定されているサーバのステータスがUIに表示されます。

確認する項目	使用するコマンド
DNSの設定ステータス	`vserver services name-service dns check`
LDAPの設定ステータス	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                |
```

設定済みのサーバ（name-servers/ldap-servers）の少なくとも1つが到達可能でサービスを提供している場合、設定の検証に成功します。一部のサーバに到達できない場合は警告が表示されます。

NASネームサービススイッチエントリを管理するための**ONTAP**コマンド

ネームサービススイッチエントリの管理では、エントリを作成、表示、変更、削除できます。

状況	使用するコマンド
ネームサービススイッチエントリを作成します。	`vserver services name-service ns-switch create`
ネームサービススイッチエントリを表示する	`vserver services name-service ns-switch show`
ネームサービススイッチエントリを変更する	`vserver services name-service ns-switch modify`
ネームサービススイッチエントリを削除する	`vserver services name-service ns-switch delete`

の詳細については `vserver services name-service ns-switch`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

"NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

NASネームサービスキャッシュを管理するためのONTAPコマンド

ネームサービスキャッシュは、Time-To-Live（TTL）値を変更することで管理できます。TTL値は、ネームサービス情報をキャッシュに保持する期間を決定します。

TTL 値を変更する対象	使用するコマンド
UNIXユーザ	`vserver services name-service cache unix-user settings`
UNIXグループ	`vserver services name-service cache unix-group settings`
UNIXネットグループ	`vserver services name-service cache netgroups settings`
ホスト	`vserver services name-service cache hosts settings`
グループメンバーシップ	`vserver services name-service cache group-membership settings`

関連情報

"ONTAPコマンド リファレンス"

NFSネームマッピングを管理するためのONTAPコマンド

ONTAPには、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
名前マッピングを作成する	`vserver name-mapping create`
特定の位置に名前マッピングを挿入する	`vserver name-mapping insert`
表示名のマッピング	`vserver name-mapping show`
2つのネームマッピングの位置を交換する注：ネームマッピングがIP修飾子エントリで設定されている場合はスワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`
ネームマッピングを削除する	`vserver name-mapping delete`

ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

の詳細については `vserver name-mapping`、を"ONTAPコマンド リファレンス"参照してください。

NASローカル**UNIX**ユーザーを管理するための**ONTAP**コマンド

ONTAPには、ローカルUNIXユーザを管理するためのコマンドが用意されています。

状況	使用するコマンド
ローカルUNIXユーザを作成する	`vserver services name-service unix-user create`
URIからローカルUNIXユーザをロードします。	`vserver services name-service unix-user load-from-uri`
ローカルUNIXユーザを表示する	`vserver services name-service unix-user show`
ローカルUNIXユーザを変更する	`vserver services name-service unix-user modify`
ローカルUNIXユーザを削除する	`vserver services name-service unix-user delete`

の詳細については `vserver services name-service unix-user`、を"ONTAPコマンド リファレンス"参照してください。

NASローカル**UNIX**グループを管理するための**ONTAP**コマンド

ONTAPには、ローカルUNIXグループを管理するためのコマンドが用意されています。

状況	使用するコマンド
ローカルUNIXグループを作成する	`vserver services name-service unix-group create`
ローカルUNIXグループにユーザを追加する	`vserver services name-service unix-group adduser`
URIからローカルUNIXグループをロードする	`vserver services name-service unix-group load-from-uri`
ローカルUNIXグループを表示する	`vserver services name-service unix-group show`
ローカルUNIXグループを変更する	`vserver services name-service unix-group modify`

ローカルUNIXグループからユーザを削除する	`vserver services name-service unix-group deluser`
ローカルUNIXグループを削除する	`vserver services name-service unix-group delete`

の詳細については `vserver services name-service unix-group`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP NFS SVMのローカルUNIXユーザー、グループ、グループメンバーの制限

ONTAP では、クラスタ内の UNIX ユーザおよびグループの最大数の制限と、この制限を管理するためのコマンドが導入されました。これらの制限は、管理者がクラスタ内にローカルUNIXユーザおよびグループを過剰に作成しないようにすることで、パフォーマンスの問題を回避するのに役立ちます。

ローカル UNIX ユーザグループとグループメンバーの合計数には制限があります。ローカル UNIX ユーザについては別途制限があります。これらの制限はクラスタ全体に適用されます。これらの新しい制限はそれぞれデフォルト値に設定されており、あらかじめ割り当てられたハードリミットまで引き上げることができます。

データベース	デフォルトの制限	ハードリミット
ローカルUNIXユーザ	３２、７６８	六五、五三六
ローカルUNIXグループおよびグループメンバー	３２、７６８	六五、五三六

ONTAP NFS SVMのローカルUNIXユーザーとグループの制限を管理する

ONTAP には、ローカル UNIX ユーザおよびグループに対する制限を管理するための固有のコマンドが用意されています。クラスタ管理者は、これらのコマンドを使用して、過剰な数のローカル UNIX ユーザおよびグループに関連していると考えられる、クラスタ内のパフォーマンスの問題のトラブルシューティングを行うことができます。

タスクの内容

これらのコマンドは、 advanced 権限レベルのクラスタ管理者が使用できます。

ステップ

1. 次のいずれかを実行します。

状況	使用するコマンド
ローカル UNIX ユーザの制限に関する情報を表示する	`vserver services unix-user max-limit show`
ローカル UNIX グループの制限に関する情報を表示します	`vserver services unix-group max-limit show`

状況	使用するコマンド
ローカル UNIX ユーザの制限を変更する	`vserver services unix-user max-limit modify`
ローカルUNIXグループの制限を変更する	`vserver services unix-group max-limit modify`

の詳細については `vserver services unix`、を"ONTAPコマンド リファレンス"参照してください。

NFSローカルネットグループを管理するための**ONTAP**コマンド

ローカルネットグループの管理では、URIからのロード、ノード間でのステータスの確認、表示、削除を行います。

状況	使用するコマンド
URIからネットグループをロードする	`vserver services name-service netgroup load`
ノード間のネットグループのステータスを確認する	`vserver services name-service netgroup status` advanced以上の権限レベルで使用できます。
ローカルネットグループを表示します。	`vserver services name-service netgroup file show`
ローカルネットグループを削除します。	`vserver services name-service netgroup file delete`

の詳細については `vserver services name-service netgroup file`、を"ONTAPコマンド リファレンス"参照してください。

NFS NISドメイン構成を管理するための**ONTAP**コマンド

ONTAPには、NISドメイン設定を管理するための固有のコマンドが用意されています。

状況	使用するコマンド
NISドメイン設定を作成する	`vserver services name-service nis-domain create`
NISドメイン設定を表示する	`vserver services name-service nis-domain show`
NISドメイン設定のバインドステータスを表示する	`vserver services name-service nis-domain show-bound`

NIS統計を表示する	`vserver services name-service nis-domain show-statistics`advanced以上の権限レベルで使用できます。
NIS統計のクリア	`vserver services name-service nis-domain clear-statistics`advanced以上の権限レベルで使用できます。
NISドメイン設定を変更する	`vserver services name-service nis-domain modify`
NISドメイン設定を削除する	`vserver services name-service nis-domain delete`
ホスト単位のネットグループ検索のキャッシュを有効にする	`vserver services name-service nis-domain netgroup-database config modify`advanced以上の権限レベルで使用できます。

の詳細については `vserver services name-service nis-domain`、を"ONTAPコマンド リファレンス"参照してください。

NFS LDAP クライアント構成を管理するための **ONTAP** コマンド

ONTAPには、LDAPクライアント設定を管理するためのコマンドが用意されています。

SVM管理者は、クラスタ管理者が作成したLDAPクライアント設定を変更または削除することはできません。

状況	使用するコマンド
LDAPクライアント設定を作成する	`vserver services name-service ldap client create`
LDAPクライアント設定を表示する	`vserver services name-service ldap client show`
LDAPクライアント設定を変更する	`vserver services name-service ldap client modify`
LDAPクライアントのバインドパスワードを変更する	`vserver services name-service ldap client modify-bind-password`
LDAPクライアント設定を削除する	`vserver services name-service ldap client delete`

の詳細については `vserver services name-service ldap client`、を"ONTAPコマンド リファレンス"参照してください。

NFS LDAP 構成を管理するための **ONTAP** コマンド

ONTAPには、LDAP設定を管理するためのコマンドが用意されています。

状況	使用するコマンド

LDAP設定を作成する	`vserver services name-service ldap create`
LDAP設定を表示する	`vserver services name-service ldap show`
LDAP設定を変更する	`vserver services name-service ldap modify`
LDAP設定を削除する	`vserver services name-service ldap delete`

の詳細については `vserver services name-service ldap`、を"ONTAPコマンド リファレンス"参照してください。

NFS LDAP クライアント スキーマ テンプレートを管理するための **ONTAP** コマンド

ONTAPには、LDAPクライアントスキーマテンプレートを管理するための固有のコマンドが用意されています。

SVM管理者は、クラスタ管理者が作成したLDAPクライアントスキーマを変更または削除することはできません。

状況	使用するコマンド
既存のLDAPスキーマテンプレートをコピーする	`vserver services name-service ldap client schema copy`advanced以上の権限レベルで使用できます。
LDAPスキーマテンプレートを表示する	`vserver services name-service ldap client schema show`
LDAPスキーマテンプレートを変更する	`vserver services name-service ldap client schema modify`advanced以上の権限レベルで使用できます。
LDAPスキーマテンプレートを削除する	`vserver services name-service ldap client schema delete`advanced以上の権限レベルで使用できます。

の詳細については `vserver services name-service ldap client schema`、を"ONTAPコマンド リファレンス"参照してください。

NFS Kerberos インターフェース構成を管理するための **ONTAP** コマンド

ONTAPには、NFS Kerberosインターフェイスの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LIFでNFS Kerberosを有効にする	`vserver nfs kerberos interface enable`

NFS Kerberosインターフェイスの設定を表示する	`vserver nfs kerberos interface show`
NFS Kerberosインターフェイスの設定を変更する	`vserver nfs kerberos interface modify`
LIFでNFS Kerberosを無効にする	`vserver nfs kerberos interface disable`

の詳細については `vserver nfs kerberos interface`、を"ONTAPコマンド リファレンス"参照してください。

NFS Kerberos レルム構成を管理するための **ONTAP** コマンド

ONTAPには、NFS Kerberos Realmの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
NFS Kerberos Realmの設定を作成します。	`vserver nfs kerberos realm create`
NFS Kerberos Realmの設定を表示する	`vserver nfs kerberos realm show`
NFS Kerberos Realmの設定を変更する	`vserver nfs kerberos realm modify`
NFS Kerberos Realmの設定を削除する	`vserver nfs kerberos realm delete`

の詳細については `vserver nfs kerberos realm`、を"ONTAPコマンド リファレンス"参照してください。

エクスポートポリシーを管理するための**ONTAP**コマンド

ONTAPには、エクスポートポリシーを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートポリシーに関する情報を表示する	`vserver export-policy show`
エクスポートポリシーの名前を変更する	`vserver export-policy rename`
エクスポートポリシーをコピーする	`vserver export-policy copy`

エクスポートポリシーを削除する	`vserver export-policy delete`

の詳細については `vserver export-policy`、を"ONTAPコマンド リファレンス"参照してください。

エクスポートルールを管理するための**ONTAP**コマンド

ONTAPには、エクスポートルールを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートルールを作成する	`vserver export-policy rule create`
エクスポートルールに関する情報を表示する	`vserver export-policy rule show`
エクスポートルールを変更する	`vserver export-policy rule modify`
エクスポートルールを削除する	`vserver export-policy rule delete`

異なるクライアントに一致する同一のエクスポートルールを複数設定している場合は、エクスポートルールの管理時にそれらのルールの同期を維持してください。

の詳細については `vserver export-policy`、を"ONTAPコマンド リファレンス"参照してください。

NFSクレデンシャルキャッシュの設定

ONTAP SVMの**NFS**認証情報キャッシュの有効期限を変更する理由

ONTAP は、アクセス高速化とパフォーマンス向上のために、クレデンシャルキャッシュを使用して、 NFS エクスポートアクセスでのユーザ認証に必要な情報を格納します。情報を環境に合わせてカスタマイズするために、クレデンシャルキャッシュに保存する期間を設定できます。

NFS クレデンシャルキャッシュの Time-To-Live （ TTL ）の変更が問題の解決に役立つ場合があります。どのような状況がこれに該当するか、またそうした変更がどのような影響を及ぼすかを理解しておく必要があります。

理由

次の状況では、デフォルト TTL の変更を検討してください。

問題	修正アクション
環境内のネームサーバで ONTAP からの要求の負荷が高いためにパフォーマンスが低下している。	キャッシュされている受理および拒否のクレデンシャルに対するTTLを大きくして、ONTAPからネームサーバへの要求数を減らします。

問題	修正アクション
ネームサーバ管理者が、以前に拒否されたNFSユーザへのアクセスを許可するように変更を加えました。	キャッシュされている拒否のクレデンシャルに対するTTLを短くして、NFSユーザがアクセスできるようにONTAPが新しいクレデンシャルを外部ネームサーバに要求するまでの待機時間を短縮します。
ネームサーバ管理者が、以前に許可されていたNFSユーザへのアクセスを拒否する変更を行いました。	キャッシュされている受理されたクレデンシャルに対するTTLを短くして、ONTAPが新しいクレデンシャルを外部ネームサーバに要求してNFSユーザがアクセスを拒否されるようになるまでの時間を短縮します。

結果

受理されたクレデンシャルと拒否されたクレデンシャルをキャッシュする期間を個別に変更できます。ただし、その利点と欠点の両方に注意する必要があります。

状況	利点は ...	欠点は ...
受理のクレデンシャルのキャッシュ時間を長くする	ONTAPがクレデンシャルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	以前はアクセスが許可されていたが今後は許可されなくなったNFSユーザに対して、アクセスを拒否するのにかかる時間が長くなります。
受理された認証情報のキャッシュ時間を短くする	以前はアクセスが許可されていたが今後は許可されなくなったNFSユーザに対して、アクセスを拒否するのにかかる時間が短縮されます。	ONTAPがクレデンシャルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。
拒否されたクレデンシャルのキャッシュ時間を長くします	ONTAPがクレデンシャルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	以前はアクセスが許可されていなかったが今後は許可されるようになるNFSユーザにアクセスを許可するのにかかる時間が長くなります。
拒否されたクレデンシャルのキャッシュ時間を短くします	以前はアクセスが許可されていなかったが今後は許可されるようになったNFSユーザにアクセスを許可するのにかかる時間が短縮されます。	ONTAPがクレデンシャルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。

ONTAP SVMのキャッシュされた**NFS**ユーザー認証情報の有効期限を設定する

Storage Virtual Machine（SVM）のNFSサーバを変更することで、ONTAPがNFSユーザのクレデンシャルを内部キャッシュに格納する期間（Time-To-Live（TTL））を設定できます。これにより、ネームサーバの高負荷やNFSユーザアクセスに影響するクレデンシ

ャルの変更に関連する特定の問題を軽減できます。

タスクの内容

これらのパラメータはadvanced権限レベルで使用できます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

TTL を変更するキャッシュ対象	使用するコマンド
受理のクレデンシャル	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTLはミリ秒単位で測定されます。ONTAP 9.10.1以降では、デフォルトは1時間（3,600,000ミリ秒）です。ONTAP 9.9.1以前では、デフォルトは24時間（86、400,000ミリ秒）です。この値の許容範囲は 1 分（ 60 、 000 ミリ秒） ~7 日間（ 604 、 800 、 000 ミリ秒）です。
拒否の認証情報	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTLはミリ秒単位で測定されます。デフォルトは 2 時間（ 7,200,000 ミリ秒）です。この値の許容範囲は 1 分（ 60 、 000 ミリ秒） ~7 日間（ 604 、 800 、 000 ミリ秒）です。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

エクスポートポリシーキャッシュを管理します。

ONTAP NAS SVMのエクスポートポリシーキャッシュをフラッシュする

ONTAP は、アクセスを高速化するために、エクスポートポリシーに関連する情報の格納に複数のエクスポートポリシーキャッシュを使用します。エクスポートポリシーキャッシュを手動でフラッシュする(`vserver export-policy cache flush`）と古い可能性がある情報が削除され、ONTAPが適切な外部リソースから最新の情報を取得するように強制的に実行されます。これは、 NFS エクスポートへのクライアントアクセスに関するさまざまな問題の解決に役立ちます。

タスクの内容

エクスポートポリシーキャッシュの情報は、次の理由で古くなる可能性があります。

- エクスポートポリシールールが最近変更された
- ネームサーバのホスト名レコードに対する最近の変更
- ネームサーバのネットグループエントリに対する最近の変更
- ネットグループのフルロードを妨げていたネットワーク停止からのリカバリ

手順

1. ネームサービスキャッシュを有効にしていない場合は、 advanced 権限モードで次のいずれかを実行します。

フラッシュ対象	入力するコマンド
すべてのエクスポートポリシーキャッシュ（ showmount を除く）	`vserver export-policy cache flush -vserver vserver_name`
エクスポートポリシールールアクセスキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access`オプションのパラメータを使用すると、アクセスキャッシュをフラッシュするノードを指定できます `-node`。
ホスト名キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache host`
ネットグループキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache netgroup`ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. ネームサービスキャッシュが有効になっている場合は、次のいずれかを実行します。

フラッシュ対象	入力するコマンド
エクスポートポリシールールアクセスキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access`オプションのパラメータを使用すると、アクセスキャッシュをフラッシュするノードを指定できます `-node`。
ホスト名キャッシュ	`vserver services name-service cache hosts forward-lookup delete-all`

フラッシュ対象	入力するコマンド
ネットグループキャッシュ	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all`ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

ONTAP NFS SVMのエクスポートポリシーネットグループキューとキャッシュを表示する

ONTAPは、ネットグループのインポート時および解決時にネットグループキューを使用し、結果の情報を格納するためにネットグループキャッシュを使用します。エクスポートポリシーのネットグループ関連の問題をトラブルシューティングするときは、コマンドと `vserver export-policy netgroup cache show`コマンドを使用して、ネットグループキューのステータスとネットグループキャッシュの内容を表示できます `vserver export-policy netgroup queue show`。

ステップ

1. 次のいずれかを実行します。

エクスポートポリシーネットグループに関する表示対象	入力するコマンド
キュー	`vserver export-policy netgroup queue show`
キャッシュ	`vserver export-policy netgroup cache show -vserver vserver_name`

の詳細については `vserver export-policy netgroup`、を"ONTAPコマンド リファレンス"参照してください。

クライアントIPアドレスがONTAP NFSネットグループのメンバーであるかどうかを確認する

ネットグループに関連するNFSクライアントアクセスの問題をトラブルシューティングするときは、コマンドを使用して、クライアントIPが特定のネットグループのメンバーであるかどうかを確認できます `vserver export-policy netgroup check-membership`。

タスクの内容

ネットグループメンバーシップのチェックにより、クライアントがネットグループのメンバーであることまたはメンバーでないことを ONTAP が認識しているかどうかを確認できます。また、ネットグループ情報の更新中に ONTAP ネットグループキャッシュが一時的な状態にあるかどうかもわかります。この情報は、クライアントに対して予期せずアクセスが許可または拒否される理由を理解するのに役立ちます。

ステップ

1. クライアントIPアドレスのネットグループメンバーシップを確認します。 `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   このコマンドによって次のような結果が返されることがあります。

   - クライアントはネットグループのメンバーです。

     これは、リバースルックアップスキャンまたはホスト単位のネットグループ検索によって確認されました。

   - クライアントはネットグループのメンバーです。

     クライアントが ONTAP のネットグループキャッシュに見つかりました。

   - クライアントはネットグループのメンバーではありません。
   - ONTAP が現在ネットグループキャッシュを更新中なので、まだクライアントのメンバーシップを決定できません。

     これが完了するまで、メンバーシップの判断を明示的に下すことはできません。コマンドを使用し `vserver export-policy netgroup queue show`てネットグループのロードを監視し、ロード完了後にチェックを再試行します。

例

次の例は、 IP アドレスが 172.17.16.72 のクライアントが SVM vs1 上のネットグループ mercury のメンバーであるかどうかをチェックします。

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

ONTAP NFS SVMのアクセスキャッシュパフォーマンスを最適化

複数のパラメータを設定して、アクセスキャッシュを最適化したり、パフォーマンスとアクセスキャッシュに格納される情報の鮮度とのバランスをとったりすることができます。

タスクの内容

アクセスキャッシュの更新期間を設定するときは、次の点に注意してください。

- 値を大きくすると、アクセスキャッシュ内のエントリの保持期間が長くなります。

  長所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの減少によるパフォーマンスの向上が挙げられます。短所は、エクスポートポリシールールが変更されてアクセスキャッシュ

エントリが古くなった場合、エントリの更新にかかる時間が長くなることです。その結果、アクセスできるはずのクライアントが拒否され、拒否されるはずのクライアントがアクセス権を取得する可能性があります。

- 値を小さくすると、 ONTAP によるアクセスキャッシュエントリの更新頻度が高くなります。

  長所は、エントリの鮮度が向上し、クライアントに対するアクセスの許可または拒否が正しく行われる可能性が高くなることです。短所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの増加によるパフォーマンスの低下が挙げられます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

変更の対象	入力するコマンド
正のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
負のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
古いエントリのタイムアウト時間	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 新しいパラメータ設定を確認します。

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ファイルロックを管理します。

ONTAP NFS SVMのプロトコル間のファイルロックについて学習します

ファイルロックは、別のユーザが以前に開いていたファイルにユーザがアクセスできないようにするためにクライアントアプリケーションで使用される方法です。ONTAPでファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントがNFSクライアントの場合はロックを推奨します。クライアントがSMBクライアントの場合はロックは必須です。

NFSファイルとSMBファイルのロックの違いのため、SMBアプリケーションで以前に開いたファイルにNFSクライアントからアクセスすると失敗することがあります。

NFSクライアントがSMBアプリケーションでロックされているファイルにアクセスしようとすると、次の状況が発生します。

- mixed形式またはNTFS形式のボリュームでは、、 `rmdir`などのファイル操作を `rm`mv`行うと、NFSアプリケーションが失敗することがあります。
- NFSの読み取り処理と書き込み処理は、SMBの読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- ファイルの書き込み範囲が排他的なSMBバイトロックでロックされている場合、NFSの書き込み処理が失敗します。

UNIXセキュリティ形式のボリュームでは、NFSのリンク解除および名前変更処理でSMBのロック状態が無視され、ファイルへのアクセスが許可されます。UNIXセキュリティ形式のボリューム上の他のすべてのNFS処理では、SMBロック状態が維持されます。

ONTAP NFS SVMの読み取り専用ビットについて学ぶ

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。 NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、 Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、 ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、 NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。 ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファイルとして扱います。
- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、 ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、 ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、 NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときにSMBクライアントがその読み取り専用ビットを無効にすると、ONTAPはそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、 root のみです。

読み取り専用ビットは、ACL および Unix モード ビットと次のように相互作用します。

ファイルに読み取り専用ビットが設定されている場合:

- そのファイルの ACL は変更されません。NFSクライアントには、読み取り専用ビットが設定される前と同じ ACL が表示されます。
- ファイルへの書き込みアクセスを許可する Unix モード ビットはすべて無視されます。
- NFS クライアントと SMB クライアントはどちらもファイルを読み取ることはできますが、変更することはできません。
- ACLとUNIXモードビットは、読み取り専用ビットが優先されるため無視されます。つまり、ACLが書き込みアクセスを許可していても、読み取り専用ビットによって変更は禁止されます。

ファイルに読み取り専用ビットが設定されていない場合:

- ONTAP は、ACL と UNIX モード ビットに基づいてアクセスを決定します。
  - ACL または UNIX モード ビットのいずれかが書き込みアクセスを拒否した場合、NFS および SMB クライアントはファイルを変更できません。
  - ACL も UNIX モード ビットも書き込みアクセスを拒否しない場合は、NFS および SMB クライアントはファイルを変更できます。

ファイル権限の変更は、 SMB クライアントではすぐに反映されますが、 NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

ONTAP NFSと**Windows**の共有パスコンポーネントのロック処理の違いについて学習します。

Windowsとは異なり、ONTAPはファイルが開いている間、開いているファイルへのパスの各コンポーネントをロックしません。この動作はSMB共有パスにも影響します。

ONTAPではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。その結果、共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、Windows Access Control List（ACL；アクセス制御リスト）のセキュリティ設定を適用して、ユーザやアプリケーションが重要なディレクトリの名前を変更できないようにします。

詳細については、をご覧ください "クライアントがアクセスしている間にディレクトリの名前を変更しないようにする方法"。

ONTAP NFS SVMのロックに関する情報を表示します

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

タスクの内容

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定のStorage Virtual Machine （ SVM ）のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

`vserver locks show`このコマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。 SMB を使用してクライアント側キャッシュを制御します。
- 委譲。 NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。の詳細については `vserver locks show`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. コマンドを使用して、ロックに関する情報を表示します `vserver locks show`。

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。共有ロックのアクセスモードは write-deny_none であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します `/data2/data2_2/intro.pptx`。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを write-deny_none として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
```

```
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ファイルロックによってクライアントがファイルにアクセスできない場合は、現在有効なロックに関する情報を表示して、特定のロックを解除できます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

タスクの内容

コマンドは `vserver locks break`、advanced権限レベル以上でのみ使用できます。の詳細については `vserver locks break`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. ロックを解除するために必要な情報を確認するには、コマンドを使用し `vserver locks show`ます。

   の詳細については `vserver locks show`、を"ONTAPコマンド リファレンス"参照してください。

2. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM名、ボリューム名、LIF名、およびファイルパス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロックID	`vserver locks break -lockid UUID`

4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP FPolicy のファーストリードフィルタとファーストライトフィルタが **NFS** でどのように機能するかを学びます

外部FPolicyサーバを使用してFPolicyが有効になっていて、読み取り/書き込み操作が監視対象イベントとして設定されている場合、読み取り/書き込み要求のトラフィックが多いときにNFSクライアントの応答時間が長くなります。NFSクライアントの場合、FPolicyでfirst-readフィルタとfirst-writeフィルタを使用すると、FPolicy通知の数が減り、パフォーマンスが向上します。

NFSでは、クライアントはファイルのハンドルを取得してI/Oを実行します。このハンドルは、サーバおよびクライアントのリブート後も有効なままになることがあります。したがって、クライアントはハンドルを自由にキャッシュし、ハンドルを再度取得することなく、ハンドルに対する要求を送信できます。通常のセッションでは、大量の読み取り / 書き込み要求がファイルサーバに送信されます。これらすべての要求に対して通知が生成されると、次の問題が発生する可能性があります。

- 追加の通知処理が原因で負荷が大きくなり、応答時間が長くなります。

- サーバがすべての通知の影響を受けていないにもかかわらず、多数の通知がFPolicyサーバに送信される。

特定のファイルに対するクライアントからの最初の読み取り/書き込み要求を受信すると、キャッシュエントリが作成され、読み取り/書き込み数が増分されます。この要求は初回読み取り/書き込み処理とマークされ、FPolicyイベントが生成されます。NFSクライアント用のFPolicyフィルタを計画して作成する前に、FPolicyフィルタの基本的な仕組みを理解しておく必要があります。

- first-read：初回読み取りのクライアント読み取り要求をフィルタリングします。

  このフィルタをNFSイベントに使用すると、および `-file-session-io-grouping-duration`の設定によって、`-file-session-io-grouping-count`FPolicyが処理される初回読み取り要求が決定されます。

- first-write：first-writeのクライアント書き込み要求をフィルタリングします。

  このフィルタをNFSイベントに使用すると、 `-file-session-io-grouping-count`および `-file-session-io-grouping-duration`の設定によって、FPolicyが処理された初回書き込み要求が決定されます。

次のオプションがNFSサーバデータベースに追加されます。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

ONTAP SVMのNFSv4.1サーバ実装IDを変更する

NFSv4.1 プロトコルには、サーバのドメイン、名前、および日付を記録したサーバ実装 ID が含まれています。サーバ実装 ID のデフォルト値は変更できます。デフォルト値を変更すると、たとえば、使用率の統計を収集したり、相互運用性の問題をトラブルシューティングしたりするときに役立ちます。詳細については、 RFC 5661 を参照してください。

タスクの内容

3 つのオプションのデフォルト値は次のとおりです。

オプション	オプション名	デフォルト値
NFSv4.1実装ID -ドメイン	`-v4.1-implementation-domain`	NetApp .com
NFSv4.1実装ID -名前	`-v4.1-implementation-name`	クラスタバージョンの名前
NFSv4.1実装ID -日付	`-v4.1-implementation-date`	クラスタバージョンの日付

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

変更する **NFSv4.1** 実装 **ID** のオプション	入力するコマンド
ドメイン	`vserver nfs modify -v4.1 -implementation-domain domain`
名前	`vserver nfs modify -v4.1 -implementation-name name`
日付	`vserver nfs modify -v4.1 -implementation-date date`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 ACLを管理します。

ONTAP SVM で **NFSv4 ACL** を有効にするメリットについて学びます

NFSv4 ACLを有効にすると、多くのメリットがあります。

NFSv4 ACLを有効にする利点は次のとおりです。

- ファイルやディレクトリへのユーザアクセスのより詳細な制御
- NFSセキュリティの強化
- CIFSとの相互運用性の向上
- NFS のユーザあたりの最大グループ数は 16 ではなくなりました

ONTAP SVMの**NFSv4 ACL**について学ぶ

NFSv4 ACL を使用しているクライアントは、システム上のファイルとディレクトリに ACL を設定し、その ACL を表示することができます。ACLが設定されたディレクトリに新しいファイルまたはサブディレクトリを作成すると、新しいファイルまたはサブディレクトリには、該当する継承フラグが設定されたACL内のすべてのAccess Control Entry（ACE；アクセス制御エントリ）が継承されます。

ファイルやディレクトリが NFSv4 要求によって作成される場合、作成されるファイルやディレクトリの ACL は、ファイル作成要求に ACL が含まれているか、または標準の UNIX ファイルアクセス権限のみが含まれているか、および親ディレクトリに ACL が設定されているかどうかによって異なります。

- 要求にACLが含まれている場合は、そのACLが使用されます。

- 要求に標準のUNIXファイルアクセス権限のみが含まれ、親ディレクトリにACLがある場合、親ディレクトリのACLのACEに適切な継承フラグが設定されていれば、それらのACEが新しいファイルまたはディレクトリに継承されます。

  親ACLは、がに設定されている `off`場合でも継承され `-v4.0-acl`ます。

- 要求に標準のUNIXファイルアクセス権限のみが含まれ、親ディレクトリにACLがない場合は、クライアントのファイルモードを使用して標準のUNIXファイルアクセス権限が設定されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに継承できない ACL がある場合は、モードビットのみを使用して新しいオブジェクトが作成されます。

  または `vserver export-policy rule`ファミリーのコマンドで `vserver nfs`パラメータをに設定した `restricted`場合 `-chown-mode`は、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザにファイル所有権の変更が許可されていても、スーパーユーザのみがファイル所有権を変更できます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SVMのNFSv4 ACLの変更を有効または無効にする

ONTAPがACLを含むファイルまたはディレクトリに対するコマンドを受信した場合、`chmod`デフォルトではACLは保持され、モードビットの変更を反映するように変更されます。代わりにACLをドロップする場合は、パラメータをディセーブルにして動作を変更できます `-v4-acl-preserve`。

タスクの内容

unifiedセキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対するchmod、chgroup、またはchownコマンドを送信したときに、NTFSファイル権限を保持するか破棄するかを指定します。

このパラメータのデフォルトはenabledです。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
既存のNFSv4 ACLの保持と変更を有効にする（デフォルト）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
保持を無効にしてモードビットの変更時にNFSv4 ACLを破棄する	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. admin権限レベルに戻ります。

```
set -privilege admin
```

ONTAPがNFSv4 ACLを使用してファイルを削除できるかどうかを判断する方法を学びます

ファイルを削除できるかどうかを判別するために、 ONTAP は、そのファイルの DELETE ビットと、ファイルが含まれるディレクトリの DELETE_CHILD ビットの組み合わせを使用します。詳細については、 NFS 4.1 RFC 5661 を参照してください。

ONTAP SVMのNFSv4 ACLを有効または無効にする

NFSv4 ACLを有効または無効にするには、オプションと `-v4.1-acl`オプションを変更し `-v4.0-acl`ます。これらのオプションは、デフォルトでは無効になっています。

タスクの内容

> `-v4.0-acl`オプションまたは `-v4.1-acl`オプションは、NFSv4 ACLの設定と表示を制御しますが、アクセスチェックでのNFSv4 ACLの適用は制御しません。

ステップ

1. 次のいずれかを実行します。

状況	そしたら…。
NFSv4.0 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
NFSv4.1 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

ONTAP SVMのNFSv4 ACLの最大ACE制限を変更する

パラメータを変更すると、各NFSv4 ACLに許可されるACEの最大数を変更できます `-v4`

-acl-max-aces。デフォルトでは、 ACL あたりの ACE の数は 400 個に制限されています。この制限値を増やすと、400個を超えるACEを含むACLのデータをONTAPを実行するストレージシステムに移行する際に役立ちます。

タスクの内容

この制限値を増やすと、 NFSv4 ACL を含むファイルにアクセスするクライアントのパフォーマンスが低下することがあります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. NFSv4 ACLのACEの最大数を変更します。

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   有効な範囲

   `max_ace_limit`で `192`ある `1024.`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4ファイル委譲を管理します。

ONTAP SVM の **NFSv4** 読み取りファイル委任を有効または無効にする

NFSv4読み取りファイル委譲を有効または無効にするには、オプション-v4.0-read-delegationまたはオプションを変更します。読み取りファイル委譲を有効にすると、ファイルのオープンとクローズに伴うメッセージのオーバーヘッドを大幅に軽減できます。

タスクの内容

デフォルトでは、読み取りファイル委譲は無効です。

読み取りファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリする必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	そしたら…。

NFSv4読み取りファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
NFSv4.1 読み取りファイル委譲を有効にします	次のコマンドを入力します。 + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
NFSv4読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
NFSv4.1読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

結果

ファイル委譲オプションは、変更されるとすぐに有効になります。NFSをリブートしたり再起動したりする必要はありません。

ONTAP SVM の NFSv4 書き込みファイル委任を有効または無効にする

書き込みファイル委譲を有効または無効にするには、オプション`-v4.0-write -delegation`またはオプションを変更します。書き込みファイル委譲を有効にすると、ファイルのオープンとクローズだけでなく、ファイルおよびレコードのロックに関連するメッセージのオーバーヘッドを大幅に軽減できます。

タスクの内容

デフォルトでは、書き込みファイル委譲は無効です。

書き込みファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリするための追加タスクを実行する必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	そしたら...。
NFSv4書き込みファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`

状況	そしたら...。
NFSv4.1書き込みファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
NFSv4 書き込みファイル委譲を無効にします	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
NFSv4.1 書き込みファイル委譲を無効にします	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

結果

ファイル委譲オプションは、変更されるとすぐに有効になります。NFSをリブートしたり再起動したりする必要はありません。

NFSv4ファイルおよびレコードロックの設定

ONTAP SVM の NFSv4 ファイルおよびレコードのロックについて学習します。

NFSv4 クライアントの場合、 ONTAP は NFSv4 のファイルロックメカニズムをサポートしているため、すべてのファイルのロック状態がリースベースモデルで保持されます。

"NetAppテクニカルレポート3580：『NFSv4の拡張機能とベストプラクティスガイド：Data ONTAPでの実装』"

ONTAP SVMのNFSv4ロックリース期間を指定する

NFSv4ロックリース期間（ONTAPがクライアントに解除不能なロックを付与する期間）を指定するには、オプションを変更します `-v4-lease-seconds`。リース期間を短くするとサーバのリカバリにかかる時間が短縮され、リース期間を長くすると、大量のクライアントを処理するサーバに効果的です。

タスクの内容

デフォルトでは、このオプションはに設定されて `30`います。このオプションの最小値はです `10`。このオプションの最大値はロック猶予期間です。ロック猶予期間はオプションで設定できます `locking.lease_seconds`。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. admin権限レベルに戻ります。

```
set -privilege admin
```

ONTAP SVMのNFSv4ロック猶予期間を指定する

NFSv4ロック猶予期間（サーバリカバリ中にクライアントがロック状態をONTAPに再要求する期間）を指定するには、オプションを変更します `-v4-grace-seconds`。

タスクの内容

デフォルトでは、このオプションはに設定されて `45`います。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. admin権限レベルに戻ります。

```
set -privilege admin
```

ONTAP SVMのNFSv4リファーラルについて学ぶ

NFSv4 リファーラルを有効にすると、 ONTAP は NFSv4 クライアントに対して「 SVM 内」のリファーラルを提供します。SVM内リファーラルでは、クラスタノードがNFSv4要求を受け取ったときに、NFSv4クライアントがStorage Virtual Machine（SVM）の別の論理インターフェイス（LIF）を参照します。

NFSv4 クライアントは、それ以降、ターゲット LIF でリファーラルを受け取ったパスにアクセスする必要があります。元のクラスタノードがこのようなリファーラルを返すのは、データボリュームが存在するクラスタノード上の SVM に LIF があるため、クライアントがデータにより高速にアクセスでき、余分なクラスタ通信が回避されると判断された場合です。

ONTAP SVMのNFSv4リファーラルを有効または無効にする

Storage Virtual Machine（SVM）でNFSv4リファーラルを有効にするには、オプションと`-v4.0-referrals`またはを有効にし `-v4-fsid-change`ます。NFSv4リファーラルを有効にすると、この機能をサポートするNFSv4クライアントのデータアクセス速度が向上します。

開始する前に

NFSリファーラルを有効にする場合は、まずParallel NFSを無効にする必要があります。両方を同時に有効に

することはできません。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
NFSv4リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
NFSv4.1リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
NFSv4.1リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP NFS SVMの統計情報を表示する

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のNFS統計を表示することができます。

手順

1. コマンドを使用して `statistics catalog object show`、データを表示できるNFSオブジェクトを特定します。

   ```
   statistics catalog object show -object nfs*
   ```

2. コマンドとオプションの `statistics stop`コマンドを使用し `statistics start`て、1つ以上のオブジェクトからデータサンプルを収集します。
3. サンプルデータを表示するには、コマンドを使用し `statistics show`ます。

例：**NFSv3**のパフォーマンスの監視

次の例は、NFSv3プロトコルのパフォーマンスデータを表示します。

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、成功した読み取り要求と書き込み要求の数と読み取り要求と書き込み要求の総数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

関連情報

- "パフォーマンス監視のセットアップ"
- "statistics catalog object show"
- "statistics show"
- "statistics start"
- "statistics stop"

ONTAP NFS SVMのDNS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージ システム上のStorage Virtual Machine（SVM）のDNS統計を表示することができます。

手順

1. コマンドを使用して `statistics catalog object show`、データを表示できるDNSオブジェクトを特定します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. コマンドと `statistics stop`コマンドを使用して `statistics start`、1つ以上のオブジェクトからデータサンプルを収集します。
3. サンプルデータを表示するには、コマンドを使用し `statistics show`ます。

次の例は、DNSクエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

次のコマンドは、送信したDNSクエリの数と、受信した、失敗した、またはタイムアウトしたDNSクエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバのDNSクエリについて特定のエラーを受信した回数を表示するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

関連情報

- "パフォーマンス監視のセットアップ"
- "statistics catalog object show"
- "statistics show"
- "statistics start"
- "statistics stop"

ONTAP NFS SVMのNIS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のNIS統計を表示することができます。

手順

1. コマンドを使用して `statistics catalog object show`、データを表示できるNISオブジェクトを特定します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. コマンドと `statistics stop`コマンドを使用して `statistics start`、1つ以上のオブジェクトからデータサンプルを収集します。
3. サンプルデータを表示するには、コマンドを使用し `statistics show`ます。

NIS統計の監視

次の例は、NISクエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

次のコマンドは、送信したNISクエリの数と、受信した、失敗した、またはタイムアウトしたNISクエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバのNISクエリについて特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

関連情報

- "パフォーマンス監視のセットアップ"
- "statistics catalog object show"
- "statistics show"
- "statistics start"
- "statistics stop"

ONTAP NFS 経由の **VMware vStorage** のサポートについて

ONTAPは、NFS環境で特定のVMware vStorage APIs for Array Integration（VAAI）機能をサポートします。

サポートされる機能

次の機能がサポートされます。

- コピーオフロード

  ESXiホストは、仮想マシンまたは仮想マシンディスク（VMDK）を、ホストを介さずにソースとデスティネーションのデータストア間で直接コピーできます。これにより、ESXiホストのCPUサイクルとネットワーク帯域幅が節約されます。ソースボリュームがスパースの場合、コピーオフロードでスペース効率が維持されます。

- スペースリザベーション

  スペースをリザーブしてVMDKファイル用のストレージスペースを確保します。

制限事項

VMware vStorage over NFSには、次の制限事項があります。

- 次の場合、コピーオフロード処理が失敗することがあります。
  - ソースボリュームまたはデスティネーションボリュームで wafliron を実行中に、ボリュームが一時的にオフラインになっている
  - ソースボリュームまたはデスティネーションボリュームを移動しているとき
  - ソースまたはデスティネーションの LIF を移動しているとき
  - テイクオーバーまたはギブバック処理を実行しているとき
  - スイッチオーバーまたはスイッチバック処理を実行しているとき
- 次のシナリオでは、ファイルハンドル形式の違いが原因でサーバ側のコピーが失敗することがあります。

  qtreeを現在エクスポートしている、または以前にエクスポートしていたSVMから、これまでにqtreeをエクスポートしたことがないSVMにデータをコピーしようとします。この制限を回避するには、デスティネーションSVMで少なくとも1つのqtreeをエクスポートします。

関連情報

"Data ONTAPでは、どのようなVAAIオフロード処理がサポートされていますか。"

ONTAP NFS 上の **VMware vStorage** を有効または無効にする

Storage Virtual Machine（SVM）でVMware vStorage over NFSのサポートを有効または無効にするには、コマンドを使用し `vserver nfs modify`ます。

タスクの内容

デフォルトでは、VMware vStorage over NFSのサポートは無効になっています。

手順

1. SVMの現在のvStorageサポートステータスを表示します。

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
VMware vStorageのサポートを有効にする	`vserver nfs modify -vserver vserver_name -vstorage enabled`
VMware vStorageのサポートを無効にする	`vserver nfs modify -vserver vserver_name -vstorage disabled`

終了後

この機能を使用する前に、NFS Plug-in for VMware VAAIをインストールする必要があります。詳細については、「 NetApp NFS Plug-in for VMware VAAI のインストール」を参照してください。

関連情報

"NetAppのマニュアル：NetApp NFS Plug-in for VMware VAAI"

ONTAP NFS SVM で **rquota** サポートを有効または無効にする

リモートクォータプロトコル（rquota）を使用すると、NFSクライアントはリモートマシンからユーザのクォータ情報を取得できます。rquotaバージョンのサポートは、ONTAPのバージョンによって異なります。

- rquota v1はONTAP 9以降でサポートされます。
- rquota v2はONTAP 9.12.1以降でサポートされます。

  rquota v1 から rquota v2 にアップグレードすると、ユーザー クォータ制限に予期しない変更が生じる場合があります。この変更は、rquota v1 と rquota v2 の間でのクォータの計算方法の違いによるものです。詳細については、"NetAppナレッジベース: ユーザークォータ制限が予期せず変更されたのはなぜですか?"。

タスクの内容

デフォルトでは、 rquota は無効です。

ステップ

1. rquotaを有効または無効にします。

状況	入力するコマンド
SVM で rquota のサポートを有効にします	`vserver nfs modify -vserver vserver_name -rquota enable`
SVM で rquota のサポートを無効にします	`vserver nfs modify -vserver vserver_name -rquota disable`

クォータの詳細については、を参照してください"論理ストレージ管理"。

ONTAP SVM の **NFSv3** および **NFSv4** のパフォーマンス向上と **TCP** 転送サイズについて学習します。

TCP 最大転送サイズを変更することで、高レイテンシのネットワーク経由でストレージシステムに接続する NFSv3 / NFSv4 クライアントのパフォーマンスを向上させることができます。

レイテンシが 10 ミリ秒を超えるワイドエリアネットワーク（ WAN ）またはメトロエリアネットワーク（ MAN ）などの高レイテンシネットワークを介してクライアントがストレージシステムにアクセスしている場合は、 TCP 最大転送サイズを変更することで、ネットワーク接続のパフォーマンスを向上させることができます。ローカルエリアネットワーク（ LAN ）などの低レイテンシネットワークでストレージシステムにアクセスするクライアントは、これらのパラメータを変更してもパフォーマンスの向上はあまり期待できません。

スループットの向上がレイテンシの影響を上回らない場合は、これらのパラメータを使用しないでください。

ストレージ環境がこれらのパラメータの変更の恩恵を受けるかどうかを判断するには、まずパフォーマンスの低い NFS クライアントで総合的なパフォーマンス評価を行ってください。パフォーマンスの低さが、クライアント上の過剰なラウンドトリップによるレイテンシとデータ量の少ない要求によるものかどうかを確認します。このような状況では、クライアントとサーバは、接続を介して送信される小さな要求と応答を待機するデューティサイクルの大部分を消費するため、使用可能な帯域幅を完全に使用することはできません。

NFSv3 と NFSv4 の要求サイズを大きくすることで、クライアントとサーバは使用可能な帯域幅をより効果的に使用できるようになり、単位時間あたりの移動データ量が多くなります。そのため、接続の全体的な効率が向上します。

ストレージシステムとクライアントの間で設定が異なる場合があることに注意してください。ストレージシステムとクライアントでサポートされる転送処理の最大サイズは 1MB です。ただし、ストレージシステムで最大転送サイズを 1MB に設定しても、クライアントがサポートするサイズが 64KB であると、マウントの転送サイズは 64KB 以下に制限されます。

これらのパラメータを変更する前に注意しなければならないのは、変更すると、大量の応答をアセンブルして送信するのに時間がかかり、ストレージシステムでメモリ消費が増えるということです。ストレージシステムへの高レイテンシ接続が増えるほど、メモリ消費量も増加します。メモリ容量が多いストレージシステムでは、この変更による影響はほとんどありません。メモリ容量が少ないストレージシステムでは、パフォーマンスが著しく低下する可能性があります。

これらのパラメータを効果的に使用するには、クラスタの複数のノードからデータを取得する必要があります。クラスタネットワーク固有のレイテンシによって、応答の全体的なレイテンシが増加する可能性があります。これらのパラメータを使用するときに、全体的なレイテンシが増大する傾向があります。そのため、レイテンシの影響を受けやすいワークロードは悪影響を受ける可能性があります。

ONTAP SVMのNFSv3**および**NFSv4 TCP**最大転送サイズを変更する

NFSv3およびNFSv4.xプロトコルを使用するすべてのTCP接続に対して最大転送サイズを設定するオプションを変更できます `-tcp-max-xfer-size`。

タスクの内容

これらのオプションは、Storage Virtual Machine（SVM）ごとに個別に変更できます。

ONTAP 9以降では、 `v3-tcp-max-read-size`オプションと `v3-tcp-max-write-size`オプションは廃止されています。代わりにオプションを使用する必要があり `-tcp-max-xfer-size`ます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv3またはNFSv4のTCP最大転送サイズを変更する	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

オプション	範囲	デフォルト
`-tcp-max-xfer-size`	8192~1048576バイト	65536バイト

> 最大転送サイズは4KB（4096バイト）の倍数にする必要があります。要求が要件を満たしていない場合は、パフォーマンスが低下します。

3. コマンドを使用し `vserver nfs show -fields tcp-max-xfer-size`て変更を確認します。
4. 静的マウントを使用するクライアントがある場合は、アンマウントおよび再マウントして新しいパラメータサイズを有効にします。

例

次のコマンドは、vs1というSVMでNFSv3とNFSv4.xのTCP最大転送サイズを1、048576バイトに設定します。

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

ONTAP SVMのNFSユーザーに許可されるグループIDの数を設定する

ONTAPでは、Kerberos（RPCSEC_GSS）認証を使用してNFSユーザクレデンシャルを処理する場合、デフォルトで最大32個のグループIDがサポートされます。AUTH_SYS認証を使用する場合、RFC 5531で定義されているように、グループIDのデフォルトの最大数は16です。デフォルト数を超えるグループに属しているユーザがいる場合は、この最大数を 1 、 024 まで増やすことができます。

タスクの内容

デフォルト数を超えるグループIDがクレデンシャルに設定されている場合、残りのグループIDは切り捨てられ、ストレージシステムのファイルにアクセスしようとするとエラーが表示されることがあります。SVMあたりのグループの最大数は、環境内の最大グループ数に相当する数に設定する必要があります。

> 拡張グループを有効にするためのAUTH_SYS認証の前提条件を理解する(`-auth-sys-extended-groups`デフォルトの最大数である16を超えるグループIDを使用する（または、グループIDが16を超える）場合は、"NetAppナレッジベース: auth-sys-extended-groups を有効にするための前提条件は何ですか?"

次の表に、グループIDの最大数を決定するコマンドの2つのパラメータを3つの設定例で示し `vserver nfs modify`ます。

パラメータ	設定	結果として得られるグループ ID の上限数

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	これらはデフォルト設定です。
		RPCSEC_GSS：32
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS：256
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS：512
		
		AUTH_SYS：512

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

許可される補助グループの最大数の設定対象	入力するコマンド
RPCSEC_GSSの場合のみ、AUTH_SYSはデフォルト値の16のままにします。	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
RPCSEC_GSSとAUTH_SYSの両方	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. 値を確認し `-extended-groups-limit`、拡張グループがAUTH_SYSで使用されているかどうかを確認します。 `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次に、AUTH_SYS認証の拡張グループを有効にし、AUTH_SYS認証とRPCSEC_GSS認証の両方で拡張グループの最大数を512に設定する例を示します。これらの変更は、vs1というSVMにアクセスするクライアントに対してのみ行われます。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

関連情報

- "NetAppナレッジベース: ONTAP 9 の NFS 認証における AUTH_SYS 拡張グループの変更"

ONTAP SVMのNTFSセキュリティ形式のデータへのルートユーザーアクセスを制御する

NTFSセキュリティ形式のデータへのNFSクライアントアクセスを許可したり、NTFSクライアントによるNFSセキュリティ形式のデータへのアクセスを許可したりするようにONTAPを設定できます。NFSデータストアでNTFSセキュリティ形式を使用する場合は、rootユーザによるアクセスの処理方法を決定し、それに応じてStorage Virtual Machine（SVM）を設定する必要があります。

タスクの内容

rootユーザがNTFSセキュリティ形式のデータにアクセスする場合は、次の2つのオプションがあります。

- 他のNFSユーザと同様にrootユーザをWindowsユーザにマッピングし、NTFS ACLに従ってアクセスを管理します。
- NTFS ACLを無視し、rootにフルアクセスを提供します。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

root ユーザへの対処方法	入力するコマンド
Windowsユーザへのマッピング	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`

NT ACLチェックのバイパス	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

デフォルトでは、このパラメータは無効になっています。

このパラメータが有効になっていてもrootユーザに対するネームマッピングがない場合、ONTAPはデフォルトのSMB管理者のクレデンシャルを監査に使用します。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

サポートされるNFSのバージョンとクライアント

サポートされている **ONTAP NFS** のバージョンとクライアントについて学習します

ネットワークでNFSを使用する前に、ONTAPがサポートするNFSのバージョンとクライアントを確認しておく必要があります。

次の表は、ONTAPでNFSプロトコルのメジャーバージョンとマイナーバージョンがデフォルトでサポートされる状況を示しています。デフォルトでサポートされるONTAPは、そのNFSプロトコルをサポートする最も古いバージョンであるとは限りません。

バージョン	サポート対象	導入済み
NFSv3	○	すべてのONTAPリリース
NFSv4.0	○	ONTAP 8
NFSv4.1	○	ONTAP 8.1
NFSv4.2	○	ONTAP 9.8
pNFS	○	ONTAP 8.1

ONTAPでサポートされるNFSクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ONTAP の **NFSv4.0** 機能のサポートについて学ぶ

ONTAP は、 SPKM3 および LIPKEY のセキュリティ機能を除く NFSv4.0 の必須機能をすべてサポートしています。

次の NFSv4 機能がサポートされます。

- * コンパウンド *

  クライアントは、 1 つのリモート手順呼び出し（ RPC ）要求で複数のファイル操作を要求できます。

- * ファイル委譲 *

  サーバは、一部のタイプのクライアントにファイル制御を委譲して読み取りおよび書き込みアクセスを許可します。

- * 擬似 fs *

  NFSv4 サーバでストレージシステム上のマウントポイントの決定に使用します。NFSv4 にはマウントプロトコルはありません。

- * ロック *

  リースベース。NFSv4 には独立した Network Lock Manager （ NLM ；ネットワークロックマネージャ）または Network Status Monitor （ NSM ；ネットワークステータスモニタ）プロトコルはありません。

NFSv4.0 プロトコルの詳細については、 RFC 3530 を参照してください。

NFSv4 の **ONTAP** サポートの制限について学ぶ

ONTAPでのNFSv4のサポートにはいくつかの制限があることに注意してください。

- 委譲機能は、すべてのクライアントタイプでサポートされているわけではありません。
- ONTAP 9 .4以前のリリースでは、UTF8以外のボリュームでASCII以外の文字を含む名前はストレージシステムで拒否されます。

  ONTAP 9 .5以降のリリースでは、utf8mb4言語設定で作成され、NFS v4を使用してマウントされたボリュームにはこの制限は適用されなくなりました。

- すべてのファイルハンドルは永続的です。サーバは揮発性ファイルハンドルを提供しません。
- 移行とレプリケーションはサポートされていません。
- NFSv4クライアントは、読み取り専用負荷共有ミラーではサポートされていません。

  ONTAPは、NFSv4クライアントを直接読み取りおよび書き込みアクセス用負荷共有ミラーのソースにルーティングします。

- 名前付き属性はサポートされていません。
- 次の属性を除くすべての推奨属性がサポートされています。
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`

- quota_avail_soft
- quota_used
- system
- time_backup

> 属性はサポートされませ `quota*`んが、ONTAPはRQUOTA側のバンドプロトコルを通じてユーザクォータとグループクォータをサポートします。

ONTAPの**NFSv4.1**サポートについて

NFSv4.1が有効になっている場合、NFSv.8以降でONTAP 9はデフォルトでnconnect機能を使用できます。

以前のNFSクライアント実装では、マウントでTCP接続を1つしか使用しません。ONTAPでは、1つのTCP接続がIOPSの増加に伴うボトルネックになる可能性があります。

ただし、nconnect対応クライアントは、1つのNFSマウントに複数のTCP接続（最大16）を関連付けることができます。nconnectは1つのIPのみを使用し、その1つのIP上で複数のTCP接続を確立してNFSエクスポートをマウントします。このようなNFSクライアントでは、ファイル処理がラウンドロビン方式で複数のTCP接続に分散されるため、使用可能なネットワーク帯域幅からより高いスループットが得られます。nconnect は、NFSv3とNFSv4.1のマウントでのみ推奨されます。

NFS クライアントのマニュアルを参照して、 nConnect がクライアントバージョンでサポートされているかどうかを確認してください。

ONTAP 9.9.1以降では、NFSv4.1がデフォルトで有効になっています。以前のリリースでは、Storage Virtual Machine（SVM）にNFSサーバを作成するときにオプションを指定し、に設定する `enabled`ことで有効にすることができ `-v4.1`ました。

ONTAP は、 NFSv4.1 のディレクトリレベルおよびファイルレベルの委譲をサポートしていません。

ONTAPの**NFSv4.2**サポートについて

ONTAP 9 .8以降では、ONTAPでNFSv4.2プロトコルがサポートされ、NFSv4.2対応クライアントのアクセスが許可されます。

NFSv4.2は、ONTAP 9 .9.1以降ではデフォルトで有効になっています。ONTAP 9 .8では、Storage Virtual Machine（SVM）にNFSサーバを作成するときにオプションを指定してに設定し `enabled`、v4.2を手動で有効にする必要があります。 `-v4.1`NFSv4.1を有効にすると、クライアントはv4.2としてマウントした状態でNFSv4.1の機能を使用できるようになります。

ONTAPの以降のリリースでは、NFSv4.2のオプション機能のサポートが拡張されています。

最初の文字	**NFSv4.2**のオプションの機能
ONTAP 9 12.1	• NFS拡張属性 • スパースファイル • スペースリザベーション
ONTAP 9 .9.1	NFSラベルのMandatory Access Control（MAC；必須アクセス制御）

NFS v4.2セキュリティラベル

ONTAP 9 .9.1以降では、NFSセキュリティラベルを有効にできます。デフォルトでは無効になっています。

NFS v4.2セキュリティラベルでは、ONTAP NFSサーバは必須アクセス制御（MAC）に対応し、クライアントから送信されたsec_label属性を格納および取得します。

詳細については、を参照してください "RFC 7240"。

手順

1. 権限の設定をadvancedに変更します。

```
set -privilege advanced
```

2. セキュリティラベルを有効にします。

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS拡張属性

ONTAP 9.12.1以降では、NFS拡張属性（xattrs）がデフォルトで有効になっています。

拡張属性は、最新のNFSクライアントで定義され、有効になっている標準のNFS属性です "RFC 8276"。ユーザ定義のメタデータをファイルシステムオブジェクトに添付するために使用でき、高度なセキュリティの導入に役立ちます。

NFS拡張属性は、現在のところNDMPダンプ処理ではサポートされていません。ファイルまたはディレクトリで拡張属性が検出されると、ダンプは続行されますが、それらのファイルまたはディレクトリの拡張属性はバックアップされません。

拡張属性を無効にする必要がある場合は、コマンドを使用し `vserver nfs modify -v4.2-xattrs disabled`ます。

ONTAP のパラレル NFS サポートについて学ぶ

ONTAP は、 Parallel NFS （ pNFS ；パラレル NFS ）をサポートします。pNFS プロトコルは、クラスタの複数のノードに分散されたファイルセットのデータにクライアントが直接アクセスできるようにして、パフォーマンスを向上します。これにより、クライ

アントはボリュームへの最適なパスを見つけることができます。

ONTAP NFSハードマウントについて学ぶ

マウントの問題をトラブルシューティングするときは、正しい種類のマウントを使用していることを確認する必要があります。NFS は、ソフトマウントとハードマウントの 2 つのマウントタイプをサポートしています。信頼性を確保するために、ハードマウントのみを使用してください。

特に NFS タイムアウトが頻繁に発生する可能性がある場合は、ソフトマウントは使用しないでください。タイムアウトによって競合状態が発生し、データが破損する可能性があります。

NFSトSMBノファイルオヨヒテイレクトリノメイメイキソク

ONTAP NFSおよび**SMB**のファイルとディレクトリの命名依存関係について学習します

ファイルとディレクトリの命名規則は、 ONTAP クラスタおよびクライアントの言語設定に加え、ネットワーククライアントのオペレーティングシステムとファイル共有プロトコルによって異なります。

オペレーティングシステムとファイル共有プロトコルによって、次の項目が決まります。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAPでは、ONTAPのリリースに応じて、ファイル、ディレクトリ、およびqtreeの名前でマルチバイト文字がサポートされます。

ONTAP NFS SVM のさまざまなオペレーティング システムで有効な文字について学習します。

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、 UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン（ : ）を使用しないでください。コロンは、 MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限はオペレーティングシステムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティングシステムのマニュアルを参照してください。

ONTAP NFSマルチプロトコル環境におけるファイル名とディレクトリ名の大文字と小文字の区別について学習します。

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。マルチプロトコル環境におけるこれらの影響と、SMB共有の作成時にパスを指定する場合や、共有内のデータにアクセスする場合に実行する必要がある対処方法を理解しておく必要があります。

SMBクライアントでという名前のディレクトリを作成すると、 `testdir`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `testdir`。ただし、SMBユーザがあとでディレクトリ名を作成しようとすると、SMBクライアントではその名前がすでに存在しているとみなされるため作成 `TESTDIR`

できません。NFSユーザがあとでという名前のディレクトリを作成すると、 `TESTDIR`このディレクトリ名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ディレクトリ名の大文字と小文字が区別されるため、両方のディレクトリ名が作成したとおりにと `TESTDIR`表示されます（例：） `testdir`。
- SMBクライアントでは、2つのディレクトリを区別するために8.3形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TESTDI~1`表示され `testdir`ます。
  - ONTAPは、2つのディレクトリを区別するためにディレクトリ名を作成します `TESTDI~1`。

    この場合、Storage Virtual Machine（SVM）で共有を作成または変更するときに共有パスを指定するときは、8.3形式の名前を使用する必要があります。

ファイルについても同様に、SMBクライアントでを作成すると、 `test.txt`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `text.txt`。ただし、SMBユーザがあとでを作成しようとすると、 `Test.txt`SMBクライアントではその名前がすでに存在しているとみなされるため作成できません。NFSユーザがという名前のファイルをあとで作成すると、 `Test.txt`このファイル名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ファイル名の大文字と小文字が区別されるため、両方のファイル名が作成したとおりに、およびと `Test.txt`表示されます `test.txt`。
- SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。1つのファイルにはベースファイル名が付いています。追加のファイルには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TEST~1.TXT`表示され `test.txt`ます。
  - ONTAPは、2つのファイルを区別するためにファイル名を作成します `TEST~1.TXT`。

> Vserver cifs character-mappingコマンドを使用して文字マッピングを作成した場合、通常は大文字と小文字が区別されないWindows検索では大文字と小文字が区別される可能性があります。これは、文字マッピングが作成されていて、ファイル名がその文字マッピングを使っている場合にのみ、ファイル名のルックアップで大文字小文字が区別されることを意味します。

ONTAP NFSのファイル名とディレクトリ名の作成について学習します

ONTAP は、 SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2 つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、 ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（ ~ ）と 1~5 の数字が追加されます。

  同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成する `specifications.html`と、ONTAPではという8.3形式のファイル名が作成されます `specif~1.htm`。この名前がすでに存在する場合、 ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという別のファイルを作成すると `specifications_new.html`、の8.3形式は `specifications_new.html`になり `specif~2.htm`ます。

ONTAP NFS におけるマルチバイトのファイル名、ディレクトリ名、**qtree** 名の処理について学習します。

ONTAP 9 .5以降では、4バイトのUTF-8エンコード名がサポートされているため、基本多言語面（BMP）以外のUnicode補助文字を含むファイル名、ディレクトリ名、ツリー名を作成および表示できます。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8エンコード名のサポートを有効にするために、コマンドファミリーと `volume`コマンドファミリーで新しい_utf8mb4_言語コードを使用でき `vserver`ます。

- 次のいずれかの方法で新しいボリュームを作成する必要があります。
- ボリューム・オプションを明示的に設定し `-language`ます。

  ```
  volume create -language utf8mb4 {…}
  ```

- ボリュームオプションを指定して作成または変更されたSVMからボリュームオプションを継承し `-language`ます。

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- ONTAP 9 .6以前を使用している場合、utf8mb4をサポートするために既存のボリュームを変更することはできません。utf8mb4対応の新しいボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

  ONTAP 9 .7P1以降を使用している場合は、utf8mb4の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください "ONTAPでの作成後にボリュームの言語を変更できますか。"。

+ SVMはutf8mb4をサポートするように更新できますが、既存のボリュームの言語コードは元のままです。

+

> 4バイトのUTF-8文字を使用するLUN名は現在サポートされていません。

- 通常、Unicode文字データは、Windowsファイルシステムアプリケーションでは16-bit Unicode Transformation Format（UTF-16）を使用し、NFSファイルシステムでは8-bit Unicode Transformation Format（UTF-8）を使用して表されます。

  ONTAP 9 .5より前のリリースでは、Windowsクライアントで作成されたUTF-16の補助文字を含む名前は他のWindowsクライアントには正しく表示されましたが、NFSクライアントではUTF-8に正しく変換されませんでした。同様に、NFSクライアントで作成されたUTF-8の補助文字を含む名前は、Windowsクライアントで UTF-16に正しく変換されませんでした。

- ONTAP 9 .4以前を実行しているシステムで、有効または無効な補助文字を含むファイル名を作成する

と、ONTAPはファイル名を拒否し、無効なファイル名エラーを返します。

この問題を回避するには、ファイル名にBMP文字のみを使用して補助文字を使用しないようにするか、ONTAP 9 .5以降にアップグレードしてください。

qtree名にはUnicode文字を使用できます。

- qtree名を設定または変更するには、コマンドファミリーまたはSystem Managerを使用し `volume qtree` ます。
- qtree名には、日本語や中国語などのUnicode形式のマルチバイト文字を含めることができます。
- ONTAP 9 .5より前のリリースでは、BMP文字（つまり、3バイトで表現できる文字）のみがサポートされていました。

> ONTAP 9 .5より前のリリースでは、qtreeの親ボリュームのジャンクションパスに、Unicode文字を使用したqtree名とディレクトリ名を含めることができます。 `volume show`親ボリュームの言語設定がUTF-8の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定がUTF-8のいずれかでない場合は、ジャンクションパスの一部が数値のNFS名に置き換えられて表示されます。

- 9.5以降のリリースでは、utf8mb4が有効なボリュームにqtreeが含まれていれば、qtree名で4バイト文字がサポートされます。

ONTAP NFSボリューム上の**SMB**ファイル名変換の文字マッピングを構成する

NFSクライアントは、SMBクライアントおよび特定のWindowsアプリケーションで無効な文字を含むファイル名を作成できます。ボリュームでのファイル名の変換のための文字マッピングを設定すると、本来は無効なNFS名を持つファイルにSMBクライアントからアクセスできるようになります。

タスクの内容

SMBクライアントがNFSクライアントによって作成されたファイルにアクセスすると、ONTAPはファイル名を確認します。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、 ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、重要な情報を長いファイル名にエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステム上のクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMBクライアントで有効でない文字を含むファイル名をNFSクライアントが作成する場合は、無効なNFS文字をSMBと特定のWindowsアプリケーションの両方で使用できるUnicode文字に変換するマップを定義できます。たとえば、この機能は、CATIA MCADおよびMathematicaアプリケーションだけでなく、この要件を持つ他のアプリケーションもサポートしています。

文字マッピングはボリューム単位で設定できます。

ボリュームに文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイント全体には適用されません。

  文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字または不正な文字を表すUnicode文字は、通常はファイル名に使用されない文字であることを確認する必要があります。使用されていないと、不要なマッピングが発生します。

  たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用されていれば 'Windows クライアントが "a-b`" という名前のファイルにアクセスしようとすると ' その要求は NFS 名 "a:b`" にマップされます (望ましい結果ではありません)

- 文字マッピングを適用したあともマッピングに無効なWindows文字が含まれている場合、ONTAPはWindows 8.3ファイル名にフォールバックします。
- FPolicy通知、NAS監査ログ、およびセキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- DPタイプのSnapMirror関係が作成された場合、ソースボリュームの文字マッピングはデスティネーションDPボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされたWindows名はNFS名に変わるため、名前の検索はNFSのセマンティクスに従って行われます。これには、NFS検索では大文字と小文字が区別されることも含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windowsの大文字と小文字を区別しない動作に依存してはなりません。ただし8.3形式の名前は使用可能で、大文字と小文字は区別されません。
- 部分マッピングまたは無効なマッピング：名前をマッピングしてディレクトリ列挙（「dir」）を実行するクライアントに戻ったあと、生成されたUnicode名がWindowsで有効かどうかがチェックされます。その名前に無効な文字が含まれている場合、またはWindowsで無効な文字が含まれている場合（例：「.」または空白で終わる場合）は、無効な名前の代わりに8.3形式の名前が返されます。

ステップ

1. 文字マッピングを設定します。

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   マッピングは、「 : 」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16進数を使用して入力されたUnicode文字です。例： 3C ： E03C

   コロンで区切られた各ペアの最初の値 `mapping_text`は、変換するNFS文字の16進値です。2番目の値は、SMBで使用されるUnicode値です。マッピングペアは一意である必要があります（1対1のマッピングが存在する必要があります）。

   - ソースマッピング

     次の表に、ソースマッピングで許可されるUnicode文字セットを示します。

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C	\	バックスラッシュ
0x3A	：	コロン
0x2A	*	アスタリスク

0x3F	?	疑問符
0x22	"	引用符
0x3C	<	より小さい
0x3E	>	次の値より大きい
0x7C		
縦線	0xB1	±

◦ ターゲットマッピング

ターゲット文字には、 U+E0000…U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、 Storage Virtual Machine （ SVM ） vs1 上の「 data 」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

SMBファイル名変換の文字マッピングを管理するための**ONTAP NFS**コマンド

文字マッピングを管理するには、FlexVolでSMBファイル名の変換に使用する情報を作成、変更、表示、または削除します。

状況	使用するコマンド
新しいファイル文字マッピングを作成する	`vserver cifs character-mapping create`
ファイル文字マッピングに関する情報を表示する	`vserver cifs character-mapping show`
既存のファイル文字マッピングを変更する	`vserver cifs character-mapping modify`

ファイル文字マッピングを削除します。	`vserver cifs character-mapping delete`

の詳細については `vserver cifs character-mapping`、を"ONTAPコマンド リファレンス"参照してください。

NFSトランキングを管理します。

ONTAP NFSトランキングの詳細

NFSv4.1クライアントでは、セッショントランキングを利用してNFSサーバ上の異なるLIFへの複数の接続を開くことができます。これにより、データ転送速度が向上し、マルチパスによる耐障害性が実現しますONTAP 9。

トランキングは、FlexVolボリュームをトランキング対応のクライアント（特にVMwareおよびLinuxクライアント）にエクスポートする場合や、NFS over RDMA、TCP、pNFSにエクスポートする場合に便利です。

lif.14.1では、トランキングは1つのノードのONTAP 9に制限されています。トランキングは複数のノードにまたがるLIFにはできません。

FlexGroupボリュームはトランキングでサポートされています。これによりパフォーマンスは向上しますが、FlexGroupボリュームへのマルチパスアクセスはシングルノードでしか設定できません。

このリリースのマルチパスでは、セッショントランキングのみがサポートされます。

トランキングの使用方法

トランキングによるマルチパスのメリットを活用するには、トランキング対応NFSサーバがあるSVMに関連付けられた一連のLIF（_trunking group_と呼ばれます）が必要です。トランキンググループ内のLIFは、クラスタの同じノードにホームポートがあり、それらのホームポートに配置されている必要があります。トランキンググループ内のすべてのLIFが同じフェイルオーバーグループのメンバーであることを推奨します。

ONTAPでは、1つのクライアントからノードあたり最大16のトランク接続がサポートされます。

クライアントがトランキング対応サーバからエクスポートをマウントする場合、クライアントはトランキンググループ内のLIFのIPアドレスの数を指定します。クライアントが最初のLIFに接続したあとに追加されたLIFは、NFSv4.1セッションに追加され、トランキンググループの要件を満たしている場合にのみトランキングに使用されます。クライアントは、独自のアルゴリズム（ラウンドロビンなど）に基づいて、複数の接続にNFS処理を分散します。

最大のパフォーマンスを得るには、シングルパスエクスポートではなく、マルチパスエクスポート専用のSVMでトランキングを設定します。つまり、トランキングが有効なクライアントのみにエクスポートが提供されているSVM内のNFSサーバでのみトランキングを有効にします。

サポートされるクライアント

ONTAP NFSv4.1サーバは、NFSv4.1セッショントランキングに対応したすべてのクライアントとのトランキングをサポートしています。

次のクライアントは、ONTAP 9.14.1でテスト済みです。

- VMware-ESXi 7.0U3F以降
- Linux - Red Hat Enterprise Linux（RHEL）8.8および9.3

> フェイルオーバー時（コントローラフェイルオーバーなど）にトランキングされたLIFが別のノードに移行された場合、RHEL NFSクライアントではトランキングが再確立されません。LIFを別のノードに移行すると、LIFはトランキンググループから削除されます。トランキンググループ内のすべてのLIFを移行した場合、NFSクライアントは最初のLIFのみを使用してI/Oを継続します。

> NFSサーバでトランキングが有効になっている場合、トランキングをサポートしていないNFSクライアントでエクスポートされた共有にアクセスすると、パフォーマンスが低下することがあります。これは、SVMデータLIFへの複数のマウントに使用されるTCP接続が1つだけであるためです。

NFSトランキングと**nconnect**の違い

NFSv4.1が有効になっている場合、NFSv.8以降でONTAP 9はデフォルトでnconnect機能を使用できます。nconnect対応クライアントでは、1つのNFSマウントで、1つのLIFを介して複数のTCP接続（最大16）を確立できます。

一方、トランキングは_multipathing_functionalityで、複数のLIFを介して複数のTCP接続を提供します。環境に追加のNICを使用できる場合は、トランキングによってnconnectの機能を超えた並列処理とパフォーマンスが向上します。

詳細については、をご覧ください "nconnect"。

トランキング用に新しい**NFS**サーバとエクスポートを設定する

ONTAP SVMにトランキング対応**NFS**サーバを作成する

ONTAP 9.14.1以降では、NFSサーバでトランキングを有効にできます。NFSv4.1は、NFSサーバの作成時にデフォルトで有効になります。

開始する前に

トランキング対応のNFSサーバを作成するにはSVMが必要です。SVMの条件：

- クライアントのデータ要件に対応する十分なストレージを基盤としています。
- NFSに対して有効にします。

既存のSVMを使用できますが、トランキングを有効にするにはすべてのNFSv4.xクライアントを再マウントする必要があるため、システムが停止する可能性があります。再マウントできない場合は、NFSサーバ用に新しいSVMを作成します。

手順

1. 適切なSVMが存在しない場合は作成します。

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. 新しく作成したSVMの設定とステータスを確認します。

   ```
   vserver show -vserver svm_name
   ```

   詳細については、をご覧ください "SVMの作成"。

3. NFSサーバを作成します。

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. NFSが実行されていることを確認します。

   ```
   vserver nfs status -vserver svm_name
   ```

5. NFSが必要に応じて設定されていることを確認します。

   ```
   vserver nfs show -vserver svm_name
   ```

   詳細はこちら"NFSサーバの設定"

終了後

必要に応じて次のサービスを設定します。

- "DNS"
- "LDAP"
- "Kerberos"

ONTAP NFSトランキング用のネットワークの準備

NFSv4.1トランキングを利用するには、トランキンググループ内のLIFが同じノードに配置され、同じノードにホームポートがある必要があります。LIFは、同じノードのフェイルオーバーグループに設定する必要があります。

タスクの内容

LIFとNICを1対1でマッピングするとパフォーマンスが最大限に向上しますが、トランキングを有効にする必要はありません。少なくとも2つのNICをインストールするとパフォーマンスが向上しますが、必須ではありません。

トランキンググループ内のLIFはすべて同じフェイルオーバーグループに属している必要があります。同じノードのフェイルオーバーグループにLIFが設定されている場合、そのノードでコントローラのフェイルオーバーが発生するとLIFがオフラインになることがあります。同じノードのフェイルオーバーグループにLIFが設定されておらず、別のノードにフェイルオーバーされると、トランキングは機能しなくなります。

フェイルオーバーグループの接続（および基盤となるNIC）を追加または削除するときは、常にトランキングフェイルオーバーグループを調整する必要があります。

開始する前に

- フェイルオーバーグループを作成するには、NICに関連付けられているポート名を確認しておく必要があります。

- すべてのポートが同じノード上にある必要があります。

手順

1. 使用するネットワークポートの名前とステータスを確認します。

```
network port show
```

2. フェイルオーバーグループを作成します。

```
network interface failover-groups create -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```

フェイルオーバーグループは必須ではありませんが、使用することを強く推奨します。

- `<svm_name>`は、NFSサーバが含まれているSVMの名前です。
- `<ports_list>`は、フェイルオーバーグループに追加するポートのリストです。

  ポートは、のよう `node1:e0c`な形式で追加され `<node_name>:<port_number>`ます。

  次のコマンドは、SVM vs1にフェイルオーバーグループfg3を作成し、ポートを3つ追加します。

  ```
  network interface failover-groups create -vserver vs1 -failover-group fg3
  -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
  ```

  詳細はこちら"フェイルオーバーグループ："

の詳細については `network interface failover-groups create`、を"ONTAPコマンド リファレンス"参照してください。

3. 必要に応じて、トランキンググループのメンバー用のLIFを作成します。

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

- `-home-node`- network interface revertコマンドをLIFで実行したときにLIFが戻るノード。

  オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

- `-home-port`は、network interface revertコマンドをLIFに対して実行したときにLIFが戻る物理ポートまたは論理ポートです。
- IPアドレスは、オプションではなく、オプションと `-netmask`オプション `-subnet`で指定できます `-address`。
- 別のIPサブネットにクライアントまたはドメインコントローラがある場合は、IPアドレスを割り当てるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内での静的ルートの作成に関する詳細については、を"ONTAPコマンド リファレンス"参照し `network route create`てください。

- `-service-policy`- LIFのサービスポリシー。ポリシーを指定しない場合は、デフォルトポリシーが自動的に割り当てられます。コマンドを使用し `network interface service-policy show`て、使用可能なサービスポリシーを確認します。
- `-auto-revert`-起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はfalseですが、環境内のネットワーク管理ポリシーに応じてtrueに設定できます。

  トランキンググループ内のすべてのLIFに対してこの手順を繰り返します。

  次のコマンドは、ノードの `cluster1_01`ポートに `e0c`SVM用 `vs1`にを作成し `lif-A`ます。

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

詳細はこちら"LIFの作成"

4. LIFが作成されたことを確認します。

   ```
   network interface show
   ```

5. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

関連情報

- "ネットワークping"
- "ネットワークインターフェイス"
- "network port show"

ONTAPボリュームエクスポートポリシーを作成する

データ共有へのクライアントアクセスを許可するには、ボリュームを1つ以上作成し、ボリュームに少なくとも1つのルールが設定されたエクスポートポリシーを設定する必要があります。

クライアントのエクスポート要件：

- Linuxクライアントでは、トランキング接続ごと（つまりLIFごと）に、個別のマウントと個別のマウントポイントが必要です。
- VMwareクライアントでは、複数のLIFを指定したエクスポートされたボリュームに対してマウントポイントが1つだけ必要です。

  VMwareクライアントには、エクスポートポリシーでルートアクセスが必要です。

手順

1. エクスポートポリシーを作成します。

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   ポリシー名の最大文字数は256文字です。

2. エクスポートポリシーが作成されたことを確認します。

   ```
   vserver export-policy show -policyname policy_name
   ```

   例

   次のコマンドは、 vs1 という SVM で、 exp1 という名前のエクスポートポリシーを作成し、作成を確認します。

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   パラメータには、 `-clientmatch`エクスポートをマウントするトランキング対応のLinuxまたはVMwareクライアントを指定する必要があります。

   詳細はこちら"エクスポートルールを作成しています。"

4. ジャンクションポイントを設定してボリュームを作成します。

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

   詳細はこちら"ボリュームを作成します。"

5. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

   ```
   volume show -vserver svm_name -volume volume_name -junction-path
   ```

NFSトランキング用に**ONTAP**ボリュームまたはデータ共有をマウント

トランキングをサポートするLinuxおよびVMwareクライアントは、トランキングが有効になっているONTAP NFSv4.1サーバからボリュームまたはデータ共有をマウントできます。

詳細はこちらをご覧ください "サポートされるクライアント"。

Linuxクライアントの要件

ONTAP 9.16.1以降とRed Hat Enterprise Linuxバージョン8.7以降（RHEL 8の場合）または9.2以降（RHEL 9の場合）をLinuxクライアントとして使用している場合、トランキンググループに必要なマウントポイントは1つだけです。次のオプションを使用して、エクスポートしたボリュームをマウントし`trunkdiscovery`ます。

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

それ以外の場合は、トランキンググループ内の接続ごとに個別のマウントポイントが必要です。次のようなコマンドを使用して、オプションを使用してエクスポートしたボリュームをマウントします `max_connect`。

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

version(`vers`）の値は以降である必要があります `4.1`。

この `max_connect`値は、トランキンググループ内の接続数に対応します。

VMwareクライアントの要件

トランキンググループ内の各接続のIPアドレスを含むMOUNTステートメントが必要です。

次のようなコマンドを使用して、エクスポートしたデータストアをマウントします。

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

`-H`値はトランキンググループ内の接続に対応しています。

既存の**NFS**エクスポートをトランキングに適合させる

シングルパスエクスポートの**ONTAP NFS**トランキングへの適合

既存のシングルパス（非トランキング）のNFSv4.1エクスポートでトランキングを使用するように設定できます。トランキング対応のクライアントは、サーバとクライアントの前提条件を満たしていれば、サーバでトランキングが有効になるとすぐにパフォーマンスの向上を利用できます。

シングルパスエクスポートをトランキング用に適応させると、エクスポートされたデータセットを既存のボリュームおよびSVMに保持できます。これを行うには、NFSサーバでトランキングを有効にし、ネットワーク設定とエクスポート設定を更新し、エクスポートされた共有をクライアントに再マウントする必要があります。

トランキングをイネーブルにすると、サーバが再起動されます。VMwareクライアントでは、エクスポートしたデータストアを再マウントする必要があります。Linuxクライアントでは、オプションを使用してエクスポートしたボリュームを再マウントする必要があります `max_connect`。

ONTAP NFSサーバでトランキングを有効にする

トランキングはNFSサーバで明示的に有効にする必要があります。NFSv4.1は、NFSサーバの作成時にデフォルトで有効になります。

トランキングを有効にしたら、次のサービスが必要に応じて設定されていることを確認します。

- "DNS"
- "LDAP"
- "Kerberos"

手順

1. トランキングを有効にし、NFSv4.1が有効になっていることを確認します。

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. NFSが実行されていることを確認します。
   ```
   vserver nfs status -vserver svm_name
   ```
3. NFSが必要に応じて設定されていることを確認します。

   ```
   vserver nfs show -vserver svm_name
   ```

   詳細については、"NFSサーバの設定"このSVMからWindowsクライアントにデータを提供する場合は、共有を移動してからサーバを削除します。
   ```
   vserver cifs show -vserver svm_name
   ```

   +
   ```
   vserver cifs delete -vserver svm_name
   ```

ONTAP NFSトランキング用のネットワークの更新

NFSv4.1トランキングを利用するには、トランキンググループ内のLIFが同じノードに配置され、同じノードにホームポートがある必要があります。LIFは、同じノードのフェイルオーバーグループに設定する必要があります。

タスクの内容

LIFとNICを1対1でマッピングするとパフォーマンスが最大限に向上しますが、トランキングを有効にする必要はありません。少なくとも2つのNICをインストールするとパフォーマンスが向上しますが、必須ではありません。

トランキンググループ内のLIFはすべて同じフェイルオーバーグループに属している必要があります。同じノードのフェイルオーバーグループにLIFが設定されている場合、そのノードでコントローラのフェイルオーバーが発生するとLIFがオフラインになることがあります。同じノードのフェイルオーバーグループにLIFが設定されておらず、別のノードにフェイルオーバーされると、トランキングは機能しなくなります。

フェイルオーバーグループの接続（および基盤となるNIC）を追加または削除するときは、常にトランキングフェイルオーバーグループを調整する必要があります。

開始する前に

- フェイルオーバーグループを作成するには、NICに関連付けられているポート名を確認しておく必要があります。
- すべてのポートが同じノード上にある必要があります。

手順

1. 使用するネットワークポートの名前とステータスを確認します。

   ```
   network port show
   ```

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

2. トランキングフェイルオーバーグループを作成するか、既存のフェイルオーバーグループを変更します。

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ```
   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   フェイルオーバーグループは必須ではありませんが、使用することを強く推奨します。

   - `<svm_name>`は、NFSサーバが含まれているSVMの名前です。
   - `<ports_list>`は、フェイルオーバーグループに追加するポートのリストです。

     ポートはの形式で追加され `<node_name>:<port_number>`ます（例：） `node1:e0c。

     次のコマンドは、SVM vs1のフェイルオーバーグループを作成し `fg3`てポートを3つ追加します。

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   詳細はこちら"フェイルオーバーグループ："

3. 必要に応じて、トランキンググループのメンバー用に追加のLIFを作成します。

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node`- network interface revertコマンドをLIFで実行したときにLIFが戻るノード。

     オプションを使用すると、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定できます `-auto-revert`。

   - `-home-port`は、network interface revertコマンドをLIFに対して実行したときにLIFが戻る物理ポートまたは論理ポートです。

- オプションと `-netmask`オプションでIPアドレスを指定できます `-address`。
- IPアドレスを手動で（サブネットを使用せずに）割り当てるときに、クライアントまたはドメインコントローラが別のIPサブネットにある場合は、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内の静的ルートの作成について `network route create`は、コマンドページを参照してください。の詳細については `network route create`、を"ONTAPコマンド リファレンス"参照してください。
- `-service-policy`- LIFのサービスポリシー。ポリシーを指定しない場合は、デフォルトポリシーが自動的に割り当てられます。コマンドを使用し `network interface service-policy show`て、使用可能なサービスポリシーを確認します。

  の詳細については `network interface service-policy show`、を"ONTAPコマンド リファレンス"参照してください。
- `-auto-revert`-起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定します。*デフォルト設定はfalse *ですが、環境内のネットワーク管理ポリシーに応じてtrueに設定できます。

  トランキンググループに追加するLIFごとに、この手順を繰り返します。

  次のコマンドは、ノードの `cluster1_01`ポートに `e0c`SVM用 `vs1`にを作成し `lif-A`ます。

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

詳細はこちら"LIFの作成"

4. LIFが作成されたことを確認します。

   ```
   network interface show
   ```

5. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

関連情報

- "ネットワークping"
- "ネットワークインターフェイス"

ONTAPボリュームのエクスポートポリシーを変更します。

クライアントが既存のデータ共有のトランキングを利用できるようにするには、エクスポートポリシーとルール、およびそれらが接続されているボリュームの変更が必要になる場合があります。LinuxクライアントとVMwareデータストアには、エクスポートに関

するさまざまな要件があります。

クライアントのエクスポート要件：

- Linuxクライアントでは、トランキング接続ごと（つまりLIFごと）に、個別のマウントと個別のマウントポイントが必要です。

  ONTAP 9 14.1にアップグレードしていて、すでにボリュームをエクスポートしている場合は、そのボリュームをトランキンググループで引き続き使用できます。

- VMwareクライアントでは、複数のLIFを指定したエクスポートされたボリュームに対してマウントポイントが1つだけ必要です。

  VMwareクライアントには、エクスポートポリシーでルートアクセスが必要です。

手順

1. 既存のエクスポートポリシーが設定されていることを確認します。

   ```
   vserver export-policy show
   ```

2. 既存のエクスポートポリシールールがトランキング構成に適していることを確認します。

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   特に、エクスポートをマウントするトランキング対応のLinuxクライアントまたはVMwareクライアントがパラメータで正しく識別されていることを確認します `-clientmatch`。

   調整が必要な場合は、コマンドを使用してルールを変更する `vserver export-policy rule modify`か、新しいルールを作成します。

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   詳細はこちら"エクスポートルールを作成しています。"

3. エクスポートした既存のボリュームがオンラインであることを確認します。

   ```
   volume show -vserver svm_name
   ```

NFSトランキング用の**ONTAP**またはデータ共有の再マウント

トランキングされていないクライアント接続をトランキングされた接続に変換するには、LinuxクライアントおよびVMwareクライアントの既存のマウントを、LIFに関する情報を使用してアンマウントし、再マウントする必要があります。

詳細はこちらをご覧ください "サポートされるクライアント"。

VMwareクライアントをアンマウントすると、データストア上のVMが停止します。別の方法として、トランキングを有効にした新しいデータストアを作成し、* Storage VMotion *を使用してVMを古いデータストアから新しいデータストアに移動します。詳細については、VMwareのドキュメントを参照してください。

Linuxクライアントの要件

ONTAP 9.16.1以降とRed Hat Enterprise Linuxバージョン8.7以降（RHEL 8の場合）または9.2以降（RHEL 9の場合）をLinuxクライアントとして使用している場合、トランキンググループに必要なマウントポイントは1つだけです。次のオプションを使用して、エクスポートしたボリュームをマウントし`trunkdiscovery`ます。

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

それ以外の場合は、トランキンググループ内の接続ごとに個別のマウントポイントが必要です。オプションを使用して、次のようなコマンドを実行し、エクスポートしたボリュームをマウントし`max_connect`ます。

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

version(`vers`）の値は以降である必要があります `4.1`。

この `max_connect`値は、トランキンググループ内の接続数に対応します。

VMwareクライアントの要件

トランキンググループ内の各接続のIPアドレスを含むMOUNTステートメントが必要です。

次のようなコマンドを使用して、エクスポートしたデータストアをマウントします。

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

`-H`値は、トランキンググループ内の接続に対応している必要があります。

RDMA経由のNFSを管理します。

ONTAPでのRDMA経由のNFSの詳細

RDMA経由のNFSは、RDMA対応のネットワークアダプタを使用するため、ストレージシステムメモリとホストシステムメモリの間でデータを直接コピーできるため、CPUの中断やオーバーヘッドを回避できます。

NFS over RDMA構成は、機械学習や分析など、レイテンシの影響を受けやすいワークロードや広帯域ワークロードを抱えているお客様向けに設計されています。ONTAP NFS over RDMAは、NFSベースのあらゆるワークロードに使用できます。さらに、NVIDIAでは、RDMA経由でNFSを拡張して、GPUダイレクトストレージ（GDS）を有効にしています。GDSは、CPUとメインメモリをすべてバイパスし、RDMAを使用してストレージシステムとGPUメモリの間でデータを直接転送することで、GPU対応のワークロードをさらに高速化します。

ONTAP 9.10.1以降では、NFSv4.0プロトコルでRDMA経由のNFS構成がサポートされます。以降のONTAPリリースでは、サポートされるNFSバージョンが追加されています。

要件

- 使用するNFSのバージョンに対応した正しいバージョンのONTAPを実行していることを確認します。

NFSバージョン	**ONTAP**のサポート
NFSv4.0	ONTAP 9.10.1以降
NFSv4.1	ONTAP 9.14.1以降
NFSv3	ONTAP 9.15.1以降

  - ONTAP 9.12.1以降では、System Managerを使用してNFS over RDMAを設定できます。ONTAP 9.10.1および9.11.1では、CLIを使用してNFS over RDMAを設定する必要があります。
- ハイアベイラビリティ（HA）ペアの両方のノードのバージョンを同じにする必要があります。
- ストレージシステムコントローラがRDMAをサポートしている必要があります。

ONTAPバージョン	**RDMA**をサポートするコントローラ
9.10.1以降	• AFF A400 • AFF A700用 • AFF A800用
ONTAP 9.14.1以降	• AFF Cシリーズ • AFF A900用
ONTAP 9.15.1以降	• AFF A1K用 • AFF A90用 • AFF A70用
ONTAP 9.16.1以降	• AFF A50用 • AFF A30用 • AFF A20用

- データLIFは、RDMAをサポートするように設定する必要があります。
- ターゲットRNICのサポートについては、を参照してください "NetApp Hardware Universe"。

- NFS over RDMAでサポートされるクライアントオペレーティングシステムについては、を参照して "ネットアップのInteroperability Matrix（IMT）"ください。RoCE v2でサポートされているRNICについては、それぞれのRNICベンダーのマニュアルを参照してください。

インターフェイスグループは、RDMA経由のNFSではサポートされません。

次のステップ

- NFS over RDMA用のNICの設定
- RDMA経由のNFS用のLIFの設定
- NFS over RDMAのNFS設定

関連情報

- "RDMA"
- NFSトランキングの概要
- "RFC 7530 ： NFS バージョン 4 プロトコル"
- "RFC 8166 ：リモート手順コールバージョン 1 用のリモートダイレクトメモリアクセストランスポート"
- "RFC 8167 ： RPC-over-RDMA トランスポート上の双方向リモート手順コール"
- "RFC 8267 ： RPC-over-RDMA バージョン 1 への NFS 上位レイヤバインディング"

NFS over RDMA用のNICの設定

RDMA経由のNFSでは、クライアントシステムとストレージプラットフォームの両方でNIC設定を行う必要があります。

ストレージプラットフォームの構成

ターゲットRNICのサポートについては、を参照してください "NetApp Hardware Universe"。

ハイアベイラビリティ（HA）構成を使用している場合は、RDMAフェイルオーバーをサポートするために両方のノードで同じRNICを使用する必要があります。NICはRoCEに対応している必要があります。

- ONTAP 9.10.1以降では、次のコマンドを使用して、RDMAオフロードプロトコルのリストを表示できます。

```
network port show -rdma-protocols roce
```

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

- ONTAP 9.16.1以降では、優先度フロー制御（PFC）を使用することを推奨します。次のコマンドを使用してPFCを設定し `network port modify`ます。

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- ONTAP 9.16.1より前のバージョンでは、デフォルトのグローバルフロー制御（GFC）を使用することを推奨します。フロー制御設定が変更されている場合は、次のコマンドを使用してGFCを設定し `network port modify`ます。

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
full
```

  の詳細については `network port modify`、を"ONTAPコマンド リファレンス"参照してください。

クライアントシステム構成

NFS over RDMAでサポートされるクライアントオペレーティングシステムについては、を参照して "ネットアップのInteroperability Matrix（IMT ）"ください。RoCE v2でサポートされているRNICについては、それぞれのRNICベンダーのマニュアルを参照してください。

クライアントとサーバは直接接続できますが、フェイルオーバーのパフォーマンスを向上させるためにはスイッチの使用を推奨します。

クライアント、サーバ、スイッチ、およびスイッチ上のすべてのポートは、ジャンボフレームを使用して設定する必要があります。クライアントとスイッチのフロー制御設定は、ONTAPのフロー制御設定と一致している必要があります。ONTAP 9.16.1以降では、ONTAP、スイッチ、およびクライアントで優先度フロー制御を有効にして設定することを推奨します。ONTAP 9.16.1より前のバージョンでは、グローバルフロー制御を使用することを推奨します。

この設定を確認したら、RDMAを使用してNFSエクスポートをマウントできます。

System Manager

Managerを使用してoverのネットワークインターフェイスを設定するには、ONTAP 9 12.1以降を使用している必要があります。

手順

1. RDMAがサポートされているかどうかを確認します。[Network]>[Ethernet Ports]に移動し、グループビューで適切なノードを選択します。ノードを展開するときに、特定のポートの* rdma protocols フィールドを確認します。 RoCE は**RDMA**がサポートされていることを示し、ダッシュ（-*）はサポートされていないことを示します。
2. VLANを追加するには、**+VLAN***を選択します。適切なノードを選択します。**[ポート]***ドロップダウンメニューで、使用可能なポートに「 RoCE Enabled *」というテキストが表示されます（RDMAがサポートされている場合）。RDMAがサポートされていない場合は、テキストは表示されません。
3. 新しいNFSサーバを設定するには、のワークフローに従いNFSを使用したLinuxサーバ用のNASストレージの有効化ます。

   ネットワークインターフェイスを追加する際には、「* RoCEポートを使用*」を選択できます。RDMA経由のNFSを使用するすべてのネットワークインターフェイスに対して、このオプションを選択します。

CLI

1. コマンドを使用して、NFSサーバでRDMAアクセスが有効になっているかどうかを確認します。

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   デフォルトでは、 `-rdma`が有効になっている必要があります。有効になっていない場合は、NFSサーバでRDMAアクセスを有効にします。

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. RDMA経由でNFSv4.0を使用してクライアントをマウントします。
   a. protoパラメータの入力は、サーバのIPプロトコルのバージョンによって異なります。IPv4の場合は、を使用し `proto=rdma`ます。IPv6の場合は、を使用し `proto=rdma6`ます。
   b. 標準ポート2049ではなく、NFSターゲットポートをとして指定し `port=20049`ます。

      ```
      mount -o vers=4,minorversion=0,proto=rdma,port=20049
      <Server_IP_address>:/<volume_path> <mount_point>
      ```

3. オプション：クライアントをアンマウントする必要がある場合は、次のコマンドを実行します。
   `unmount <mount_path>`

詳細情報

- ONTAP NFSサーバーを作成する
- NFSを使用したLinuxサーバ用のNASストレージの有効化

RDMA経由のNFS用のLIFの設定

RDMA経由のNFSを使用するには、LIF（ネットワークインターフェイス）をRDMAと互換性があるように設定する必要があります。LIFとそのフェイルオーバーペアの両方でRDMAがサポートされている必要があります。

新しいLIFを作成する

System Manager

Managerで経由の用のネットワークインターフェイスを作成するには、ONTAP 9 .12.1以降を実行している必要があります。

手順

1. Network > Overview > Network Interfaces *を選択します。
2. を選択します ＋ Add 。
3. NFS、SMB / CIFS、S3 を選択すると、[RoCEポートを使用]*オプションが表示されます。「RoCEポートを使用する」のチェックボックスをオンにします。
4. Storage VMとホームノードを選択します。名前、 IPアドレス、およびサブネットマスクを割り当てます。
5. IPアドレスとサブネットマスクを入力すると、System Managerはブロードキャストドメインのリストをを備えたドメインにフィルタリングします。ブロードキャストドメインを選択してください。必要に応じてゲートウェイを追加できます。
6. [保存（ Save ）] を選択します。

CLI

手順

1. LIFを作成します。

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - サービスポリシーは、default-data-files、またはdata-NFSネットワークインターフェイスサービスを含むカスタムポリシーのいずれかである必要があります。
   - `-rdma-protocols`パラメータにはリストを指定できます。このリストはデフォルトでは空です。`roce`を値として追加すると、LIFはRoCEオフロードをサポートしているポートにのみ設定でき、Bot LIFの移行とフェイルオーバーに影響します。

LIFを変更する

System Manager

Managerで経由の用のネットワークインターフェイスを作成するには、ONTAP 9 .12.1以降を実行している必要があります。

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*>[編集]*を選択します ⋮ 。
3. RoCEポートを使用する*をオンにしてNFS over RDMAを有効にするか、オフにして無効にしてください。ネットワークインターフェイスがRoCE対応ポート上にある場合は、「RoCEポートを使用する」の横にチェックボックスが表示されます。
4. 必要に応じて他の設定を変更します。
5. 「* Save *（保存）」を選択して、変更を確定します。

CLI

1. LIFのステータスは、コマンドを使用して確認できます `network interface show`。サービスポリシーにはdata-NFSネットワークインターフェイスサービスを含める必要があります。 `-rdma -protocols`リストにはを含める必要があります `roce`。上記のいずれかの条件が満たされていない場合は、LIFを変更します。

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. LIFを変更するには、次のコマンドを実行します。

   ```
   network interface modify vserver SVM_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address
   IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
   -policy policy_name -auto-revert {true|false} -rdma-protocols roce
   ```

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

ⓘ 特定のオフロードプロトコルを必要とするようにLIFを変更するときに、そのプロトコルをサポートするポートにLIFが現在割り当てられていないとエラーが発生します。

LIFを移行する

ONTAPでは、RDMA経由のNFSを使用するためにネットワークインターフェイス（LIF）を移行することもできます。この移行を実行する場合は、デスティネーションポートがRoCEに対応していることを確認する必要があります。ONTAP 9.12.1以降では、この手順をSystem Managerで実行できます。System Managerは、ネットワークインターフェイスのデスティネーションポートを選択する際に、RoCEに対応しているかどうかを指定します。

LIFをRDMA経由のNFS構成に移行できるのは、次の場合のみです。

- RoCE対応ポートでホストされるNFS RDMAネットワークインターフェイス（LIF）です。

- RoCE対応ポートでホストされるNFS TCPネットワークインターフェイス（LIF）です。
- RoCE非対応のポートでホストされるNFS TCPネットワークインターフェイス（LIF）です。

ネットワークインターフェイスの移行の詳細については、を参照してくださいLIFを移行する。

関連情報

- LIFの作成
- LIFの作成
- LIFを変更する
- LIFを移行する

NFS設定を変更する

ほとんどの場合、RDMA経由のNFS用のNFS対応Storage VMの設定を変更する必要はありません。

ただし、MellanoxチップとLIFの移行に関連する問題に対処している場合は、NFSv4ロック猶予期間を延長する必要があります。デフォルトでは、猶予期間は45秒に設定されています。ONTAP 9 .10.1以降では、猶予期間の最大値は180（秒）です。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

このタスクの詳細については、を参照してくださいONTAP SVMのNFSv4ロック猶予期間を指定する。

CLIを使用したSMBの設定

ONTAP CLIを使用したSMB設定の詳細

ONTAP 9 CLIコマンドを使用して、新規または既存のSVMの新しいボリュームまたはqtreeに格納されているファイルへのSMBクライアントアクセスを設定できます。

> *SMB*(Server Message Block) は、 Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（ CLI ）および OnCommand 管理ツールでは、 _cifs_という メッセージが引き続き表示されます。

次の手順は、ボリュームまたはqtreeへのSMBアクセスを設定する場合に使用します。想定している状況は次のとおりです。

- SMBバージョン2以降を使用する。

- NFSクライアントではなく、SMBクライアントのみを処理する（マルチプロトコル構成ではない）。
- 新しいボリュームはNTFSファイル権限を使用して保護されます。
- SVM管理者Privilegesではなく、クラスタ管理者Privilegesが必要です。

  SVM と LIF を作成するにはクラスタ管理者権限が必要です。他の SMB 設定タスクには、 SVM 管理者権限で十分です。

- System Managerや自動スクリプトツールではなく、CLIを使用する必要がある。

  System Managerを使用してNASマルチプロトコルアクセスを設定する方法については、を参照してください"NFSとSMBの両方を使用したWindowsとLinux用のNASストレージのプロビジョニング"。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

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

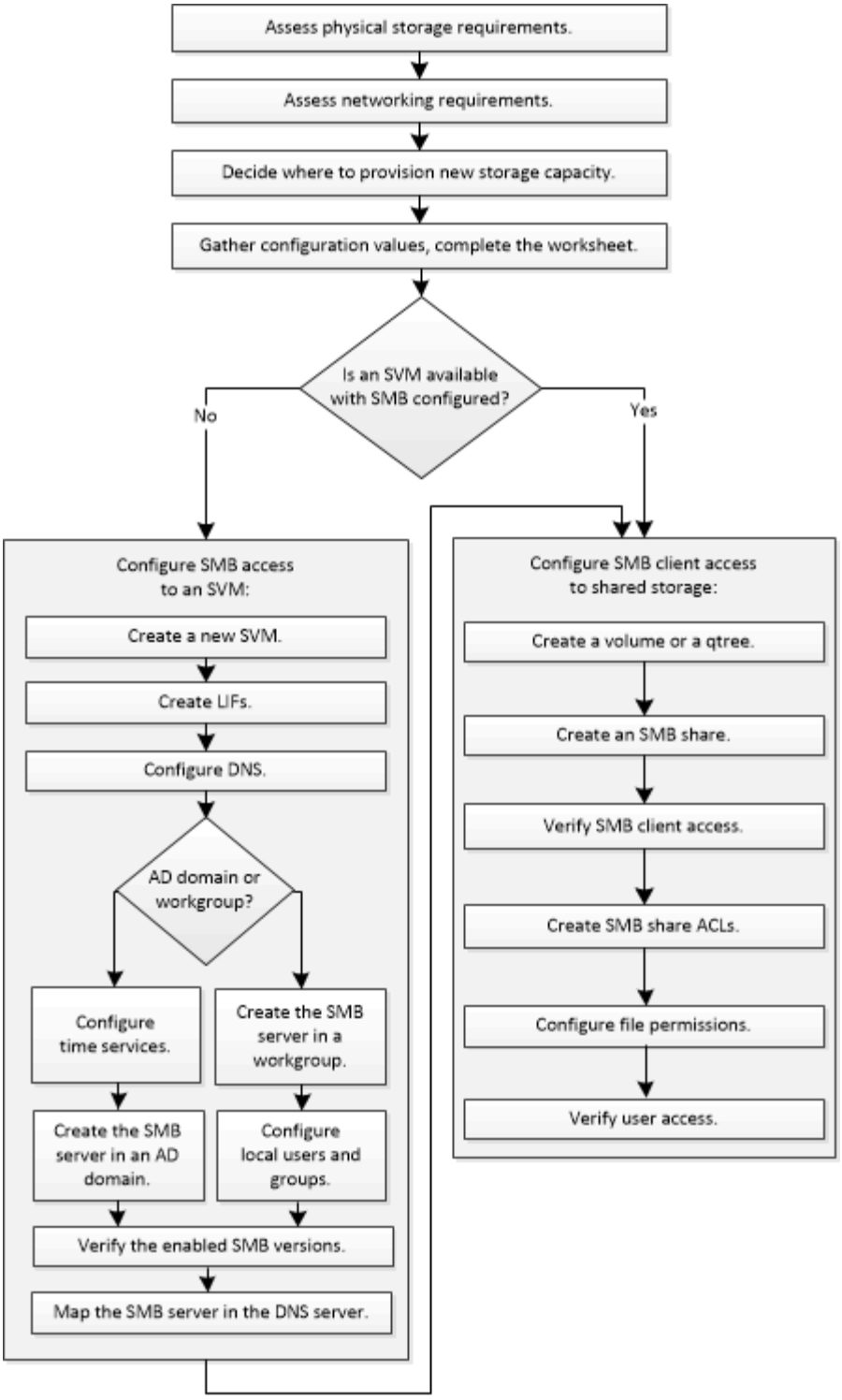
ONTAP SMBプロトコル機能の範囲の詳細については、を参照して"SMBリファレンスノガイヨウ"ください。

ONTAPで実行するその他の方法

実行するタスク	参照先
再設計されたSystem Manager（ONTAP 9 .7以降で使用可能）	"SMBを使用したWindowsサーバ用のNASストレージのプロビジョニング"
System Manager Classic（ONTAP 9 .7以前で使用可能）	"SMBセツテイノカイヨウ"

ONTAP SMBの設定ワークフロー

SMBを設定するには、物理ストレージとネットワークの要件を評価し、目的に応じたワークフローを選択します。新規または既存のSVMへのSMBアクセスを設定するか、すでにSMBアクセスの設定が完了している既存のSVMにボリュームまたはqtreeを追加します。



準備

ONTAP SMB物理ストレージ要件の評価

クライアント用のSMBストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリューム用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。 `storage aggregate show`

   十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 十分なスペースを備えたアグリゲートがない場合は、コマンドを使用して既存のアグリゲートにディスクを追加する `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成し `storage aggregate create`ます。

関連情報

- "storage aggregate add-disks"
- "storage aggregate create"

ONTAP SMBネットワーク要件の評価

クライアントにSMBストレージを提供する前に、SMBプロビジョニングの要件を満たすようにネットワークが正しく設定されていることを確認する必要があります。

開始する前に

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）

- 外部ファイアウォール

手順

1. 使用可能な物理ポートと仮想ポートを表示します。 `network port show`

   - 可能な場合は、データネットワークの速度が最も速いポートを使用してください。
   - 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

2. サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、サブネットが存在し、十分な数のアドレスが使用可能であることを確認します。 `network subnet show`

   の詳細については `network subnet show`、を"ONTAPコマンド リファレンス"参照してください。

   サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。

   の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

3. 使用可能なIPspaceを表示します。 `network ipspace show`

   デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

   の詳細については `network ipspace show`、を"ONTAPコマンド リファレンス"参照してください。

4. IPv6アドレスを使用する場合は、IPv6がクラスタで有効になっていることを確認します。 `network options ipv6 show`

   必要に応じて、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

   および `network options ipv6 modify`の詳細については `network options ipv6 show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBストレージ容量プロビジョニングの詳細

新しい SMB ボリュームまたは qtree を作成する前に、その配置先を新規、既存のどちらの SVM にするかを決め、 SVM にどのような設定が必要になるかを確認しておく必要があります。この決定によって、ワークフローが決まります。

選択肢

- 新しい SVM 、または SMB が有効になっているものの設定されていない既存の SVM 上でボリュームまたは qtree をプロビジョニングする場合は、「 SVM への SMB アクセスの設定」と「 SMB 対応 SVM へのストレージ容量の追加」の両方の手順を実行します。

  SVMへのSMBアクセスの設定

  共有ストレージへの SMB クライアントアクセスの設定

次のいずれかに該当する場合は、新しいSVMを作成します。

- クラスタでSMBを初めて有効にする場合。
- クラスタ内の既存のSVMでSMBサポートを有効にするのが望ましくない場合。
- クラスタ内に SMB 対応 SVM が 1 つ以上あり、次のいずれかの接続が必要な場合。
  - ワークグループ内の別の Active Directory フォレストへの接続。
  - 分離されたネームスペース内の SMB サーバへの接続（マルチテナンシーシナリオ）。SMBが有効になっているが設定はまだ完了していない既存のSVMでストレージをプロビジョニングする場合も、このオプションを選択する必要があります。これは、SANアクセス用のSVMを作成した場合や、SVM作成時にプロトコルが有効になっていなかった場合に該当します。

SVMでSMBを有効にしたあとに、ボリュームまたはqtreeのプロビジョニングに進みます。

- SMB アクセスの設定が完了している既存の SVM でボリュームまたは qtree をプロビジョニングする場合は、「 SMB 対応 SVM へのストレージ容量の追加」の手順を実行します。

  共有ストレージへの SMB クライアントアクセスの設定

ONTAP SMB設定ワークシート

SMB設定ワークシートを使用すると、クライアントのSMBアクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所に関する決定に応じて、ワークシートのいずれかまたは両方のセクションを完了する必要があります。

- SVMへのSMBアクセスを設定する場合は、両方のセクションを完了する必要があります。

  SVMへのSMBアクセスの設定

  共有ストレージへの SMB クライアントアクセスの設定

- SMB対応SVMにストレージ容量を追加する場合は、2番目のセクションのみを完了する必要があります。

  共有ストレージへの SMB クライアントアクセスの設定

パラメータの詳細については、を"ONTAPコマンド リファレンス"参照してください。

SVMへの**SMB**アクセスの設定

- SVM を作成するためのパラメータ *

新しいSVMを作成する場合は、コマンドで次の値を指定します `vserver create`。の詳細については `vserver create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	新しいSVMの名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意のSVM名を適用する別の命名規則に従います。	
`-aggregate`	新しいSMBストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-rootvolume`	SVMルート ボリュームの一意の名前を指定します。	
`-rootvolume-security-style`	SVMのNTFSセキュリティ形式を使用します。	`ntfs`
`-language`	このワークフローではデフォルトの言語設定を使用します。	`C.UTF-8`
`ipspace`	オプション： IPspace は、 SVM が配置される個別の IP アドレススペースです。	

- LIF 作成用のパラメータ *

LIFを作成する場合は、コマンドで次の値を指定します `network interface create`。の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-lif`	新しいLIFの名前を指定します。	
`-role`	このワークフローではデータLIFのロールを使用します。	`data`
`-data-protocol`	このワークフローではSMBプロトコルのみを使用します。	`cifs`

フィールド	説明	あなたの価値
-home-node	LIFに対してコマンドを実行したときにLIFが戻るノード network interface revert。 の詳細については network interface revert、を"ONTAPコマンド リファレンス"参照してください。	
-home-port	LIFに対してコマンドを実行したときにLIFが戻るポートまたはインターフェイスグループ network interface revert。	
-address	新しいLIFによるデータアクセスに使用する、クラスタ上のIPv4アドレスまたはIPv6アドレスを指定します。	
-netmask	LIFのネットワークマスクとゲートウェイ。	
-subnet	IPアドレスのプール。および -netmask`の代わりに使用して `-address、アドレスとネットマスクを自動的に割り当てます。	
-firewall-policy	このワークフローではデフォルトのデータファイアウォールポリシーを使用します。	data
-auto-revert	オプション：起動時またはその他の状況下でデータ LIF がホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はです false。	

- DNS ホスト名解決のパラメータ *

DNSを設定する場合は、コマンドで次の値を指定します vserver services name-service dns create。の詳細については vserver services name-service dns create、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-domains	最大5つのDNSドメイン名。	

フィールド	説明	あなたの価値
-name-servers	DNSネームサーバごとに最大3つのIPアドレス。	

Active Directoryドメインでの**SMB**サーバのセットアップ

- タイムサービス設定のパラメータ *

タイムサービスを設定する場合は、コマンドで次の値を指定します `cluster time-service ntp server create`。の詳細については `cluster time-service ntp server create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-server	Active Directory ドメイン用の NTP サーバのホスト名または IP アドレスを指定します。	

- Active Directory ドメイン内に SMB サーバを作成するためのパラメータ *

新しいSMBサーバを作成し、ドメイン情報を指定する場合は、コマンドで次の値を指定します `vserver cifs create`。の詳細については `vserver cifs create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-vserver	SMB サーバを作成する SVM の名前を指定します。	
-cifs-server	SMB サーバの名前（最大 15 文字）を指定します。	
-domain	SMB サーバに関連付ける Active Directory ドメインの完全修飾ドメイン名（ FQDN ）を指定します。	
-ou	オプション： SMB サーバに関連付ける Active Directory ドメイン内の組織単位を指定します。デフォルトでは、このパラメータはCN=Computersに設定されています。	
-netbios-aliases	オプション： NetBIOS エイリアスのリストを指定します。 NetBIOS エイリアスは、 SMB サーバ名の別名です。	

フィールド	説明	あなたの価値
-comment	オプション：サーバのテキストコメントを指定します。Windowsクライアントは、ネットワーク上のサーバを参照するときに、SMBサーバの説明を確認できます。	

ワークグループでの**SMB**サーバのセットアップ

- ワークグループで SMB サーバーを作成するためのパラメータ *

新しいSMBサーバを作成し、サポートされているSMBバージョンを指定する場合は、コマンドで次の値を指定し `vserver cifs create`ます。の詳細については `vserver cifs create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-vserver	SMB サーバを作成する SVM の名前を指定します。	
-cifs-server	SMB サーバの名前（最大 15 文字）を指定します。	
-workgroup	ワークグループの名前（最大 15 文字）を指定します。	
-comment	オプション：サーバのテキストコメントを指定します。Windowsクライアントは、ネットワーク上のサーバを参照するときに、SMBサーバの説明を確認できます。	

- ローカルユーザー作成用のパラメータ *

コマンドを使用してローカルユーザを作成する場合は、次の値を指定し `vserver cifs users-and-groups local-user create`ます。これらの値は、ワークグループ内、およびオプションで `AD` ドメイン内の `SMB` サーバに必要です。の詳細については `vserver cifs users-and-groups local-user create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-vserver	ローカルユーザを作成する SVM の名前を指定します。	
-user-name	ローカルユーザの名前（最大 20 文字）を指定します。	

フィールド	説明	あなたの価値
`-full-name`	オプション：ユーザのフルネームを指定します。フルネームにスペースが含まれている場合は、フルネームを二重引用符で囲みます。	
`-description`	オプション：ローカルユーザの概要。説明にスペースが含まれている場合は、パラメータを引用符で囲みます。	
`-is-account-disabled`	オプション：ユーザアカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。	

- ローカルグループを作成するためのパラメータ *

コマンドを使用してローカルグループを作成する場合は、次の値を指定し `vserver cifs users-and-groups local-group create`ます。AD ドメインおよびワークグループ内の SMB サーバの場合はオプションです。の詳細については `vserver cifs users-and-groups local-group create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	ローカルグループを作成する SVM の名前を指定します。	
`-group-name`	ローカルグループの名前（最大 256 文字）を指定します。	
`-description`	オプション：ローカルグループの概要。説明にスペースが含まれている場合は、パラメータを引用符で囲みます。	

SMB対応**SVM**へのストレージ容量の追加

- ボリュームを作成するためのパラメータ *

qtreeではなくボリュームを作成する場合は、コマンドで次の値を指定します `volume create`。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	新しいボリュームをホストする新規または既存のSVMの名前を指定します。	
`-volume`	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
`-aggregate`	新しいSMBボリューム用の十分なスペースがあるクラスタ内のアグリゲートの名前を指定します。	
`-size`	新しいボリュームのサイズとして任意の整数を指定します。	
`-security-style`	このワークフローにはNTFSセキュリティ形式を使用します。	`ntfs`
`-junction-path`	新しいボリュームのマウント先とする、ルート（/）の下の場所を指定します。	

- qtree を作成するためのパラメータ *

ボリュームではなくqtreeを作成する場合は、コマンドで次の値を指定します `volume qtree create`。の詳細については `volume qtree create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	qtreeを含むボリュームが配置されているSVMの名前。	
`-volume`	新しいqtreeを格納するボリュームの名前。	
`-qtree`	新しいqtreeには、64文字以下の一意のわかりやすい名前を指定します。	
`-qtree-path`	ボリュームとqtreeを別 々 の引数として指定する代わりに、qtreeパスをの形式で `/vol/volume_name/qtree_name\>` 指定できます。	

- SMB 共有作成のパラメータ *

コマンドでは、次の値を指定します `vserver cifs share create`。の詳細については `vserver cifs share create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	SMB 共有を作成する SVM の名前を指定します。	
`-share-name`	作成する SMB 共有の名前（最大 256 文字）を指定します。	
`-path`	SMB 共有へのパスの名前（最大 256 文字）を指定します。このパスは、共有を作成する前にボリューム内に存在している必要があります。	
`-share-properties`	オプション：共有プロパティのリストを指定します。デフォルト設定は `oplocks`、、 `browsable changenotify`、および `show-previous-versions`です。	
`-comment`	オプション：サーバのテキストコメント（最大 256 文字）を指定します。Windows クライアントは、ネットワーク上で参照するとき、この SMB 共有概要を確認できます。	

* SMB 共有アクセス制御リスト（ ACL ）を作成するためのパラメータ *

コマンドでは、次の値を指定します `vserver cifs share access-control create`。の詳細については `vserver cifs share access-control create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	SMB ACL を作成する SVM の名前を指定します。	
`-share`	作成先の SMB 共有の名前を指定します。	
`-user-group-type`	共有の ACL に追加するユーザまたはグループのタイプを指定します。デフォルトのタイプはです。 `windows`	`windows`

フィールド	説明	あなたの価値
`-user-or-group`	共有の ACL に追加するユーザまたはグループを指定します。ユーザ名を指定する場合は、「ドメイン名」の形式でユーザのドメインを含める必要があります。	
`-permission`	ユーザまたはグループの権限を指定します。	`[No_access
Read	Change	Full_Control]`

SVMへのSMBアクセスの設定

ONTAP SVMへのSMBアクセスの設定

SMB クライアントアクセス用に SVM を設定していない場合は、新しい SVM を作成して設定するか、既存の SVM を設定する必要があります。SMB を設定する場合は、 SVM ルートボリュームへのアクセスを許可し、 SMB サーバを作成し、 LIF を作成し、ホスト名解決を有効にし、ネームサービスを設定し、必要に応じて Kerberos セキュリティの有効化。

ONTAP SVMを作成してSMBデータアクセスを提供する

SMBクライアントにデータアクセスを提供するSVMがクラスタ内に1つもない場合は、SVMを作成する必要があります。

開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

手順

1. SVMを作成します。 `vserver create -vserver *svm_name* -rootvolume *root_volume_name* -aggregate *aggregate_name* -rootvolume-security-style ntfs -language C.UTF-8 -ipspace *ipspace_name*`
   - オプションにはNTFS設定を使用し `-rootvolume-security-style`ます。
   - デフォルトのC.UTF-8オプションを使用し `-language`ます。
   - この `ipspace`設定はオプションです。
2. 新しく作成したSVMの設定とステータスを確認します。 `vserver show -vserver *vserver_name*`

   `Allowed Protocols`フィールドに CIFSを含める必要があります。このリストは後で編集できます。

`Vserver Operational State`フィールドには状態が表示されている必要があり `running`ます。状態が表示された場合は `initializing`、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

例

次のコマンドは、データアクセス用のSVMをIPspace内に作成し `ipspaceA`ます。

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて状態になっていることを示しています running。ルートボリュームには、ルールが含まれていないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

ONTAP SVMでSMBプロトコルが有効になっていることを確認する

SVMでSMBを設定して使用する前に、プロトコルが有効になっていることを確認する必要があります。

タスクの内容

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、コマンドを使用してあとから有効にすることができます `vserver add-protocols`。

作成したプロトコルは、 LIF から追加または削除することはできません。

コマンドを使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols`。

手順

1. SVMに対して現在有効または無効になっているプロトコルを確認します。 `vserver show -vserver vserver_name -protocols`

   コマンドを使用して、クラスタ内のすべてのSVMで現在有効になっているプロトコルを表示することもできます `vserver show-protocols`。

2. 必要に応じて、プロトコルを有効または無効にします。
   - SMBプロトコルを有効にする手順は次のとおりです。 `vserver add-protocols -vserver vserver_name -protocols cifs`
   - プロトコルを無効にするには： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. 有効なプロトコルと無効なプロトコルが正しく更新されたことを確認します。 `vserver show -vserver vserver_name -protocols`

例

次のコマンドは、 vs1 という SVM で現在有効 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

次のコマンドは、vs1というSVMで有効になっているプロトコルのリストにを追加することで、SMB経由のアクセスを許可し `cifs`ます。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

ONTAP SVMルートボリュームの**SMB**エクスポートポリシーを開く

SVMルートボリュームのデフォルトのエクスポートポリシーには、すべてのクライアントにSMB経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVMとそのボリュームに対するSMBクライアントのアクセスがすべて拒否されます。

タスクの内容

新しいSVMが作成されると、デフォルトのエクスポートポリシー（default）がSVMのルートボリュームに対して自動的に作成されます。SVM上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを1つ以上作成する必要があります。

デフォルトのエクスポートポリシーですべてのSMBアクセスが開いていることを確認してから、個 々 のボリュームまたはqtreeにカスタムのエクスポートポリシーを作成して個 々 のボリュームへのアクセスを制限します。

手順

1. 既存のSVMを使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。
`vserver export-policy rule show`

   次のようなコマンド出力が表示されます。

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

   オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVMルートボリュームのエクスポートルールを作成します。 `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. コマンドを使用してルールの作成を確認します `vserver export-policy rule show`。

結果

これで、SVMで作成されたすべてのボリュームまたはqtreeに、すべてのSMBクライアントからアクセスできるようになります。

ONTAP SMB LIFの作成

LIFは、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

開始する前に

- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

- LIFで処理されるトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9 .5以前では、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。

  の詳細については `network interface`、を"ONTAPコマンド リファレンス"参照してください。

- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、同じサブネットにすでに設定されている他のLIFと同じブロードキャストドメイン内の指定したホームノード上の任意のポートを自動的に選択します。

手順

1. LIFを作成します。

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol cifs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

* ONTAP 9.5 以前 *
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

* ONTAP 9.6 以降 *
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - `-role`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。
   - `-data-protocol`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。ONTAP 9 .5以前を使用している場合は `-data-protocol`、LIFの作成時にパラメータを指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。
   - `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network`

interface revert。

オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます -auto-revert。

- -home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert。
- オプションと -netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address。
- サブネットを使用してIPアドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときに、ゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
- IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内での静的ルートの作成に関する詳細については、を"ONTAPコマンド リファレンス"参照し `network route create`てください。
- オプションには -firewall-policy、LIFのロールと同じデフォルトを使用し `data`ます。

  必要に応じて、あとからカスタムファイアウォールポリシーを作成して追加できます。

  ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- -auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false。

2. LIFが正常に作成されたことを確認します。

   network interface show

3. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	network ping
IPv6アドレス	network ping6

例

次のコマンドは、LIFを作成し、パラメータと `-netmask`パラメータを使用してIPアドレスとネットワークマスク値を指定し `-address`ます。

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワークマスク値を指定したサブネット（client1_sub）から割り当てます。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

次のコマンドは、サービスポリシーが割り当てられたNASデータLIFを作成する方法を示してい `default-data-files`ます。

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

関連情報

- "ネットワークping"
- "ネットワークインターフェイスのリバート"

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定できvserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。の詳細については `vserver services name-service dns、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。の詳細については `vserver services name-service dns create、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

詳細については、をご覧ください "SVM でのダイナミック DNS の設定"。

手順

1. SVMでDNSを有効にします。vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   コマンドは `vserver services name-service dns create`設定の自動検証を実行し、ONTAPがネームサーバに接続できない場合はエラーメッセージを報告します。

2. コマンドを使用して、DNSドメイン設定を表示しますvserver services name-service dns show。

   次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. コマンドを使用して、ネームサーバのステータスを検証し `vserver services name-service dns check`ます。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Active DirectoryドメインでのSMBサーバのセットアップ

SMBサーバのONTAPタイムサービスの設定

アクティブドメインコントローラでSMBサーバを作成する前に、クラスタ時間とSMBサーバが属するドメインのドメインコントローラの時間のずれが5分以内であることを確認する必要があります。

タスクの内容

同期には、Active Directory ドメインが使用するのと同じ NTP サーバーを使用するようにクラスター NTP サービスを構成する必要があります。

手順

1. コマンドを使用してタイムサービスを設定します `cluster time-service ntp server create`。
   - 対称認証を使用せずにタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address`
   - 対称認証を使用してタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. コマンドを使用して、タイムサービスが正しく設定されていることを確認します `cluster time-service ntp server show`。

```
cluster time-service ntp server show
```

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

関連情報

- "クラスタタイムサービスNTP"

サーバの対称認証を管理するための**ONTAP**コマンド

ONTAP 9 .5以降では、ネットワークタイムプロトコル（NTP）バージョン3がサポートされます。NTPv3にはSHA-1キーを使用した対称認証が含まれているため、ネットワークセキュリティが向上します。

作業	使用するコマンド
対称認証を使用せずにNTPサーバを設定する	`cluster time-service ntp server create -server server_name`
対称認証を使用してNTPサーバを設定する	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
既存のNTPサーバの対称認証を有効にする必要なキーIDを追加することで、既存のNTPサーバを変更して認証を有効にすることができます。	`cluster time-service ntp server modify -server server_name -key-id key_id`
共有NTPキーを設定する	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共有キーはIDで参照されます。ID、そのタイプ、および値がノードとNTPサーバの両方で同じである必要があります。
不明なキーIDでNTPサーバを設定する	`cluster time-service ntp server create -server server_name -key-id key_id`

作業	使用するコマンド
NTPサーバで設定されていないキーIDでサーバを設定します。	`cluster time-service ntp server create -server server_name -key-id key_id` キーID、タイプ、および値は、NTPサーバに設定されているキーID、タイプ、および値と同じである必要があります。
対称認証を無効にする	`cluster time-service ntp server modify -server server_name -authentication disabled`

関連情報

- "クラスタタイムサービスNTP"

ONTAP Active Directoryドメインに**SMB**サーバを作成する

コマンドを使用すると、SVM上にSMBサーバを作成し、所属先のActive Directory（AD）ドメインを指定できます `vserver cifs create`。

開始する前に

データ処理に使用するSVMおよびLIFが、SMBプロトコルを許可するように設定されている必要があります。LIFは、SVM上で設定されているDNSサーバ、およびSMBサーバの追加先ドメインのADドメインコントローラに接続できる必要があります。

SMBサーバの追加先のADドメイン内のマシンアカウントの作成を許可されているすべてのユーザが、SVM上にSMBサーバを作成できます。これには、他のドメインのユーザを含めることができます。

ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

タスクの内容

Activity DirectoryドメインにSMBサーバを作成する場合は、次の点に注意してください。

- ドメインを指定するときは、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用する必要があります。
- デフォルト設定では、SMBサーバマシンアカウントはActive Directory CN=Computerオブジェクトに追加されます。
- オプションを使用すると、SMBサーバを別の組織単位（OU）に追加できます `-ou`。
- 必要に応じて、SMBサーバの1つ以上のNetBIOSエイリアス（最大200）をカンマで区切って追加できます。

  SMBサーバのNetBIOSエイリアスを設定すると、他のファイルサーバのデータをSMBサーバに統合し、SMBサーバが元のサーバの名前に応答するようにする場合に役立ちます。

およびオプションのパラメータと命名要件の詳細については `vserver cifs`、を参照し"ONTAPコマンドリファレンス"てください。

ONTAP 9 .8以降では、ドメインコントローラへの接続を暗号化するように指定できます。ONTAPオプションがに設定され `true`ている場合、ドメインコントローラの通信に暗号化が必要です `-encryption-required-for-dc-connection`。デフォルトはです。 `false`暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されます。です。

"SMBの管理"SMBサーバ設定オプションの詳細については、を参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMBサーバを認証のみに使用する場合は、CIFSライセンスは必要ありません。

2. ADドメインにSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

   次のコマンドは、ドメイン「 example.com`": 」に SMB サーバ「 'smb_server01' 」を作成します

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   次のコマンドは、ドメイン「 m ydomain.com`" 」に SMB サーバ「 'smb_server02' 」を作成し、 keytab ファイルを使用して ONTAP 管理者を認証します。

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. コマンドを使用して、SMBサーバの設定を確認します `vserver cifs show`。

   この例では、「 `s MB_SERVER01' 」という名前の SMB サーバが SVM vs1.example.com 上に作成され、「 example.com`" ドメイン」に追加されたことがコマンド出力に示されています。

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. 必要に応じて、ドメインコントローラ（ONTAP 9 .8以降）との暗号化通信を有効にします。 `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

例

次のコマンドは、 SVM vs2.example.com の「 example.com`" 」ドメインに「 'MB_Server02' 」という名前の SMB サーバを作成します。マシン・アカウントは "`OU=eng 、 OU=corp 、 DC=example 、 DC=com コンテナに作成されますSMBサーバにはNetBIOSエイリアスが割り当てられます。

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                      CIFS Server NetBIOS Name: SMB_SERVER02
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
              CIFS Server Administrative Status: up
                        CIFS Server Description: -
                        List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

次のコマンドは、別のドメインのユーザ（ここでは信頼できるドメインの管理者）が、 SVM vs3.example.com 上に「 smb_server03 」という名前の SMB サーバを作成できるようにします。オプションは `-domain`、SMBサーバを作成するホームドメイン（DNSの設定で指定）の名前を指定します。オプションは `username`、信頼できるドメインの管理者を指定します。

- ホームドメイン：example.com
- 信頼できるドメイン：trust.lab.com
- 信頼できるドメインのユーザ名： Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

ONTAP SMB認証用のkeytabファイルの作成

ONTAP 9.7 以降 ONTAP では、 keytab ファイルを使用した Active Directory （ AD ）サーバとの SVM 認証がサポートされます。AD管理者はkeytabファイルを生成し、Uniform Resource Identifier（URI）としてONTAP管理者が使用できるようにします。このURIは、コマンドでADドメインとのKerberos認証が必要な場合に指定します `vserver cifs`。

AD管理者は、Windows Serverの標準コマンドを使用してkeytabファイルを作成できます `ktpass`。このコマンドは、認証が必要なプライマリドメインで実行する必要があります。 `ktpass`コマンドを使用してkeytabファイルを生成できるのはプライマリドメインユーザのみです。信頼できるドメインユーザを使用して生成されたキーはサポートされません。

keytab ファイルは、特定の ONTAP 管理者ユーザ用に生成されます。管理者ユーザのパスワードが変更されないかぎり、特定の暗号化タイプとドメインに対して生成されたキーは変更されません。そのため、管理者ユーザのパスワードを変更するたびに、新しいkeytabファイルが必要になります。

次の暗号化タイプがサポートされています。

- AES256-SHA1
- DES-CBC-MD5

  ONTAP では、 DES-CBC-CRC 暗号化タイプはサポートされていません。

- RC4-HMAC

最も高度な暗号化タイプは AES256 です。 ONTAP システムで有効な場合は AES256 を使用してください。

keytab ファイルは、管理パスワードを指定して生成するか、ランダムに生成されたパスワードを使用して生成できます。ただし、 keytab ファイル内のキーを復号化するために AD サーバ側で管理者ユーザに固有な秘密鍵が必要になるため、ある時点で使用できるパスワードオプションはどちらか 1 つだけです。特定の管理者の秘密鍵を変更すると、 keytab ファイルは無効になります。

ワークグループでのSMBサーバのセットアップ

ONTAPワークグループでのSMBサーバ設定の詳細

ワークグループ内のメンバーとして SMB サーバをセットアップするには、 SMB サーバを作成してから、ローカルユーザとローカルグループを作成します。

Microsoft Active Directory ドメインインフラを使用できない場合は、ワークグループに SMB サーバを設定できます。

ワークグループモードの SMB サーバでは NTLM 認証のみがサポートされ、 Kerberos 認証はサポートされません。

指定したワークグループを使用して**ONTAP SVM**に**SMB**サーバを作成する

コマンドを使用すると、SVM上にSMBサーバを作成し、所属先のワークグループを指定できます `vserver cifs create`。

開始する前に

データ処理に使用するSVMおよびLIFが、SMBプロトコルを許可するように設定されている必要があります。LIFは、SVMで設定されているDNSサーバに接続できる必要があります。

タスクの内容

ワークグループモードのSMBサーバでは、SMBの次の機能はサポートされません。

- SMB3カンシフロトコル
- SMB3 CA共有
- SQL over SMB
- フォルダ リダイレクト
- 移動プロファイル
- グループ ポリシー オブジェクト（GPO）
- ボリュームSnapshotサービス（VSS）

およびオプションの設定パラメータと命名要件の詳細については `vserver cifs`、を参照して"ONTAPコマンド リファレンス"ください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMBサーバを認証のみに使用する場合は、CIFSライセンスは必要ありません。

2. ワークグループ内にSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   次のコマンドは ' ワークグループ "workgroup01" 内に SMB サーバ "'smb_server01" を作成します

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. コマンドを使用して、SMBサーバの設定を確認します `vserver cifs show`。

   次の例では、コマンド出力は、ワークグループ「 workgroup01 」内の SVM vs1.example.com 上に「

'smb_server01' 」という名前の SMB サーバが作成されたことを示しています。

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

終了後

ワークグループ内のCIFSサーバの場合は、SVM上にローカルユーザ、および必要に応じてローカルグループを作成する必要があります。

関連情報

"SMBの管理"

ローカル**ONTAP SMB**ユーザアカウントの作成

SVMに格納されたデータへのSMB接続を介したアクセスの認証に使用できるローカルユーザアカウントを作成できます。SMBセッションの作成時の認証にローカルユーザアカウントを使用することもできます。

タスクの内容

ローカルユーザの機能は、SVMの作成時にデフォルトで有効になります。

ローカルユーザアカウントを作成するときは、ユーザ名を指定する必要があり、アカウントを関連付けるSVMを指定する必要があります。

およびオプションのパラメータと命名要件の詳細については `vserver cifs users-and-groups local-user`、を参照し"ONTAPコマンド リファレンス"てください。

手順

1. ローカルユーザを作成します。 `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   次のオプションのパラメータが役に立つ場合があります。

   - `-full-name`

     ユーザのフルネーム。

- `-description`

  ローカルユーザの説明。

- `-is-account-disabled {true|false}`

  ユーザアカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。

ローカルユーザのパスワードの入力を求められます。

2. ローカルユーザのパスワードを入力し、確認のためにもう一度入力します。
3. ユーザが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

例

次の例では、 SVM vs1.example.com に関連付けられた「 `S MB_SERVER1\Sue` 」という完全な名前のローカルユーザ「 `S ue Chang-」 を作成します。

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

ローカル**ONTAP SMB**グループを作成する

SVM に関連付けられたデータへの SMB 接続によるアクセスの許可に使用できるローカルグループを作成できます。また、グループのメンバーに付与するユーザ権限と機能を定義した権限を割り当てることもできます。

タスクの内容

ローカルグループの機能は、 SVM の作成時にデフォルトで有効になります。

ローカルグループを作成するときは、グループの名前を指定する必要があり、グループを関連付ける SVM を指定する必要があります。グループ名を指定する際、ローカルドメイン名は指定してもしなくても構いません。また、オプションで、ローカルグループの概要を指定することもできます。別のローカルグループにローカルグループを追加することはできません。

およびオプションのパラメータと命名要件の詳細については `vserver cifs users-and-groups local-group`、を参照し"ONTAPコマンド リファレンス"てください。

手順

1. ローカルグループを作成します。 `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   次のオプションのパラメータが役に立つ場合があります。

   - `-description`

     ローカルグループの説明。

2. グループが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-group show -vserver vserver_name`

例

次の例では、 SVM vs1 に関連付けられるローカルグループ「 `s MB_SERVER01\engineering` 」を作成します。

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ------------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

終了後

新しいグループにメンバーを追加する必要があります。

ローカル**ONTAP SMB**グループメンバーシップを管理します。

ローカルグループメンバーシップの管理では、ローカルユーザまたはドメインユーザの追加と削除、またはドメイングループの追加と削除を行うことができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

タスクの内容

特定のグループのメンバーシップに基づいてローカルユーザ、ドメインユーザ、またはドメイングループに付与されたアクセス権や権限を取り消す場合に、メンバーをグループから削除できます。

メンバーをローカルグループに追加する場合は、次の点に注意する必要があります。

- 特殊なグループ _Everyone にユーザーを追加することはできません。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、 ONTAP で名前を SID に解決できる必要があります。

メンバーをローカルグループから削除する場合は、次の点に注意する必要があります。

- 特殊なグループ _Everyone からメンバーを削除することはできません。
- ローカルグループからメンバーを削除するには、 ONTAP で名前を SID に解決できる必要があります。

手順

1. メンバーをグループに追加するか、グループから削除します。
   - メンバーを追加します。 `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループに追加できます。

   - メンバーを削除します。 `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループから削除することができます。

例

次の例では、 SVM vs1.example.com 上のローカルグループ「 `s MB_SERVER01\engineering` 」にローカルユーザ「 ````s MB_SERVER01\engineering 」を追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

次の例では、 SVM vs1.example.com 上のローカルグループ「 `s MB_SERVER1\engineering` 」からローカルユーザ「 `s MB_SERVER01\Sue` 」および「 `S MB_SERVER01\engineering` 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

有効な**ONTAP SMB**バージョンの確認

クライアントおよびドメインコントローラとの接続に対してデフォルトで有効になっているSMBのバージョンは、ONTAP 9のリリースに応じて決まります。ご使用の環境で必

要なクライアントと機能がSMBサーバでサポートされていることを確認する必要があります。

タスクの内容

クライアントとドメインコントローラの両方と接続する場合は、可能なかぎりSMB 2.0以降を有効にしてください。セキュリティ上の理由から、SMB 1.0の使用は避け、ご使用の環境で不要であることが確認された場合は無効にしてください。

ONTAP 9 .3以降では、新しいSVMではデフォルトで無効になっています。

> がwhileに `-smb1-enabled`設定されて `false`いる場合 `-smb1-enabled-for-dc-connections true`、ONTAPはクライアントとしてのSMB 1.0の接続を拒否しますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

"SMBの管理"サポートされるSMBのバージョンと機能の詳細が表示されます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 有効になっているSMBのバージョンを確認します。

```
vserver cifs options show
```

リストを下方向にスクロールすると、クライアント接続用に有効になっているSMBのバージョンを表示できます。また、ADドメイン内のSMBサーバを設定している場合は、ADドメイン接続用に有効になっているバージョンを表示できます。

3. 必要に応じて、クライアント接続用のSMBプロトコルを有効または無効にします。
   - SMBバージョンを有効にする場合：

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

有効な値 `smb_version`は次のとおりです。

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

次のコマンドは、SVM vs1.example.comでSMB 3.1を有効にします。

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
```

```
-enabled true
```

- SMBバージョンを無効にするには：

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. SMBサーバがActive Directoryドメイン内にある場合は、必要に応じてDC接続用のSMBプロトコルを有効または無効にします。
   - SMBバージョンを有効にする場合：

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - SMBバージョンを無効にするには：

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. admin権限レベルに戻ります。

```
set -privilege admin
```

DNSサーバでの**ONTAP SMB**サーバのマッピング

Windows ユーザがドライブを SMB サーバ名にマッピングできるように、サイトの DNS サーバに、 SMB サーバ名および NetBIOS エイリアスをデータ LIF の IP アドレスにマッピングしたエントリを設定する必要があります。

開始する前に

サイトの DNS サーバに対する管理アクセス権が必要です。管理アクセス権がない場合は、 DNS 管理者にこのタスクの実行を依頼する必要があります。

タスクの内容

SMB サーバ名に NetBIOS エイリアスを使用する場合は、各エイリアスに DNS サーバのエントリポイントを作成することを推奨します。

手順

1. DNSサーバにログインします。
2. フォワードルックアップ（ A - アドレスレコード）とリバースルックアップ（ PTR - ポインタレコード）のエントリを作成して、 SMB サーバ名をデータ LIF の IP アドレスにマッピングします。
3. NetBIOS エイリアスを使用する場合は、エイリアスの正規名（ CNAME リソースレコード）のルックアッ

プエントリを作成して、各エイリアスを SMB サーバのデータ LIF の IP アドレスにマッピングします。

結果

ネットワーク全体にマッピングが反映されると、 Windows ユーザがドライブを SMB サーバ名またはその NetBIOS エイリアスにマッピングできるようになります。

共有ストレージへの**SMB**クライアントアクセスの設定

共有**ONTAP**ストレージへの**SMB**クライアントアクセスの設定

SVM 上の共有ストレージに対する SMB クライアントアクセスを許可するには、ストレージコンテナを提供するボリュームまたは qtree を作成し、そのコンテナの共有を作成または変更する必要があります。その後、共有およびファイルの権限を設定し、クライアントシステムからのアクセスをテストできます。

開始する前に

- SVMでSMBの設定が完了している必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Active Directory ドメインまたはワークグループ設定への追加または変更が完了している必要があります。

ボリュームまたは**qtree**のストレージコンテナを作成する

ONTAP SMBボリュームの作成

コマンドを使用すると、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create`。

タスクの内容

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームの作成時に指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、コマンドを使用して、SVMネームスペースでボリュームを_mount_theにする必要があります `volume mount`。

開始する前に

- SMBがセットアップされて実行されている必要があります。
- SVMのセキュリティ形式はNTFSである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. ジャンクションポイントを設定してボリュームを作成します。 `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]}`

`-security-style ntfs -junction-path` *junction_path*]

の選択肢は `-junction-path`次のとおりです。

- ルートの直下。例： `/new_vol`

  新しいボリュームを作成し、 SVM のルートボリュームに直接マウントされるように指定することができます。

- 既存のディレクトリの下（例： `/existing_dir/new_vol`

  新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

たとえば、新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は `/new_dir/new_vol`、SVMのルートボリュームにジャンクションされている新しい親ボリュームを最初に作成する必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 `volume show -vserver` *svm_name* `-volume` *volume_name* `-junction`

例

次のコマンドは、 SVM vs1.example.com およびアグリゲート aggr1 上に、 users1 という名前の新しいボリュームを作成します。新しいボリュームは、で使用でき `/users`ます。ボリュームのサイズは750GBで、ボリュームギャランティのタイプはvolume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

次のコマンドでは、「 home4` 」という名前の新しいボリュームを SVM 「 vs1.example.com`" 」およびアグリゲート「 aggr1 」に作成します。ディレクトリは `/eng/`vs1 SVM`のネームスペース内にすでに存在し、新しいボリュームがで使用可能になります `/eng/home`。これがネームスペースのホームディレクトリになります。 `/eng/`ボリュームのサイズは`750GB`で、ボリュームギャランティのタイプは（デフォルト）です `volume`。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

ONTAP SMB qtreeの作成

コマンドを使用すると、データを含むqtreeを作成し、そのプロパティを指定できます `volume qtree create`。

開始する前に

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVMのセキュリティ形式はNTFSであり、SMBがセットアップされて実行されている必要があります。

手順

1. qtreeを作成します。 `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   ボリュームとqtreeを別 々 の引数として指定するか、の形式でqtreeパスの引数を指定できます `/vol/volume_name/_qtree_name`。

2. 目的のジャンクションパスでqtreeが作成されたことを確認します。 `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成し `/vol/data1`ます。

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
         Is Export Policy Inherited: true
```

ONTAP SMB共有を作成する際の要件と考慮事項

SMB 共有を作成する前に、特にホームディレクトリに関して、共有パスと共有プロパティの要件を理解しておく必要があります。

SMB共有を作成するには、クライアントがアクセスするディレクトリパス構造を（コマンドのオプションを`vserver cifs share create`使用して）指定する必要があり`-path`ます。ディレクトリパスは、 SVM ネームスペース内に作成したボリュームまたは qtree のジャンクションパスに相当します。ディレクトリパスと対応するジャンクションパスは、共有を作成する前に存在している必要があります。

共有パスには次の要件があります。

- ディレクトリパス名の最大文字数は255文字です。
- パス名にスペースが含まれている場合は、文字列全体を引用符で囲む必要があります（例： `"/new volume/mount here"`）。
- (`\\servername\sharename\filepath`共有のUNCパスの文字数が256文字を超えている場合（UNCパスの先頭のは除く）、Windowsの[プロパティ]ボックスの*[セキュリティ]*タブは使用できません。

  これは、ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないでください。

共有プロパティのデフォルト値は変更できます。

- すべての共有のデフォルトの初期プロパティは `oplocks`、、 `browsable`、 `changenotify`および`show-previous-versions`です。
- 共有の作成時、共有プロパティの指定はオプションです。

ただし、共有の作成時に共有プロパティを指定した場合、デフォルト値は使用されません。共有の作成時にパラメータを使用する場合 `-share-properties`は、共有に適用するすべての共有プロパティをカンマで区切って指定する必要があります。

- ホームディレクトリ共有を指定するには、プロパティを使用し `homedirectory`ます。

  この機能を使用すると、接続するユーザと一連の変数に基づいてさまざまなディレクトリにマッピングされる共有を設定できます。ユーザごとに別個の共有を作成する必要はありません。 1 つの共有を設定し、いくつかのホームディレクトリパラメータを指定して、エントリポイント（共有）とユーザのホームディレクトリ（ SVM 上のディレクトリ）間のユーザの関係を定義します。

  ⓘ 共有の作成後にこのプロパティを追加または削除することはできません。

ホームディレクトリの共有には次の要件があります。

- SMBホームディレクトリを作成する前に、コマンドを使用して、ホームディレクトリ検索パスを少なくとも1つ追加する必要があります `vserver cifs home-directory search-path add`。
- パラメータの `-share-properties`値をに指定するホームディレクトリ共有で `homedirectory` は、（`Windows`ユーザ名）動的変数を共有名に含める必要があります `%w`。

  共有名には、さらに（ドメイン名）動的変数（など `%d/%w`）を含めることも、静的な部分（など `home1_%w`）を含めることもできます `%d`。

- 管理者またはユーザが他のユーザのホームディレクトリに接続するために共有を使用する場合（コマンドのオプションを使用）は `vserver cifs home-directory modify`、動的な共有名のパターンの先頭にチルダを付ける必要があり(`~`ます。

の詳細については `vserver cifs share`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "SMBの管理"

ONTAP SMB共有の作成

SMB サーバのデータを SMB クライアントと共有するには、 SMB 共有を作成する必要があります。共有を作成するときは、共有をホームディレクトリとして指定するなど、共有プロパティを設定できます。オプションの設定により、共有をカスタマイズすることもできます。

開始する前に

共有を作成する前に、ボリュームまたは qtree のディレクトリパスが SVM ネームスペース内に存在している必要があります。

タスクの内容

共有を作成するときのデフォルトの共有ACL（デフォルトの共有権限）はです `Everyone / Full Control`。共有へのアクセスをテストしたら、デフォルトの共有 ACL を削除し、より安全な方法で置き換える必要があります。

手順

1. 必要に応じて、共有のディレクトリパス構造を作成します。

   コマンドは `vserver cifs share create`、共有の作成時にオプションで指定されたパスをチェックし `-path`ます。指定したパスが存在しない場合、コマンドは失敗します。

2. 指定したSVMに関連付けられているSMB共有を作成します。 `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`

3. 共有が作成されたことを確認します。`vserver cifs share show -share-name share_name`

例

次のコマンドは、「SHARE1」という名前のSMB共有をSVM上に作成し `vs1.example.com`ます。ディレクトリパスはで `/users`、デフォルトのプロパティを使用して作成されます。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

ONTAP SMBクライアントアクセスの確認

共有にアクセスしてデータを書き込むことで、 SMB が正しく設定されていることを確認する必要があります。SMB サーバ名と NetBIOS エイリアスを使用してアクセスをテストします。

手順

1. Windows クライアントにログインします。
2. SMB サーバ名を使用してアクセスをテストします。

   a. エクスプローラで、次の形式で共有にドライブをマッピングします。 `\\SMB_Server_Name\Share_Name`

      正常にマッピングされない場合は、 DNS マッピングがネットワーク全体にまだ反映されていない可能性があります。しばらく待ってから、再度 SMB サーバ名を使用してアクセスをテストしてください。

      SMBサーバの名前がvs1.example.comで、共有の名前がSHARE1の場合は、次のように入力します。 `\\vs0.example.com\SHARE1`

b. 新しく作成したドライブで、テストファイルを作成して削除します。

SMB サーバ名を使用した共有への書き込みアクセスが可能であることを確認できました。

3. NetBIOS エイリアスについて手順 2 を繰り返します。

ONTAP SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List（ACL；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

開始する前に

共有へのアクセスを許可するユーザまたはグループを決めておく必要があります。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があり `Everyone / Full Control`ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. 新しいACLを設定します。

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsユーザ	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`
Windowsグループ	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com`"SVM:」上の「sales」共有の「sales Team」Windowsグループに権限を与えます `Change`。

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

次のコマンドは、SVM「vs1」上の「datavol5」共有に対する「Tiger Team」という名前のローカルWindowsグループへの権限と「See Chang」という名前のローカルWindowsユーザへの権限 `Full_Control`を付与します `Change。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

ONTAP SMB共有での**NTFS**ファイル権限の設定

共有にアクセスできるユーザまたはグループにファイルアクセスを有効にするには、その共有内のファイルおよびディレクトリに対するNTFSファイル権限をWindowsクライアントから設定する必要があります。

開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

タスクの内容

"SMBの管理"標準および詳細なNTFS権限の設定方法については、Windowsのマニュアルを参照してください。

手順

1. Windows クライアントに管理者としてログインします。
2. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
3. [ネットワークドライブの割り当て *] ボックスに入力します。

   a. ドライブ文字を選択します。

   b. [* フォルダ *] ボックスに、権限を適用するデータと共有名を含む共有を含む SMB サーバー名を入力します。

      SMBサーバ名がSMB_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します。
      `\\SMB_SERVER01\SHARE1`

      SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

   c. [完了] をクリックします。

   選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

4. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
5. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
6. [* セキュリティ *] タブを選択します。

   Security タブには、 NTFS 権限が設定されているユーザとグループのリストが表示されます。[< オブジェクト > のアクセス許可] ボックスには、選択したユーザーまたはグループの有効なアクセス許可と拒否のアクセス許可のリストが表示されます。

7. [編集（ Edit ）] をクリックします。

   [< オブジェクト > のアクセス許可] ボックスが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループに対する標準の NTFS 権限を設定します	a. [追加]*をクリックします。 [ユーザー、コンピュータ、サービスアカウント、またはグループの選択] ウィンドウが開きます。 b. [選択するオブジェクト名を入力してください *] ボックスに、 NTFS アクセス権を追加するユーザまたはグループの名前を入力します。 c. [OK]*をクリックします。
ユーザまたはグループに対する標準の NTFS 権限を変更または削除する	[* グループ名またはユーザー名 *] ボックスで、変更または削除するユーザーまたはグループを選択します。

9. 次のうち必要な操作を実行します。

状況	実行する処理
新規または既存のユーザまたはグループに対する標準の NTFS 権限を設定する	[* パーミッション for < オブジェクト >*] ボックスで、選択したユーザーまたはグループに対して許可または許可しないアクセスのタイプの [許可 *] または [拒否 *] ボックスを選択します。
ユーザまたはグループを削除します	[削除（ Remove ）] をクリックします。

標準の権限ボックスの一部またはすべてを選択できない場合、権限は親オブジェクトから継承されます。[* 特別な権限 *] ボックスは選択できません。選択されている場合は、選択したユーザまたはグループに対して詳細な権限が 1 つ以上設定されていることを意味します。

10. そのオブジェクトの NTFS アクセス権の追加、削除、または編集が完了したら、 **OK** をクリックします。

ONTAP SMBユーザ共有アクセスの確認

設定したユーザが、 SMB 共有およびその中に含まれるファイルにアクセスできることをテストする必要があります。

手順

1. Windows クライアントで、共有へのアクセスを許可したいずれかのユーザとしてログインします。
2. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
3. [ネットワークドライブの割り当て *] ボックスに入力します。

   a. ドライブ文字を選択します。

   b. [* フォルダー *] ボックスに、ユーザーに提供する共有名を入力します。

SMBサーバ名がSMB_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します。
`\\SMB_SERVER01\share1`

c. [完了] をクリックします。

選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

4. テストファイルを作成し、その存在を確認し、テキストを書き込んで、テストファイルを削除します。

CLIを使用したSMBの管理

ONTAP SMBの詳細

SMBプロトコルでは、ONTAPファイルアクセス機能を使用できます。CIFSサーバの有効化、共有の作成、およびMicrosoftサービスの有効化を行うことができます。

SMB(Server Message Block) は、 Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（ CLI ）および OnCommand 管理ツールでは、 _cifs_という メッセージが引き続き表示されます。

SMBサーバのサポート

ONTAP SMBサーバのサポートの詳細

Storage Virtual Machine（SVM）でSMBサーバを有効にして設定し、SMBクライアントがクラスタ上のファイルにアクセスできるようにすることができます。

- クラスタ内のデータSVMは、それぞれ1つのActive Directoryドメインにバインドできます。
- データSVMを同じドメインにバインドする必要はありません。
- 複数のSVMを同じドメインにバインドできます。

SMBサーバを作成する前に、データの提供に使用するSVMとLIFを設定する必要があります。データネットワークがフラットでない場合は、IPspace、ブロードキャストドメイン、およびサブネットの設定も必要になることがあります。

関連情報

"ネットワーク管理"

サーバーを変更する

"システム管理"

サポートされるONTAP SMBのバージョンと機能

Server Message Block（SMB；サーバメッセージブロック）は、Microsoft Windowsのクライアントおよびサーバで使用されるリモートファイル共有プロトコルです。すべてのSMBバージョンがサポートされます。ONTAP SMBサーバが、ご使用の環境で必要な

クライアントと機能をサポートしていることを確認する必要があります。

ONTAP がサポートする SMB クライアントおよびドメインコントローラの最新情報については、Interoperability Matrix Tool を参照してください。

SMB 2.0以降のバージョンは、ONTAP SMBサーバではデフォルトで有効になっており、必要に応じて有効または無効にすることができます。SMB 1.0は必要に応じて有効または無効にすることができます。

ドメインコントローラへのSMB 1.0および2.0接続のデフォルト設定も、ONTAPのバージョンによって異なります。の詳細については `vserver cifs security modify`、を"ONTAPコマンド リファレンス"参照してください。既存のCIFSサーバでSMB 1.0を実行している環境では、できるだけ早く新しいバージョンのSMBに移行して、セキュリティとコンプライアンスを強化する必要があります。詳細については、NetApp担当者にお問い合わせください。

次の表に、SMBの各バージョンでサポートされるSMBの機能を示します。SMBの機能には、デフォルトで有効になるものと、追加の設定が必要なものがあります。

* この機能： *	* 有効化が必要： *	* **ONTAP 9** では、以下のバージョンの **SMB** がサポートされています。 *	
		3.0	3.1.1
従来のSMB 1.0の機能		X	X
永続性ハンドル		X	X
複合操作		X	X
非同期操作		X	X
読み取り/書き込みバッファサイズの増加		X	X
拡張性の向上		X	X
SMBシヨメイ	X	X	X
代替データストリーム（ADS）ファイル形式	X	X	X
Large MTU（ONTAP 9 7以降ではデフォルトで有効）	X	X	X
oplockリース		X	X

* この機能： *	* 有効化が必要： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *	
継続的可用性を備えた共有	X	X	X
永続的ハンドル		X	X
監視		X	X
SMB 暗号化： AES-128-CCM	X	X	X
スケールアウト（CA共有で必要）		X	X
透過的なフェイルオーバー		X	X
SMBマルチチャネル（ONTAP 9 4以降）	X	X	X
事前認証の整合性			X
クラスタ・クライアント・フェイルオーバーv.2（CCFv2）			X
SMB 暗号化： AES-128-GCM	X		X

関連情報

ONTAP署名を使用してネットワークセキュリティを強化する方法について学習します

サーバーの最小認証セキュリティレベルを設定する

SMB経由のデータ転送でのSMBサーバでのSMB暗号化要求の設定

"NetAppの相互運用性"

ONTAP SMBでサポートされない**Windows**の機能

ネットワークで CIFS を使用する場合は、一部の Windows の機能が ONTAP ではサポートされないことに注意する必要があります。

ONTAP では、次の Windows 機能はサポートされません。

- Encrypted File System （ EFS ；暗号化ファイルシステム）
- 変更ジャーナルでの NT File System （ NTFS ）イベントのロギング
- Microsoft File Replication Service （ FRS ；ファイルレプリケーションサービス）
- Microsoft Windows インデックスサービス
- Hierarchical Storage Management （ HSM ；階層型ストレージ管理）経由のリモートストレージ
- Windows クライアントからのクォータ管理
- Windows のクォータのセマンティクス
- LMHOSTS ファイル
- NTFS のネイティブ圧縮機能です

ONTAP SMB SVMでの**NIS**または**LDAP**ネームサービスの設定

SMBアクセスでは、NTFSセキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIXユーザへのユーザマッピングが常に実行されます。NISまたはLDAPディレクトリストアに情報が格納されているUNIXユーザにWindowsユーザをマッピングする場合や、ネームマッピングにLDAPを使用する場合は、SMBのセットアップ時にこれらのネームサービスを設定する必要があります。

開始する前に

ネームサービスインフラに合わせてネームサービスデータベース設定をカスタマイズしておく必要があります。

タスクの内容

SVMは、ネームサービスns-switchデータベースを使用して、指定されたネームサービスデータベースを検索するソースの順序を決定します。ns-switchソースには、、 `nis`、または `ldap`を任意に組み合わせて指定できます `files`。グループデータベースの場合、ONTAPは設定されているすべてのソースからグループメンバーシップを取得しようとし、統合されたグループメンバーシップ情報をアクセスチェックに使用します。UNIXグループ情報の取得時にこれらのソースのいずれかが使用できないと、ONTAPは完全なUNIXクレデンシャルを取得できず、以降のアクセスチェックが失敗することがあります。そのため、ns-switch設定でグループデータベースのすべてのns-switchソースが設定されていることを常に確認する必要があります。

デフォルトでは、SMBサーバは、すべてのWindowsユーザをローカルデータベースに格納されているデフォルトのUNIXユーザにマッピングし`passwd`ます。デフォルトの設定を使用する場合、SMBアクセスに対するNISまたはLDAP UNIXユーザおよびグループのネームサービスまたはLDAPユーザマッピングの設定はオプションです。

手順

1. UNIXユーザ、グループ、およびネットグループ情報がNISネームサービスによって管理されている場合は、NISネームサービスを次のように設定します。

   a. コマンドを使用して、ネームサービスの現在の順番を確認します `vserver services name-service ns-switch show`。

      この例では、ネームサービスソースとして使用できる3つのデータベース(`group`、 `passwd`および`netgroup`） `nis`がソースとしてのみを使用しています `files`。

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                 Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            files
vs1             passwd         true            files
vs1             netgroup       true            files
vs1             namemap        true            files
```

ソースを `group`データベースと `passwd`データベースに追加する必要があります。必要に応じてデータベースにも `netgroup`追加できます `nis`。

b. コマンドを使用して、ネームサービスns-switchデータベースを必要な順番に調整します `vserver services name-service ns-switch modify`。

パフォーマンスを最大限に高めるには、SVMで設定する予定でないネームサービスデータベースにネームサービスを追加しないでください。

複数のネームサービスデータベースの設定を変更する場合は、変更する各ネームサービスデータベースに対して個別にコマンドを実行する必要があります。

この例では、 `nis`および `files`がデータベースおよび `passwd`のソースとしてこの順序で設定されてい `group`ます。残りのネームサービスデータベースは変更されません。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. コマンドを使用して、ネームサービスの順序が正しいことを確認し `vserver services name-service ns-switch show`ます。

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                 Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            nis,
                                                files
vs1             passwd         true            nis,
                                                files
vs1             netgroup       true            files
vs1             namemap        true            files
```

d. NISネームサービス設定を作成します。+
```
vserver services name-service nis-domain create -vserver <vserver_name>
-domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

、NIS サーバーのホスト名または IP アドレスのいずれかを指定できます。

e. NISネームサービスが適切に設定されていることを確認します。 `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. UNIXユーザ、グループ、ネットグループ情報またはネームマッピングがLDAPネームサービスによって管理されている場合は、場所にある情報を使用してLDAPネームサービスを設定します"NFSの管理"。

ONTAP SMBネームサービススイッチ設定の詳細

ONTAPでは、UNIXシステムのファイルに相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf`。このテーブルを環境に合わせて適切に設定できるように、このテーブルの機能とONTAPでの使用方法を理解しておく必要があります。

ONTAPネームサービススイッチテーブルは、ONTAPが特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順序で参照するかを決定します。ネームサービススイッチテーブルは、SVMごとにONTAPで管理されます。

データベースタイプ

このテーブルには、次のデータベースタイプごとにネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名からIPアドレスへの変換	フアイル、DNS
グループ	ユーザグループ情報の検索	フアイル、NIS、LDAP
パスワード	ユーザ情報の検索	フアイル、NIS、LDAP
ネットグループ	ネットグループ情報の検索	フアイル、NIS、LDAP

データベースタイプ	ネームサービスソースの用途	有効なソース
namemap	ユーザ名のマッピング	フアイル、LDAP

ソースタイプ

ソースによって、適切な情報の取得に使用するネームサービスソースが指定されます。

ソースタイプ	情報の検索先	使用するコマンド

ファイル	ローカルソースファイル	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	SVMのNISドメイン設定で指定された外部のNISサーバ	`vserver services name-service nis-domain`
LDAP	SVMのLDAPクライアント設定で指定された外部のLDAPサーバ	`vserver services name-service ldap`
DNS	SVMのDNS設定で指定された外部のDNSサーバ	`vserver services name-service dns`

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合でも、NISまたはLDAP認証が失敗した場合に備えて、ローカルユーザをフォールバックとして含めて設定しておく必要があります `files`。

外部ソースへのアクセスに使用するプロトコル

ONTAPでは、外部ソースのサーバにアクセスするために、次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例は、SVMのネームサービススイッチ設定を表示します `svm_1`。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

ユーザーまたはグループ情報を検索するために、ONTAPはローカルソースファイルのみを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報を検索するために、ONTAPは最初に外部NISサーバを参照します。クエリから結果が返されない場合は、次にローカルネットグループファイルがチェックされます。

SVM svm_1のテーブルには、ネームマッピング用のネームサービスエントリはありません。したがって、ONTAPはデフォルトでローカルソースファイルのみを参照します。

SMBサーバを管理します。

ONTAP SMBサーバの変更

コマンドを使用して、ワークグループからActive Directoryドメイン、ワークグループから別のワークグループ、またはActive Directoryドメインからワークグループに SMBサーバを移動できます `vserver cifs modify`。

タスクの内容

SMB サーバ名や管理ステータスなど、 SMB サーバのその他の属性を変更することもできます。の詳細については `vserver cifs modify`、を"ONTAPコマンド リファレンス"参照してください。

選択肢

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。

  a. SMBサーバの管理ステータスをに設定します `down`。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. ワークグループからActive DirectoryドメインにSMBサーバを移動します。 `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

SMBサーバ用のActive Directoryマシンアカウントを作成するには、.comドメイン内のコンテナ *example*`にコンピュータを追加するための十分なPrivilegesを備えたWindowsアカウントの名前とパスワードを指定する必要があります `ou=*example* ou。

ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ`vserver cifs`にそのURIを含め `-keytab-uri`ます。

- ワークグループから別のワークグループに SMB サーバを移動します。
  a. SMBサーバの管理ステータスをに設定します down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. SMBサーバのワークグループを変更します。 `vserver cifs modify -vserver *vserver_name* -workgroup *new_workgroup_name*`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory ドメインからワークグループに SMB サーバを移動するには、次の手順を実行します。
  a. SMBサーバの管理ステータスをに設定します down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Active Directoryドメインからワークグループに SMBサーバを移動します。 `vserver cifs modify -vserver *vserver_name* -workgroup *workgroup_name*`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> ワークグループモードに切り替えるには、継続的可用性を備えた共有、シャドウコピー、 AES など、ドメインベースの機能をすべて無効にし、該当する設定がシステムによって自動的に削除されるようにする必要があります。ただし、「 EXAMPLE.COM\userName" 」などのドメインで設定された共有 ACL は正しく機能しませんが、 ONTAP で削除することはできません。このような共有 ACL は、コマンドの完了後できるだけ早く外部ツールを使用して削除してください。AES が有効になっている場合は、「 example.com 」ドメインで AES を無効にするための十分な権限を持つ Windows アカウントの名前とパスワードの入力を求められることがあります。

  - その他の属性を変更するには、コマンドの該当するパラメータを使用し `vserver cifs modify`ます。

オプションを使用した**SMB**サーバのカスタマイズ

SMBサーバのカスタマイズ方法を検討する場合は、使用可能なオプションを把握しておくと役立ちます。一部のオプションは一般的なものですが、SMBの特定の機能を有効にして設定するためのオプションもいくつかあります。SMBサーバオプションは、オプションで制御し `vserver cifs options modify`ます。

次に、admin権限レベルで使用できるSMBサーバオプションについて説明します。

- * SMB セッションタイムアウト値の設定 *

  このオプションでは、SMBセッションが切断されるまでのアイドル時間（秒）を指定できます。アイドルセッションとは、ユーザがクライアント上でファイルやディレクトリを開いていないセッションのことです。デフォルト値は900秒です。

- * デフォルトの UNIX ユーザーの構成 *

  このオプションでは、SMBサーバで使用するデフォルトのUNIXユーザを指定できます。ONTAP はデフォルトユーザ「 pcuser 」（ UID は 65534 ）を自動的に作成し、グループ「 pcuser 」（ GID は 65534 ）を作成して、デフォルトユーザを「 pcuser 」グループに追加します。SMB サーバを作成すると、 ONTAP は自動的に「 pcuser 」をデフォルトの UNIX ユーザとして設定します。

- * ゲスト UNIX ユーザの設定 *

  このオプションでは、信頼されていないドメインからログインしたユーザをマッピングするUNIXユーザの名前を指定できます。これにより、信頼されていないドメインのユーザがSMBサーバに接続できるようになります。デフォルトでは、このオプションは設定されていません（デフォルト値はありません）。そのため、信頼されていないドメインのユーザはSMBサーバへの接続を許可されません。

- * モードビットの読み取り権限付与の実行の有効化または無効化 *

  このオプションを有効または無効にすると、UNIX実行可能ビットが設定されていない場合でも、UNIXモードビットが設定された実行可能ファイルの実行を、読み取りアクセス権を持つSMBクライアントに許可するかどうかを指定できます。このオプションは、デフォルトでは無効になっています。

- * NFS クライアントからの読み取り専用ファイルの削除機能の有効化または無効化 *

  このオプションを有効または無効にして、読み取り専用属性が設定されたファイルまたはフォルダの削除をNFSクライアントに許可するかどうかを指定します。NTFSの削除セマンティクスでは、読み取り専用属性が設定されている場合、ファイルやフォルダの削除は許可されません。UNIXの削除セマンティクスでは読み取り専用ビットが無視され、代わりに親ディレクトリの権限を使用してファイルまたはフォルダを削除できるかどうかが判断されます。デフォルトの設定はで `disabled`、NTFSの削除セマンティクスが適用されます。

- * Windows Internet Name Service サーバーアドレスの設定 *

  このオプションでは、Windows Internet Name Service（WINS）サーバアドレスのリストをカンマで区切って指定できます。IPv4アドレスを指定する必要があります。IPv6アドレスはサポートされません。デフォルト値はありません。

以下に、advanced権限レベルで使用できるSMBサーバオプションについて説明します。

- * CIFS ユーザーへの UNIX グループ権限の付与 *

  このオプションでは、ファイルの所有者ではない受信CIFSユーザにグループ権限を付与するかどうかを指定します。CIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合にこのパラメータをに設定する `true`と、ファイルに対するグループ権限が付与されます。`CIFS`ユーザが`UNIX`セキュリティ形式のファイルの所有者ではない場合に、このパラメータをに設定する `false`と、通常の`UNIX`ルールに従ってファイル権限が付与されます。このパラメータは、権限がに設定された`UNIX`セキュリティ形式のファイルに適用さ `mode bits`れます。セキュリティモードが`NTFS`または`NFSv4`のファイルには適用されません。デフォルト設定はです `false`。

- * SMB 1.0の有効化または無効化*

  ONTAP 9にSMBサーバが作成されているSVMでは、SMB 1.0はデフォルトで無効になっています。3.

  > SMB.3以降ではONTAP 9、SMB.3で作成された新しいONTAP 9サーバについてはSMB 1.0がデフォルトで無効になります。セキュリティとコンプライアンスの強化に備えて、できるだけ早く新しいバージョンのSMBに移行する必要があります。詳細については、NetApp担当者にお問い合わせください。

- * SMB 2.x の有効化または無効化 *

  SMB 2.0は、LIFフェイルオーバーをサポートするSMBの最小バージョンです。SMB 2.xを無効にすると、ONTAPはSMB 3.Xも自動的に無効にします。

  SMB 2.0はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * SMB 3.0の有効化または無効化*

  SMB 3.0は、継続的可用性を備えた共有をサポートするSMBの最小バージョンです。SMB 3.0をサポートするWindowsの最小バージョンは、Windows Server 2012およびWindows 8です。

  SMB 3.0はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * SMB 3.1の有効化または無効化*

  Windows 10は、SMB 3.1をサポートする唯一のWindowsバージョンです。

  SMB 3.1はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * ODX コピーオフロードの有効化または無効化 *

  ODXコピーオフロードは、対応するWindowsクライアントで自動的に使用されます。このオプションはデフォルトで有効になっています。

- * ODX コピーオフロードの直接コピーメカニズムの有効化または無効化 *

  直接コピーメカニズムを使用すると、Windowsクライアントがコピーの実行中にファイルが変更されないモードでコピーのソースファイルを開こうとすると、コピーオフロード処理のパフォーマンスが向上します。デフォルトでは、直接コピーメカニズムが有効になっています。

- * 自動ノードリファーラルの有効化または無効化 *

  自動ノードリファーラルでは、SMBサーバはクライアントに対して、要求した共有を介してアクセスするデータのホストノードに対してローカルなデータLIFを自動的に参照することになります。

- * SMB * のエクスポート・ポリシーの有効化または無効化

  このオプションは、デフォルトでは無効になっています。

- * ジャンクションポイントのリパースポイントとしての使用の有効化または無効化 *

  このオプションを有効にすると、SMBサーバはジャンクションポイントをリパースポイントとしてSMBクライアントに公開します。このオプションは、SMB 2.x接続またはSMB 3.0接続でのみ有効です。このオプションはデフォルトで有効になっています。

  このオプションはSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * TCP 接続ごとの最大同時操作数の設定 *

  デフォルト値は255です。

- * ローカルの Windows ユーザーとグループ機能の有効化または無効化 *

  このオプションはデフォルトで有効になっています。

- * ローカル Windows ユーザー認証の有効化または無効化 *

  このオプションはデフォルトで有効になっています。

- * VSS シャドウ・コピー機能の有効化または無効化 *

  ONTAPでは、シャドウコピー機能を使用して、Hyper-V over SMBソリューションを使用して格納されたデータのリモートバックアップを実行します。

  このオプションは、SVM、およびHyper-V over SMB構成でのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * シャドウ・コピーのディレクトリ階層の設定 *

  このオプションを設定すると、シャドウコピー機能を使用する場合に、シャドウコピーを作成するディレクトリの最大階層を定義できます。

  このオプションは、SVM、およびHyper-V over SMB構成でのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * マルチドメインネームマッピングの検索機能の有効化または無効化 *

  有効にすると、 UNIX ユーザが Windows ユーザ名のドメイン部分にワイルドカード（ * ）を使用して Windows ドメインユーザにマッピングされている場合に（ * \joe など）、 ONTAP はホームドメインと双方向の信頼関係が確立されたすべてのドメインで、指定したユーザを検索します。ホームドメインは、SMBサーバのコンピュータアカウントが含まれているドメインです。

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。このオプションを有効にして優先リストを設定すると、その優先リストを使用してマルチドメインネームマッピングの検索が実行されます。

デフォルトでは、マルチドメインネームマッピングの検索は有効になります。

- * ファイルシステムセクターサイズの設定 *

  このオプションでは、ONTAPがSMBクライアントに報告するファイルシステムセクターサイズをバイト単位で設定できます。このオプションには、との `512`2つの有効な値があります `4096`。デフォルト値はです `4096`。Windowsアプリケーションが512バイトのセクターサイズのみをサポートしている場合は、この値をに設定する必要が `512`あります。

- * ダイナミックアクセス制御の有効化または無効化 *

  このオプションを有効にすると、監査を使用した集約型アクセスポリシーのステージングや、グループポリシーオブジェクトを使用した集約型アクセスポリシーの実装など、ダイナミックアクセス制御（DAC）を使用してSMBサーバ上のオブジェクトを保護できます。このオプションは、デフォルトでは無効になっています。

  このオプションはSVMでのみサポートされます。

- * 認証されていないセッションのアクセス制限の設定（ restrict anonymous ） *

  このオプションを設定すると、認証されていないセッションのアクセス制限を指定できます。制限は匿名ユーザに適用されます。デフォルトでは、匿名ユーザに対するアクセス制限はありません。

- * UNIX 対応のセキュリティを使用するボリューム（ UNIX セキュリティ形式のボリューム、または UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）での NTFS ACL の提供を有効または無効にする *

  このオプションを有効または無効にして、UNIXセキュリティ形式のファイルやフォルダのファイルセキュリティをSMBクライアントに提供する方法を指定します。有効にすると、ONTAP UNIXセキュリティ形式のボリューム内のファイルやフォルダが、NTFS ACLを使用するNTFSファイルセキュリティが設定されたファイルやフォルダとしてSMBクライアントに提供されます。無効にするとONTAP、UNIXセキュリティ形式のボリュームは、ファイルセキュリティのないFATボリュームとして表示されます。デフォルトでは、ボリュームはNTFS ACLを使用するNTFSファイルセキュリティが設定されたボリュームとして表示されます。

- * SMB 擬似オープン機能の有効化または無効化 *

  この機能を有効にすると、ONTAPがファイルやディレクトリの属性情報を照会する際のオープン要求とクローズ要求の方法が最適化され、SMB 2.xおよびSMB 3.0のパフォーマンスが向上します。デフォルトでは、SMB擬似オープン機能は有効になっています。このオプションは、SMB 2.x以降を使用する接続にのみ役立ちます。

- * UNIX 拡張の有効化または無効化 *

  このオプションを有効にすると、SMBサーバでUNIX拡張が有効になります。UNIX拡張を使用すると、SMBプロトコルを介してPOSIX/UNIX形式のセキュリティを表示できます。デフォルトでは、このオプションは無効になっています。

  Mac OSXクライアントなどのUNIXベースのSMBクライアントが環境内にある場合は、UNIX拡張を有効にする必要があります。UNIX拡張を有効にすると、SMBサーバはPOSIX/UNIXセキュリティ情報をSMB経

由でUNIXベースのクライアントに送信できるようになります。クライアントは、受け取ったセキュリティ情報をPOSIX/UNIXセキュリティに変換します。

- * 略称を使用した検索のサポートの有効化または無効化 *

  このオプションを有効にすると、SMBサーバは短縮名に対して検索を実行できます。このオプションを有効にした検索クエリでは、8.3形式のファイル名と長いファイル名が照合されます。このパラメータのデフォルト値はです `false`。

- * DFS 対応の自動通知のサポートの有効化または無効化 *

  このオプションを有効または無効にして、共有に接続するSMB 2.xおよびSMB 3.0クライアントにSMBサーバからDFS対応を自動的に通知するかどうかを指定します。ONTAPは、SMBアクセス用のシンボリックリンクの実装でDFSリファーラルを使用します。有効にすると、シンボリックリンクアクセスが有効かどうかに関係なく、SMBサーバは常にDFS対応を通知します。無効にすると、シンボリックリンクアクセスが有効になっている共有にクライアントが接続する場合にのみ、SMBサーバはDFS対応を通知します。

- * SMB クレジットの最大数の設定 *

  ONTAP 9 .4以降では、クライアントとサーバがSMBバージョン2以降を実行している場合に、オプションを設定して `-max-credits`SMB接続に付与するクレジット数を制限できます。デフォルト値は128です。

- * SMB マルチチャネルのサポートの有効化または無効化 *

  ONTAP 9 .4以降のリリースでこのオプションを有効にする `-is-multichannel-enabled`と、クラスタとそのクライアントに適切なNICが導入されている場合に、SMBサーバは単一のSMBセッションに対して複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。このパラメータのデフォルト値はです `false`。

  SMBマルチチャネルが有効な場合は、次のパラメータも指定できます。

  - マルチチャネルセッションごとに許可される最大接続数。このパラメータのデフォルト値は32です。
  - マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。このパラメータのデフォルト値は256です。

ONTAP SMBサーバオプションの設定

SMBサーバオプションは、Storage Virtual Machine（SVM）でのSMBサーバの作成後にいつでも設定できます。

ステップ

1. 必要な操作を実行します。

SMBサーバオプションの設定	入力するコマンド
admin権限レベルで設定	`vserver cifs options modify -vserver` *`vserver_name options`*

SMBサーバオプションの設定	入力するコマンド
advanced権限レベルで設定	a. `set -privilege advanced` b. `vserver cifs options modify -vserver vserver_name options` c. `set -privilege admin`

SMBサーバオプションの詳細および設定については `vserver cifs options modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBユーザへのUNIXグループ権限付与の設定

このオプションを設定すると、受信SMBユーザがファイルの所有者でない場合でも、ファイルまたはディレクトリにアクセスするグループ権限を付与できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. UNIXグループ権限付与を必要に応じて設定します。

状況	入力するコマンド
ユーザがファイルの所有者でない場合にもファイルやディレクトリにアクセスするためのグループ権限を付与する	`vserver cifs options modify -grant-unix-group-perms-to-others true`
ユーザがファイルの所有者でない場合でも、ファイルまたはディレクトリへのアクセスを無効にしてグループ権限を取得する	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. admin権限レベルに戻ります。 `set -privilege admin`

匿名ユーザに対するONTAP SMBアクセス制限の設定

デフォルトでは、認証されていない匿名ユーザ（ _null ユーザ）はネットワーク上の特定の情報にアクセスできます。SMBサーバオプションを使用して、匿名ユーザに対するアクセス制限を設定できます。

タスクの内容

`-restrict-anonymous`SMBサーバオプションは、Windowsのレジストリエントリに対応し`RestrictAnonymous`ます。

匿名ユーザは、ユーザ名と詳細、アカウントポリシー、共有名など、ネットワーク上のWindowsホストから特

定のタイプのシステム情報をリストまたは列挙できます。匿名ユーザのアクセスを制御するには、次の3つのアクセス制限設定のいずれかを指定します。

値	説明
`no-restriction` （デフォルト）	匿名ユーザに対するアクセス制限を指定しません。
`no-enumeration`	匿名ユーザに対して列挙だけを制限します。
`no-access`	匿名ユーザに対してアクセスを制限します。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. restrict anonymousを設定します。 `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver` *`vserver_name`*
4. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

利用可能なサーバーオプション

UNIXセキュリティ形式のデータに対するファイルセキュリティの**SMB**クライアントへの提供方法を管理します。

UNIXセキュリティ形式のデータに対する**SMB**クライアントへの**ONTAP**ファイルセキュリティの提供について

SMBクライアントへのNTFS ACLの提供を有効または無効にすることで、UNIXセキュリティ形式のデータに関するファイルセキュリティをSMBクライアントに提供する方法を選択できます。それぞれの設定には利点があり、ビジネス要件に最適な設定を選択するために理解しておく必要があります。

デフォルトでは、ONTAPはUNIXセキュリティ形式のボリュームに対するUNIXアクセス権をNTFS ACLとしてSMBクライアントに提供します。これは次のような場合に適しています。

- Windows の [プロパティ] ボックスの [セキュリティ *] タブを使用して、 UNIX アクセス権を表示および編集する。

  処理がUNIXシステムで許可されていない場合、Windowsクライアントから権限を変更することはできません。たとえば、所有していないファイルの所有権は変更できません。これは、UNIXシステムではこの処理が許可されていないためです。この制限により、SMBクライアントはファイルやフォルダに対して設定されたUNIXアクセス権をバイパスできないようになっています。

- UNIXセキュリティ形式のボリューム上のファイルの編集や保存に特定のWindowsアプリケーション（Microsoft Officeなど）を使用しており、ONTAPでの保存時にUNIXアクセス権を維持する必要がある場合。
- 使用するファイルのNTFS ACLを読み取ることを想定した特定のWindowsアプリケーションが環境内にあります。

状況によっては、NTFS ACLとしてのUNIXアクセス権の提供を無効にすることができます。この機能を無効にすると、ONTAPはUNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供します。UNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供する理由はいくつかあります。

- UNIXアクセス権を変更するには、UNIXクライアントでマウントを使用する必要があります。

  UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合は、[セキュリティ]タブは使用できません。マッピングされたドライブは、ファイル権限がないFATファイルシステムでフォーマットされているように見えます。

- SMBを介したアプリケーションを使用している場合、アクセスするファイルやフォルダにNTFS ACLを設定していますが、データがUNIXセキュリティ形式のボリューム上にあると失敗する可能性があります。

  ONTAPでボリュームがFATと報告された場合、アプリケーションはACLの変更を試行しません。

関連情報

- FlexVolボリュームのセキュリティスタイルを設定する
- qtreeでのセキュリティ形式の設定

UNIXセキュリティ形式のデータに対する**ONTAP SMB**クライアントへの**NTFS ACL**の提供の設定

UNIX セキュリティ形式のデータ（ UNIX セキュリティ形式のボリュームと UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）に対する NTFS ACL の SMB クライアントへの提供を有効または無効にできます。

タスクの内容

このオプションを有効にすると、 ONTAP は、 UNIX 対応のセキュリティ形式を使用するボリュームのファイルおよびフォルダを NTFS ACL を使用するように SMB クライアントに提供します。このオプションを無効にした場合は、ボリュームが SMB クライアントに FAT ボリュームとして提供されます。デフォルトでは、 NTFS ACL が SMB クライアントに提供されます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. UNIX NTFS ACLオプションを設定します。 `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
4. admin権限レベルに戻ります。 `set -privilege admin`

ONTAP SMB FlexVolボリュームの**UNIX**アクセス権の保持に関する詳細

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリテ

ィプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

ONTAP SMBサーバ用のWindowsの[セキュリティ]タブを使用したUNIX権限の管理について

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 Windows クライアントのセキュリティタブを使用できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

  モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

SMBサーバのセキュリティ設定を管理します。

ONTAP SMBクライアント認証の処理について

SMB接続を確立してSVMに格納されているデータにアクセスする前に、ユーザはSMBサーバが属しているドメインで認証される必要があります。SMBサーバでは、KerberosとNTLM（NTLMv1またはNTLMv2）の2つの認証方式がサポートされます。Kerberosは、ドメインユーザの認証に使用されるデフォルトの方法です。

Kerberos認証

ONTAPは、認証されたSMBセッションの作成時にKerberos認証をサポートします。

KerberosはActive Directoryのプライマリ認証サービスです。KerberosサーバまたはKerberos Key Distribution Center（KDC；キー配布センター）サービスは、Active Directoryのセキュリティ原則に関する情報を格納および取得します。NTLMモデルとは異なり、SMBサーバなどの別のコンピュータとのセッションを確立するActive Directoryクライアントは、KDCに直接接続してセッションクレデンシャルを取得します。

NTLM認証

NTLMクライアント認証は、パスワードに基づくユーザ固有のシークレットの共有情報に基づくチャレンジ応答プロトコルを使用して行われます。

ユーザがローカルのWindowsユーザアカウントを使用してSMB接続を作成した場合、認証はSMBサーバによってNTLMv2を使用してローカルに行われます。

ONTAP SVMディザスタリカバリ設定の**SMB**サーバセキュリティ設定の詳細

IDが保持されないディザスタリカバリデスティネーションとして設定されているSVMを作成する前に（ `-identity-preserve`SnapMirror構成でオプションがに設定されている `false`）、デスティネーションSVMでのSMBサーバセキュリティ設定の管理方法を確認しておく必要があります。

- デフォルト以外の SMB サーバセキュリティ設定はデスティネーションにレプリケートされません。

  デスティネーション SVM 上に SMB サーバを作成した場合、すべての SMB サーバセキュリティ設定はデフォルト値に設定されます。SVM のディザスタリカバリ先を初期化、更新、再同期した場合、ソース上の SMB サーバのセキュリティ設定はデスティネーションにレプリケートされません。

- デフォルト以外の SMB サーバセキュリティ設定は手動で設定する必要があります。

  ソース SVM 上で SMB サーバセキュリティ設定をデフォルト以外にしている場合、デスティネーションが読み書き可能になったあと（ SnapMirror 関係が解除されたあと）にデスティネーション SVM 上で手動で同じ設定を行う必要があります。

ONTAP SMBサーバのセキュリティ設定に関する情報を表示する

Storage Virtual Machine（SVM）上のSMBサーバセキュリティ設定に関する情報を表示できます。この情報を使用して、セキュリティ設定が正しいことを確認できます。

タスクの内容

表示されるセキュリティ設定は、そのオブジェクトのデフォルト値、またはONTAP CLIまたはActive Directoryグループポリシーオブジェクト（GPO）を使用して設定されたデフォルト以外の値です。

一部のオプションが無効なため、ワークグループモードのSMBサーバに対してはコマンドを使用しない `vserver cifs security show`でください。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定したSVMのすべてのセキュリティ設定	`vserver cifs security show -vserver` *vserver_name*
SVMの特定のセキュリティ設定	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]`と入力して、使用できるフィールドを指定できます `-fields ?`。

例

次の例は、SVM vs1のすべてのセキュリティ設定を表示します。

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                           Kerberos Clock Skew:        5 minutes
                           Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:         7 days
                         Kerberos KDC Timeout:         3 seconds
                           Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:        false
                         LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
               SMB1 Enabled for DC Connections:        false
               SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:         false
 AES session key enabled for NetLogon channel:         false
  Try Channel Binding For AD LDAP Connections:         false
```

表示される設定は、実行中のONTAPのバージョンによって異なります。

次の例は、SVM vs1のKerberosのクロックスキューを表示します。

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

関連情報

GPO構成に関する情報を表示する

ローカル**SMB**ユーザに対する**ONTAP**パスワードの複雑さの設定

パスワードの複雑さの要件を使用すると、Storage Virtual Machine（SVM）上のローカルSMBユーザに対するセキュリティを強化できます。パスワードの複雑さの要件はデフォルトでは有効になっています。この機能は、いつでも無効にして再度有効にすることができます。

開始する前に

CIFSサーバでローカルユーザ、ローカルグループ、およびローカルユーザ認証が有効になっている必要があります。

タスクの内容

一部のオプションが無効なため、ワークグループモードのCIFSサーバに対してはコマンドを使用しない `vserver cifs security modify`でください。

手順

1. 次のいずれかを実行します。

ローカル**SMB**ユーザに対するパスワードの複雑さの要件の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
無効にする	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. パスワードの複雑さの要件に関するセキュリティ設定を確認します。 `vserver cifs security show -vserver` *`vserver_name`*

例

次の例では、SVM vs1のローカルSMBユーザに対してパスワードの複雑さの要件を有効にしています。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

関連情報

- サーバーのセキュリティ設定に関する情報を表示する
- ローカルユーザーとグループについて学ぶ
- ローカルユーザのパスワードの要件
- ローカルユーザアカウントのパスワードの変更

ONTAP SMBサーバの**Kerberos**セキュリティ設定を変更する

許可されるKerberosクロックスキューの最大時間、Kerberosチケットの有効期間、チケットを更新する最大日数など、CIFSサーバのKerberosセキュリティ設定を変更できます。

タスクの内容

コマンドによるCIFSサーバのKerberos設定の変更では `vserver cifs security modify`、パラメータで指定した単一のStorage Virtual Machine（SVM）の設定のみを変更 `-vserver`できます。Active Directoryのグループポリシーオブジェクト（GPO）を使用すると、同じActive Directoryドメインに属するクラスタ上のすべてのSVMのKerberosセキュリティ設定を一元管理できます。

手順

1. 次の操作を1つ以上実行します。

状況	入力するコマンド
Kerberosクロックスキューの許容最大時間を分（9.13.1以降）または秒（9.12.1以前）で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* デフォルト設定は5分です。
Kerberosチケットの有効期間を時間単位で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` デフォルト設定は10時間です。

チケットの最大更新日数を指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* デフォルトの設定は7日です。
KDC上のソケットのタイムアウトを指定します。このタイムアウトを過ぎると、すべてのKDCが到達不能としてマークされます。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* デフォルト設定は3秒です。

2. Kerberosセキュリティ設定を確認します。

   `vserver cifs security show -vserver` *`vserver_name`*

例

次の例では、 SVM vs1 の Kerberos セキュリティ設定を「 Kerberos Clock Skew 」に 3 分、「 Kerberos Ticket Age 」に 8 時間に変更しています。

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                     Kerberos Clock Skew:                    3 minutes
                     Kerberos Ticket Age:                    8 hours
                   Kerberos Renewal Age:                     7 days
                   Kerberos KDC Timeout:                     3 seconds
                     Is Signing Required:                 false
          Is Password Complexity Required:                  true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

関連情報

"サーバーのセキュリティ設定に関する情報を表示する"

"サポートされるGPO"

"CIFSサーバへのグループ ポリシー オブジェクトの適用"

SMB サーバの *LMCompatibilityLevel* とも呼ばれる SMB サーバの最小セキュリティレベルを設定することで、 SMB クライアントアクセスのビジネスセキュリティ要件を満たすことができます。最小セキュリティレベルは、SMBサーバによって許可されるSMBクライアントからのセキュリティトークンの最小レベルです。

タスクの内容

- ワークグループモードのSMBサーバでは、NTLM認証のみがサポートされます。Kerberos認証はサポートされていません。
- LMCompatibilityLevelはSMBクライアント認証にのみ適用され、管理者認証には適用されません。

最低限の認証セキュリティレベルは、サポートされている4つのセキュリティレベルのいずれかに設定できます。

値	説明
`lm-ntlm-ntlmv2-krb` （デフォルト）	Storage Virtual Machine（SVM）は、LM、NTLM、NTLMv2、Kerberos認証セキュリティを許可します。
`ntlm-ntlmv2-krb`	SVMは、NTLM、NTLMv2、Kerberos認証セキュリティを許可します。SVMはLM認証を拒否します。
`ntlmv2-krb`	SVMは、NTLMv2とKerberos認証セキュリティを許可します。SVMはLMとNTLM認証を拒否します。
`krb`	SVMは、Kerberos認証セキュリティのみを許可します。SVMはLM、NTLM、NTLMv2認証を拒否します。

手順

1. 最小認証セキュリティレベルを設定します。 `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 認証セキュリティレベルが目的のレベルに設定されていることを確認します。 `vserver cifs security show -vserver` *`vserver_name`*

関連情報

Kerberosベースの通信用にAES暗号化を構成する

Kerberosベースの通信による最大限のセキュリティを確保するには、SMBサーバでAES-256暗号化とAES-128暗号化を有効にします。デフォルトでは、SVMでのSMBサーバの作成時にAdvanced Encryption Standard（AES）暗号化は無効になっています。AES暗

号化が提供する強固なセキュリティを活用するには、AES暗号化を有効にする必要があります。

SMBのKerberos関連の通信は、SVMでSMBサーバを作成する際や、SMBセッションのセットアップフェーズで使用されます。SMBサーバでは、Kerberos通信で次の暗号化タイプがサポートされます。

- AES 256
- AES 128
- デス
- RC4-HMAC

Kerberos通信で最高のセキュリティを持つ暗号化タイプを使用する場合は、SVMのKerberos通信でAES暗号化を有効にする必要があります。

SMBサーバを作成すると、ドメインコントローラによってActive Directoryにコンピュータマシンアカウントが作成されます。この時点で、KDCは特定のマシンアカウントの暗号化機能を認識します。その後、認証時にクライアントがサーバに提示するサービスチケットを暗号化するために、特定の暗号化タイプが選択されます。

ONTAP 9.12.1 以降では、Active Directory (AD) KDC にアドバタイズする暗号化タイプを指定できます。オプションを使用すると `-advertised-enc-types`、推奨される暗号化タイプを有効にしたり、弱い暗号化タイプを無効にしたりできます。方法をご確認ください"Kerberosベースの通信用にAES暗号化を構成する"。

> SMB 3.0で使用できるIntel AES New Instructions（Intel AES NI）は、AESアルゴリズムを強化し、サポートされているプロセッサファミリーでのデータ暗号化を高速化します。SMB 3.1.1以降では、SMB暗号化で使用されるハッシュアルゴリズムとしてAES-128-CCMに代わってAES-128-GCMが使用されます。

関連情報

サーバーのセキュリティ設定を変更する

ONTAP SMB Kerberosベースの通信用の**AES**暗号化の設定

Kerberosベースの通信で最も強力なセキュリティを活用するには、SMBサーバでAES-256暗号化とAES-128暗号化を使用する必要があります。ONTAP 9.13.1以降では、AES暗号化がデフォルトで有効になります。SMBサーバでActive Directory（AD）KDCとのKerberosベースの通信にAES暗号化タイプを選択したくない場合は、AES暗号化を無効にすることができます。

AES暗号化がデフォルトで有効になっているかどうかと、暗号化タイプを指定できるかどうかは、ONTAPのバージョンによって異なります。

ONTAPのバージョン	**AES**暗号化が有効になっている...	暗号化タイプを指定できますか。
9.13.1以降	デフォルト	○
9.12.1	シユトウ	○
9.11.1以前	シユトウ	いいえ

ONTAP 9 .12.1以降では、AES暗号化はオプションを使用して有効または無効にでき `-advertised-enc`

-types`ます。このオプションを使用すると、AD KDCにアドバタイズされる暗号化タイプを指定できます。デフォルトの設定はと `des`です `rc4`が、AESタイプを指定するとAES暗号化が有効になります。オプションを使用して、弱いRC4およびDES暗号化タイプを明示的に無効にすることもできます。AES.11.1以前でONTAP 9は、オプションを使用してAES暗号化を有効または無効にする必要があります `-is-aes-encryption-enabled。暗号化タイプを指定することはできません。

セキュリティを強化するために、Storage Virtual Machine（SVM）はAESセキュリティオプションが変更されるたびにAD内のマシンアカウントのパスワードを変更します。パスワードを変更するには、マシンアカウントを含む組織単位（OU）の管理ADクレデンシャルが必要になる場合があります。

IDが保持されないディザスタリカバリデスティネーションとしてSVMが設定されている場合（SnapMirrorの設定でオプションがに設定されている false`場合 `-identity-preserve）、デフォルト以外のSMBサーバセキュリティ設定はデスティネーションにレプリケートされません。ソースSVMでAES暗号化を有効にした場合は、AES暗号化を手動で有効にする必要があります。

例 **13.** 手順

ONTAP 9.12.1以降

1. 次のいずれかを実行します。

Kerberos 通信の **AES** 暗号化タイプの設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
無効にする	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

*注:*この `-is-aes-encryption-enabled`オプションはONTAP 9 12.1では廃止されており、今後のリリースで削除される可能性があります。

2. AES暗号化が必要に応じて有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMBサーバが所属するOUの管理ADクレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信の **AES** 暗号化タイプの設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
無効にする	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. AES暗号化が必要に応じて有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   `is-aes-encryption-enabled`フィールドには、AES暗号化が有効になっているかどうかと `false`無効になっているかが表示されます `true`。

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMBサーバが所属するOUの管理ADクレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

関連情報

"ドメインユーザがDomain-Tunnelを使用するクラスタにログインできない"

SMB署名を使用したネットワークセキュリティの強化

ONTAP SMB署名を使用したネットワークセキュリティの強化について

SMB署名は、リプレイアタックを防止することで、SMBサーバとクライアント間のネットワークトラフィックが危険にさらされないようにします。デフォルトでは、ONTAPはクライアントから要求されたときにSMB署名をサポートします。ストレージ管理者は、必要に応じて、 SMB 署名を必須にするように SMB サーバを設定できます。

CIFS サーバの SMB 署名セキュリティ設定に加えて、クライアントと CIFS サーバ間の通信のデジタル署名を制御する Windows クライアント上の SMB 署名ポリシーが 2 つあります。ビジネス要件に合わせて設定を行うことができます。

クライアント SMB ポリシーは、 Microsoft 管理コンソール（ MMC ）または Active Directory の GPO を使用して設定した Windows ローカルセキュリティポリシー設定で制御されます。クライアントの SMB 署名とセキュリティ問題の詳細については、 Microsoft Windows のマニュアルを参照してください。

ここでは、 Microsoft クライアントの 2 つの SMB 署名ポリシーについて説明します。

- `Microsoft network client: Digitally sign communications (if server agrees)`

  この設定は、クライアントのSMB署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定がクライアントで無効になっている場合、クライアントのCIFSサーバとの通信は、CIFSサーバのSMB署名の設定によって異なります。

- `Microsoft network client: Digitally sign communications (always)`

  この設定は、クライアントがサーバとの通信に SMB 署名を必要とするかどうかを制御します。デフォルトでは無効になっています。この設定がクライアントで無効になっている場合、SMB署名の動作は、のポリシー設定とCIFSサーバの設定に基づき `Microsoft network client: Digitally sign communications (if server agrees)`ます。

ご使用の環境に、 SMB 署名を必要とするように設定された Windows クライアントが含まれる場合、 CIFS サーバ上の SMB 署名を有効にする必要があります。有効にしないと、 CIFS サーバはこれらのシステムにデータを提供できません。

クライアントとCIFSサーバのSMB署名設定の有効な結果は、SMBセッションでSMB 1.0が使用されるかSMB 2.x以降が使用されるかによって異なります。

次の表に、セッションでSMB 1.0が使用される場合の有効なSMB署名の動作を示します。

クライアント	**ONTAP —** 署名は不要	**ONTAP —** 署名が必要
署名は無効になっており、不要です	署名されません	署名済み
署名が有効になっており、不要である	署名されません	署名済み
署名が無効になっており、必要です	署名済み	署名済み
署名が有効になっており、必要です	署名済み	署名済み

古いバージョンのWindowsのSMB 1クライアントや一部のWindows以外のSMB 1クライアントでは、署名がクライアントでは無効になっていてCIFSサーバでは必要な場合、接続に失敗することがあります。

次の表に、セッションでSMB 2.xまたはSMB 3.0が使用される場合の有効なSMB署名の動作を示します。

SMB 2.x クライアントと SMB 3.0 クライアントでは、 SMB 署名は常に有効になります。無効にすることはできません。

クライアント	**ONTAP —** 署名は不要	**ONTAP —** 署名が必要
署名は不要です	署名されません	署名済み
署名が必要です	署名済み	署名済み

次の表に、 Microsoft クライアントおよびサーバの SMB 署名のデフォルト動作を示します。

プロトコル	ハッシュアルゴリズム	有効 / 無効を切り替えられます	必須 / 不要	クライアントのデフォルト	サーバのデフォルト	**DC** のデフォルト
SMB 1.0	MD5	○	○	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	○	不要	不要	必須
SMB 3.0	AES-CMAC ：	いいえ	○	不要	不要	必須

Microsoftでは、または `Digitally sign communications (if server agrees)`グループポリシー設定の使用を推奨していません `Digitally sign communications (if client agrees)`。Microsoftでは、レジストリ設定の使用も推奨していません `EnableSecuritySignature`。これらのオプションはSMB 1の動作にのみ影響し、グループポリシー設定または `RequireSecuritySignature`レジストリ設定に置き換えることができます。`Digitally sign communications (always)`詳細については、Microsoftのブログを参照してください。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The SMB署名の基礎（SMB1とSMB2の両方をカバー）]

ONTAP SMB署名のパフォーマンスへの影響

SMBセッションでSMB署名を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行しているクラスタノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワークトラフィックの量に変化はありませんが、クライアントとサーバの両方でCPU使用率が増加したことを示しています。

パフォーマンスへの影響の程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9 .7以

降では、新しい暗号化オフロードアルゴリズムによって署名済みSMBトラフィックのパフォーマンスを向上させることができます。SMB署名オフロードは、SMB署名が有効になっている場合はデフォルトで有効になります。

SMB署名のパフォーマンス向上には、AES-NIオフロード機能が必要です。お使いのプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証できます。

ほとんどのWindowsクライアントは、サーバでSMB署名が有効になっている場合、SMB署名をデフォルトでネゴシエートします。一部のWindowsクライアントでSMB保護が必要な場合や、SMB署名がパフォーマンスの問題を引き起こしている場合は、リプレイアタックに対する保護を必要としないWindowsクライアントでSMB署名を無効にすることができます。WindowsクライアントでのSMB署名の無効化については、Microsoft Windowsのマニュアルを参照してください。

ONTAPの**SMB**署名の設定に関する推奨事項

SMBクライアントとCIFSサーバの間のSMB署名の動作は、セキュリティ要件に応じて設定できます。CIFSサーバでSMB署名を設定する際に選択する設定は、セキュリティ要件によって異なります。

SMB署名はクライアントとCIFSサーバのどちらでも設定できます。SMB署名を設定する際は、次の推奨事項を考慮してください。

状況	推奨事項
クライアントとサーバ間の通信のセキュリティを強化する	クライアントのセキュリティ設定を有効にして、クライアントでSMB署名を必須にします `Require Option (Sign always)`。
特定のStorage Virtual Machine（SVM）へのすべてのSMBトラフィックに署名する	セキュリティ設定でSMB署名を必須にするように設定して、CIFSサーバでSMB署名を必須にします。

Windowsクライアントのセキュリティ設定の詳細については、Microsoftのドキュメントを参照してください。

複数のデータ**LIF**の**ONTAP SMB**署名の設定について

SMB サーバで SMB 署名要求を有効または無効にするときは、 SVM に複数のデータ LIF が設定されている場合のガイドラインに注意する必要があります。

SMB サーバを設定する際に、複数のデータ LIF が設定されていることがあります。その場合、DNSサーバにはCIFSサーバのレコードエントリが複数含まれ `A`、SMBサーバホスト名はすべて同じですが、IPアドレスはそれぞれ一意です。たとえば、2つのデータLIFが設定されているSMBサーバには、次のDNSレコードエントリがあり `A`ます。

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

通常の動作では、 SMB 署名要求の設定を変更すると、クライアントからの新しい接続だけが SMB 署名の設定変更の影響を受けます。ただし、この動作には例外があります。クライアントに共有への既存の接続がある場合、設定の変更後、クライアントは元の接続を維持しながら同じ共有への新しい接続を作成します。この場合、新規と既存の SMB 接続の両方で新しい SMB 署名の要件が適用されます。

次の例を考えてみましょう。

1. client1は、パスを使用してSMB署名を必要とせずに共有に接続します `O:\`。
2. ストレージ管理者が、 SMB 署名を要求するように SMB サーバの設定を変更したとします。
3. Client1は、パスを使用して（パスを使用した接続は維持したまま `O:\`）、SMB署名を使用して同じ共有に接続します `S:\`。
4. その結果、ドライブと `S:\`ドライブの両方でデータにアクセスするときにSMB署名が使用され `O:\`ます。

受信**SMB**トラフィックの**ONTAP**署名の設定

SMBメッセージへのクライアントによる署名を強制するには、SMB署名要求を有効にします。有効にすると、ONTAPは有効な署名のあるSMBメッセージのみを受け入れます。SMB署名を許可するが要求しない場合は、SMB署名要求を無効にすることができます。

タスクの内容

デフォルトでは、SMB署名要求は無効になっています。SMB署名要求はいつでも有効または無効にできます。

次の状況では、SMB署名はデフォルトで無効になりません。

1. SMB署名要求が有効になっており、クラスタがSMB署名をサポートしていないバージョンのONTAPにリバートされた。
2. その後、クラスタがSMB署名をサポートするバージョンのONTAPにアップグレードされた。

   この場合、サポートされているバージョンのONTAPで最初に設定されたSMB署名の設定は、リバートとその後のアップグレードを通じて保持されます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップする際にコマンドのオプション `snapmirror create`で選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

このオプションを（ID保持）に `true`設定する `-identity-preserve`と、SMB署名のセキュリティ設定がデスティネーションにレプリケートされます。

このオプションを（非ID保持）に `false`設定する `-identity-preserve`と、SMB署名のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションのCIFSサーバセキュリティ設定

はデフォルト値に設定されます。ソースSVMでSMB署名要求を有効にした場合は、デスティネーションSVMでSMB署名要求を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

SMB 署名要求の設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -is-signing-required true`
無効にする	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

2. 次のコマンドの出力で、フィールドの値が目的の値に設定されているかどうかを判断して、SMB署名要求が有効または無効になっていることを確認し `Is Signing Required`ます。 `vserver cifs security show -vserver vserver_name -fields is-signing-required`

例

次の例では、SVM vs1でSMB署名要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

関連情報

- "スナップミラー作成"

ONTAP SMBセッションが署名されているかどうかの確認

CIFSサーバで接続されているSMBセッションに関する情報を表示できます。この情報を使用して、SMBセッションが署名されているかどうかを確認できます。これは、必要なセキュリティ設定を使用してSMBクライアントセッションが接続されているかどうかを確認する場合に役立ちます。

手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定したStorage Virtual Machine（SVM）上の署名されたすべてのセッション	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
SVM上の特定のSession IDを使用する署名されたセッションの詳細	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

例

次のコマンドを実行すると、SVM vs1上の署名されたセッションに関するセッション情報が表示されます。デフォルトのサマリー出力には ' Is Session Signed 出力フィールドは表示されません

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドは、Session IDが2のSMBセッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報を表示します。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

関連情報

SMB署名済みセッションの統計の監視

ONTAP SMB署名セッションの統計の監視

SMBセッションの統計を監視して、確立されたセッションのうち、署名されているセッションと署名されていないセッションを確認できます。

タスクの内容

advanced権限レベルでコマンドを実行する `statistics`と、署名済みSMBセッションの数を監視するためのカウンタが提供され `signed_sessions`ます。この `signed_sessions`カウンタでは、次の統計オブジェクトを使用できます。

- `cifs`すべてのSMBセッションについてSMB署名を監視できます。
- `smb1`SMB 1.0セッションのSMB署名を監視できます。
- `smb2`SMB 2.xセッションとSMB 3.0セッションのSMB署名を監視できます。

  オブジェクトの出力にはSMB 3.0の統計が表示され `smb2`ます。

署名されたセッションの数をセッションの総数と比較する場合は、カウンタの出力とカウンタの出力 `established_sessions`を比較できます `signed_sessions`。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなけれ

ば、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を特定するのに役立ちます。

手順

1. 権限レベルをadvancedに設定します。+
`set -privilege advanced`
2. データ収集を開始します。+
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id`はテキスト文字列です。同じCLIセッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以前のデフォルトサンプルが上書きされます。

   必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

   の詳細については `statistics start`、を"ONTAPコマンド リファレンス"参照してください。

3. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。

   詳細はこちら `statistics stop`の中で"ONTAPコマンド リファレンス" 。

4. SMB署名統計を表示します。

表示する情報	入力するコマンド
署名されたセッション	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	署名されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   単一のノードの情報のみを表示する場合は、オプションのパラメータを指定します `-node`。

   の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

5. admin権限レベルに戻ります。+
`set -privilege admin`

例

次の例は、vs1というStorage Virtual Machine（SVM）について、SMB 2.xとSMB 3.0の署名統計を監視する方法を示しています。

次のコマンドは、advanced権限レベルに移行します。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

次のコマンドは、ノードごとに署名されたSMBセッションと確立されたSMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

次のコマンドは、node2の署名済みSMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

次のコマンドは、admin権限レベルに戻ります。

```
cluster1::*> set -privilege admin
```

関連情報

- SMBセッションが署名されているかどうかの確認
- "パフォーマンスの監視と管理の概要"

SMBを介したデータ転送での**SMB**サーバでの**SMB**暗号化要求の設定

ONTAP SMB暗号化の詳細

SMBを介したデータ転送でのSMB暗号化は、SMBサーバで有効または無効にできるセキュリティ強化です。共有プロパティ設定を使用して、共有ごとに必要なSMB暗号化を設定することもできます。

デフォルトでは、Storage Virtual Machine（SVM）でのSMBサーバの作成時にSMB暗号化は無効になっています。SMB暗号化が提供する強固なセキュリティを活用するには、SMB暗号化を有効にする必要があります。

暗号化SMBセッションを作成するには、SMBクライアントがSMB暗号化をサポートしている必要があります。SMB暗号化は、Windows Server 2012およびWindows 8以降のWindowsクライアントでサポートされています。

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

- SMBサーバのセキュリティ オプション：SVMでこの機能を有効にする
- SMB共有プロパティ：共有ごとにSMB暗号化を設定する

SVM上のすべてのデータへのアクセスに暗号化を要求するか、選択した共有のデータにアクセスする場合のみにSMB暗号化を要求するかを決定できます。SVMレベルの設定は、共有レベルの設定よりも優先されます。

実際に適用されるSMB暗号化設定は、この2つの設定の組み合わせによって決まります。次の表を参照してください。

SMB サーバ **SMB** 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しい	正しくない	SVMのすべての共有でサーバレベルの暗号化が有効になっています。この設定では、SMBセッション全体で暗号化が行われます。
正しい	正しい	共有レベルの暗号化に関係なく、SVMのすべての共有でサーバレベルの暗号化が有効になります。この設定では、SMBセッション全体で暗号化が行われます。
正しくない	正しい	特定の共有で共有レベルの暗号化が有効になっている。この設定では、ツリー接続から暗号化が行われます。

SMB サーバ SMB 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しくない	正しくない	暗号化は有効になっていません。

暗号化をサポートしていないSMBクライアントは、暗号化が必要なSMBサーバや共有には接続できません。

暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

ONTAP SMB暗号化によるパフォーマンスへの影響

SMBセッションでSMB暗号化を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行しているクラスタノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワークトラフィックの量に変化はありませんが、クライアントとサーバの両方でCPU使用率が増加したことを示しています。

パフォーマンスへの影響の程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9 .7以降では、新しい暗号化オフロードアルゴリズムにより、暗号化されたSMBトラフィックのパフォーマンスを向上させることができます。SMB暗号化オフロードは、SMB暗号化が有効になっている場合はデフォルトで有効になります。

SMB暗号化のパフォーマンスを強化するには、AES-NIオフロード機能が必要です。お使いのプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB暗号化のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証できます。

SMB暗号化は、SMBサーバではデフォルトで無効になっています。SMB暗号化は、暗号化を必要とするSMB共有またはSMBサーバでのみ有効にしてください。SMB暗号化では、ONTAPは要求を復号化し、要求ごとに応答を暗号化する追加の処理を実行します。そのため、SMB暗号化は必要な場合にのみ有効にしてください。

受信トラフィックの**ONTAP SMB**暗号化の有効化または無効化

受信 SMB トラフィックに SMB 暗号化を必須にする場合は、 CIFS サーバ上または共有レベルで有効にすることができます。デフォルトでは、 SMB 暗号化は必須ではありません。

タスクの内容

CIFS サーバ上で SMB 暗号化を有効にすることができます。この場合、 CIFS サーバ上のすべての共有が環境によって暗号化されます。CIFS サーバ上のすべての共有で SMB 暗号化要求を有効にしない場合、または受信 SMB トラフィックの SMB 暗号化要求を共有ごとに有効にする場合は、 CIFS サーバ上で SMB 暗号化要求を無効にすることができます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップするときにコマンドのオプション `snapmirror create`で選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

このオプションを（ID保持）に `true`設定する `-identity-preserve`と、SMB暗号化のセキュリティ設定がデスティネーションにレプリケートされます。

このオプションを（非ID保持）に `false`設定する `-identity-preserve`と、SMB暗号化のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションのCIFSサーバセキュリティ設定はデフォルト値に設定されます。ソース SVM で SMB 暗号化を有効にしている場合は、デスティネーションで CIFS サーバの SMB 暗号化を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

CIFSサーバでの受信**SMB**トラフィックの**SMB**暗号化要求の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
無効にする	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. CIFSサーバでのSMB暗号化要求が必要に応じて有効または無効になっていることを確認します。`vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   `is-smb-encryption-required`フィールドには、CIFSサーバでSMB暗号化要求が有効になっているかどうかと、SMB暗号化要求が無効になっているかどうか`false`が表示されます `true`。

例

次の例では、SVM vs1のCIFSサーバの受信SMBトラフィックのSMB暗号化要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

関連情報

- "スナップミラー作成"

クライアントが暗号化された**ONTAP SMB**セッションを使用して接続中かどうかの確認

接続中の SMB セッションに関する情報を表示して、クライアントが暗号化された SMB 接続を使用しているかどうかを確認できます。これは、必要なセキュリティ設定を使用してSMBクライアントセッションが接続されているかどうかを確認する場合に役立ちます。

タスクの内容

SMB クライアントセッションには、次の 3 つのいずれかの暗号化レベルを設定できます。

- `unencrypted`

  SMB セッションは暗号化されません。Storage Virtual Machine（SVM）レベルの暗号化も共有レベルの暗号化も設定されません。

- `partially-encrypted`

  ツリー接続が行われると、暗号化が開始されます。共有レベルの暗号化が設定されています。SVM レベルの暗号化は有効になりません。

- `encrypted`

  SMB セッションは完全に暗号化されます。SVM レベルの暗号化が有効です。共有レベルの暗号化は、有効になる場合とならない場合があります。SVM レベルの暗号化設定は、共有レベルの暗号化設定よりも優先されます。

手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した SVM のセッションで、指定した暗号化設定を使用するセッション	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定した SVM の特定のセッション ID の暗号化設定	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

例

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、暗号化設定を含む詳細なセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

ONTAPの**SMB**暗号化統計情報の監視

SMB暗号化の統計を監視して、確立されたセッションと共有接続のうち、暗号化されているものと暗号化されていないものを確認できます。

タスクの内容

advanced権限レベルでコマンドを実行する `statistics`と次のカウンタが表示され、暗号化されたSMBセッションおよび共有接続の数を監視できます。

カウンタ名	説明
`encrypted_sessions`	暗号化されたSMB 3.0セッションの数
`encrypted_share_connections`	ツリー接続が行われた暗号化された共有の数を示します。
`rejected_unencrypted_sessions`	クライアントの暗号化機能がないために拒否されたセッションセットアップの数
`rejected_unencrypted_shares`	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

- `cifs`すべてのSMB 3.0セッションについてSMB暗号化を監視できます。

  オブジェクトの出力にはSMB 3.0の統計が表示され `cifs`ます。暗号化されたセッション数をセッションの合計数と比較する場合は、カウンタの出力とカウンタの出力 `established_sessions`を比較できます `encrypted_sessions`。

  暗号化された共有接続の数を共有接続の総数と比較するには、カウンタの出力とカウンタの出力 `connected_shares`を比較します `encrypted_share_connections`。

- `rejected_unencrypted_sessions`SMB暗号化をサポートしていないクライアントから暗号化を必要とするSMBセッションの確立が試行された回数を示します。
- `rejected_unencrypted_shares`SMB暗号化をサポートしていないクライアントから暗号化が必要なSMB共有への接続が試行された回数を示します。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を特定するのに役立ちます。

手順

1. 権限レベルをadvancedに設定します。+
   `set -privilege advanced`
2. データ収集を開始します。+
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id`はテキスト文字列です。同じCLIセッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以前のデフォルトサンプルが上書きされます。

   必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

   の詳細については `statistics start`、を"ONTAPコマンド リファレンス"参照してください。

3. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。

   詳細はこちら `statistics stop`の中で"ONTAPコマンド リファレンス" 。

4. SMB暗号化統計を表示します。

表示する情報	入力するコマンド
暗号化されたセッション	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	暗号化されたセッションと確立されたセッション

表示する情報	入力するコマンド
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	暗号化された共有接続
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
暗号化された共有接続と接続された共有	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒否された非暗号化セッション	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒否された非暗号化共有接続
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

単一のノードの情報のみを表示する場合は、オプションのパラメータを指定します `-node`。

の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

5. admin権限レベルに戻ります。+
`set -privilege admin`

例

次の例は、「vs1」というStorage Virtual Machine（SVM）について、SMB 3.0暗号化統計情報を監視する方法を示しています。

次のコマンドは、advanced権限レベルに移行します。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

次のコマンドは、指定したノードについて、暗号化されたSMBセッションと確立されたSMBセッションをサンプルから表示します。

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

次のコマンドは、指定したノードについて、拒否された暗号化されていないSMBセッション数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

次のコマンドは、指定したノードについて、接続されているSMB共有と暗号化されたSMB共有の数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

次のコマンドは、指定したノードについて、拒否された暗号化されていないSMB共有接続の数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

関連情報

- サーバー上で利用可能な統計、オブジェクト、カウンターを決定する
- "パフォーマンスの監視と管理の概要"

セキュアな**LDAP**セッション通信

ONTAP SMB LDAPの署名と封印の詳細

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへのクエリに

対してLDAPセッションセキュリティを有効にすることができます。Storage Virtual Machine（SVM）のCIFSサーバセキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、シークレットキーテクノロジを使用してLDAPペイロードデータの整合性を確認します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。LDAPトラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトはです `none`。

CIFSトラフィックに対するLDAPの署名と封印は、コマンドのオプションを `vserver cifs security modify`使用して`SVM`で有効にします `-session-security-for-ad-ldap`。

ONTAP SMBサーバでの**LDAP**の署名と封印の有効化

CIFS サーバで Active Directory LDAP サーバとのセキュアな通信に署名と封印を使用するためには、 CIFS サーバのセキュリティ設定を変更して LDAP の署名と封印を有効にする必要があります。

開始する前に

AD サーバ管理者に問い合わせて、適切なセキュリティ設定値を決定する必要があります。

手順

1. Active Directory LDAPサーバとのトラフィックの署名と封印を有効にするCIFSサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   署名(`sign`、データ整合性）、署名と封印(`seal`、データの整合性と暗号化を有効にすることができます。また、 `none`署名と封印のどちらも有効にしないことも可能です。デフォルト値はです `none`。

2. LDAPの署名と封印のセキュリティ設定が正しく設定されていることを確認します。 `vserver cifs security show -vserver` *`vserver_name`*

> SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、コマンドのオプション `vserver services name-service ldap client modify`で対応する設定を有効にする必要があります。 `-session-security`

LDAP over TLSの設定

ONTAP SMB SVM用の自己署名ルート**CA**証明書のエクスポート

LDAP over SSL/TLSを使用してActive Directory通信を保護するには、まずActive Directory証明書サービスの自己署名ルートCA証明書のコピーを証明書ファイルにエクスポートし、ASCIIテキストファイルに変換する必要があります。ONTAPでは、このテキストファイルを使用して証明書をStorage Virtual Machine（SVM）にインストールします。

開始する前に

CIFSサーバが属しているドメイン用にActive Directory証明書サービスがインストールされ、設定されている必要があります。Active Director証明書サービスのインストールと設定については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNetライブラリ：technet.microsoft.com"

ステップ

1. ドメインコントローラのルートCA証明書をテキスト形式で取得します `.pem`。

   "Microsoft TechNetライブラリ：technet.microsoft.com"

終了後

SVMに証明書をインストールします。

関連情報

"Microsoft TechNetライブラリ"

ONTAP SMB SVMへの自己署名ルート**CA**証明書のインストール

LDAPサーバへのバインド時にTLSを使用したLDAP認証が必要な場合は、最初に自己署名ルートCA証明書をSVMにインストールする必要があります。

タスクの内容

TLS通信を使用するONTAP内のすべてのアプリケーションは、オンライン証明書ステータスプロトコル（OCSP）を使用してデジタル証明書のステータスを確認できます。OCSPがLDAP over TLSに対して有効になっている場合、失効した証明書は拒否され、接続は失敗します。

手順

1. 自己署名ルートCA証明書をインストールします。
   a. 証明書のインストールを開始します。 `security certificate install -vserver vserver_name -type server-ca`

      コンソール出力に次のメッセージが表示されます。 `Please enter Certificate: Press <Enter> when done`

   b. 証明書ファイルをテキストエディタで開き `.pem`、で始まる行とで終わる `-----END CERTIFICATE-----`行を含めて証明書をコピーし `-----BEGIN CERTIFICATE-----`、コマンドプロンプトのあとに証明書を貼り付けます。
   c. 証明書が正しく表示されることを確認します。
   d. Enterキーを押してインストールを完了します。
2. 証明書がインストールされたことを確認します。 `security certificate show -vserver vserver_name`

関連情報

- "セキュリティ証明書のインストール"
- "security certificate show"

ONTAP SMBサーバでの**LDAP over TLS**の有効化

SMBサーバでActive Directory LDAPサーバとのセキュアな通信にTLSを使用するには、SMBサーバのセキュリティ設定を変更してLDAP over TLSを有効にする必要があります。

10.1以降では、**ONTAP 9**チャネルバインドが**Active Directory**（**AD**）接続とネームサービス**LDAP**接続の両方でデフォルトでサポートされます。**ONTAP**は、**Start-TLS**または**LDAPS**が有効で、セッションセキュリティが署名または封印のいずれかに設定されている場合にのみ、**LDAP**接続でチャネルバインディングを試行します。**AD**サーバとの**LDAP**チャネルバインディングを無効または再度有効にするには、コマンドでパラメータを `**vserver cifs security modify**`使用し `**-try-channel-binding-for-ad-ldap**`ます。

詳細については、以下を参照してください。

- "ONTAP NFS SVMのLDAPについて学ぶ"
- "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"です。

手順

1. Active Directory LDAPサーバとのセキュアなLDAP通信を許可するSMBサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. LDAP over TLSのセキュリティ設定がに設定されていることを確認し `true`ます。 `vserver cifs security show -vserver` *`vserver_name`*

> SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、コマンドを使用してオプションを `vserver services name-service ldap client modify`変更する必要もあります。 `-use-start-tls`

パフォーマンスと冗長性を確保するための**ONTAP SMB**マルチチャネルの設定

ONTAP 9 .4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。

開始する前に

SMBマルチチャネル機能は、クライアントがSMB 3.0以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMBサーバではSMB 3.0以降がデフォルトで有効になっています。

タスクの内容

SMBクライアントは、ONTAPクラスタで適切な設定が見つかると、複数のネットワーク接続を自動的に検出して使用します。

SMBセッションでの同時接続数は、導入しているNICによって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

  クライアントはNICごとに1つの接続を確立し、すべての接続にセッションをバインドします。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

  クライアントはNICごとに最大4つの接続を確立し、すべての接続にセッションをバインドします。クライアントは、10G以上の容量の複数のNICで接続を確立できます。

また、次のパラメータを変更することもできます（advanced権限）。

- `-max-connections-per-session`

  マルチチャネルセッションごとに許可される最大接続数。デフォルトの接続数は32です。

  デフォルトよりも多くの接続を有効にする場合は、クライアント設定を調整する必要があります（デフォルトの接続数は32）。

- `-max-lifs-per-session`

  マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。デフォルトは256のネットワークインターフェイスです。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAPがSMBマルチチャネルセッションを報告していることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、すべてのSMBセッションに関する情報を表示します。1つのセッションに対する複数の接続が表示されています。

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

次の例は、セッションID 1のSMBセッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

SMBサーバでのデフォルトの**Windows**ユーザから**UNIX**ユーザへのマッピングの設定

ユーザに対する他のマッピングの試行がすべて失敗した場合や、 UNIX と Windows の間で個々のユーザをマッピングしないようにする場合に使用するデフォルトの UNIX ユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする必要がある場合は、デフォルト UNIX ユーザを設定しないでください。

タスクの内容

デフォルトでは、デフォルト UNIX ユーザの名前は「 pcuser 」です。これは、デフォルトで、デフォルト UNIX ユーザへのユーザマッピングが有効になっていることを意味します。デフォルトの UNIX ユーザとして使用する別の名前を指定することもできます。指定する名前は、Storage Virtual Machine（SVM）用に設定されているネームサービスデータベース内に存在している必要があります。このオプションを null 文字列に設定すると、どのユーザも UNIX デフォルトユーザとして CIFS サーバにアクセスできません。つまり、 CIFS サーバにアクセスするためには、各ユーザがパスワードデータベースにアカウントを持つ必要があります。

ユーザがデフォルトの UNIX ユーザアカウントを使用して CIFS サーバに接続するには、次の前提条件を満たす必要があります。

- ユーザが認証されていること。
- ユーザが、 CIFS サーバのローカル Windows ユーザデータベース、 CIFS サーバのホームドメイン、信頼できるドメイン（ CIFS サーバでマルチドメインネームマッピング検索が有効な場合）のいずれかにあること
- ユーザ名が明示的に null 文字列にマッピングされることはありません。

手順

1. デフォルトのUNIXユーザを設定します。

状況	入力するコマンド
デフォルトの UNIX ユーザ「 pcuser 」を使用する	`vserver cifs options modify -default -unix-user pcuser`
別の UNIX ユーザアカウントをデフォルトユーザとして使用します	`vserver cifs options modify -default -unix-user user_name`
デフォルトのUNIXユーザを無効にする	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. デフォルトのUNIXユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

   次の例では、 SVM vs1 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「 pcuser 」を使用するように設定されています。

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

ゲスト**ONTAP SMB UNIX**ユーザの設定

ゲスト UNIX ユーザを設定すると、信頼されていないドメインからログインしたユーザがゲスト UNIX ユーザにマッピングされ、 CIFS サーバに接続できるようになります。ただし、信頼されていないドメインのユーザの認証を失敗にする場合は、ゲスト UNIX ユーザを設定しないでください。デフォルトでは、信頼されていないドメインのユーザによる CIFS サーバへの接続は許可されません（ゲスト UNIX アカウントは設定されません）。

タスクの内容

ゲスト UNIX アカウントを設定する場合は、次の点に注意する必要があります。

- ホームドメイン、信頼できるドメイン、またはローカルデータベースのドメインコントローラに対してCIFSサーバがユーザを認証できない場合、このオプションが有効になっていると、CIFSサーバはそのユーザをゲストユーザとみなして、指定したUNIXユーザにユーザをマッピングします。
- このオプションを null 文字列に設定すると、ゲスト UNIX ユーザは無効になります。
- いずれかのStorage Virtual Machine（SVM）ネームサービスデータベースで、ゲストUNIXユーザとして使用するUNIXユーザを作成する必要があります。
- ゲストユーザとしてログインしたユーザは、自動的に CIFS サーバの BUILTIN\guests グループのメンバーになります。
- 「 homedirs-public 」オプションは、認証されたユーザにのみ適用されます。ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
ゲストUNIXユーザの設定	`vserver cifs options modify -guest -unix-user` *`unix_name`*
ゲスト UNIX ユーザを無効にします	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. ゲストUNIXユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

   次の例では、 SVM vs1 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「 pcuser 」を使用するように設定されています。

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

ONTAP SMBルートへの管理者グループのマッピング

環境内のクライアントがすべて CIFS クライアントで、 Storage Virtual Machine （ SVM ）がマルチプロトコルストレージシステムとしてセットアップされている場合は、 SVM 上のファイルにアクセスするための root 権限を持つ Windows アカウントが少なくとも 1 つ必要です。 十分なユーザ権限がないため、この SVM を管理できません。

タスクの内容

ストレージシステムがNTFS専用にセットアップされている場合は `/etc`、ディレクトリにファイルレベルのACLが設定され、Administratorsグループはこのアクセスを使用してONTAP構成ファイルにアクセスできます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 必要に応じて、 Administrators グループをルートにマッピングする CIFS サーバオプションを設定します。

状況	そしたら...。
管理者グループメンバーをルートにマッピングします	`vserver cifs options modify -vserver *vserver_name* -is-admin-users-mapped-to-root-enabled true`アカウントをrootにマッピングするエントリがない場合でも、Administratorsグループ内のすべてのアカウントはrootとみなされ `/etc/usermap.cfg`ます。Administrators グループに属するアカウントを使用してファイルを作成する場合、 UNIX クライアントからファイルを表示するときに、ファイルはルートによって所有されます。

状況	そしたら...。
Administrators グループメンバーのルートへのマッピングを無効にします	`vserver cifs options modify -vserver *vserver_name* -is-admin-users-mapped-to-root-enabled false`Administratorsグループ内のアカウントがrootにマッピングされなくなります。ルートへのマッピングは、単一のユーザに対して明示的にのみ実行できます。

3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver *vserver_name*`
4. admin権限レベルに戻ります。 `set -privilege admin`

ONTAP SMBセッションを介して接続しているユーザのタイプに関する情報を表示する

SMBセッションを介して接続しているユーザのタイプに関する情報を表示できます。これは、適切なタイプのユーザのみがStorage Virtual Machine（SVM）上のSMBセッションを介して接続していることを確認するのに役立ちます。

タスクの内容

SMBセッションを介して接続できるユーザのタイプは次のとおりです。

- `local-user`

  ローカル CIFS ユーザとして認証されている

- `domain-user`

  ドメインユーザとして（ CIFS サーバのホームドメインまたは信頼できるドメインから）認証されている

- `guest-user`

  ゲストユーザとして認証されています

- `anonymous-user`

  匿名ユーザまたは null ユーザとして認証されています

手順

1. SMBセッションを介して接続しているユーザのタイプを確認します。 `vserver cifs session show -vserver *vserver_name* -windows-user *windows_user_name* -fields windows-user,address,lif-address,user-type`

確立されたセッションのユーザタイプ情報を表示する対象	入力するコマンド
指定したユーザタイプのすべてのセッション	`vserver cifs session show -vserver *vserver_name* -user-type {local-user

確立されたセッションのユーザタイプ情報を表示する対象	入力するコマンド
domain-user	guest-user
anonymous-user}`	特定のユーザの場合

例

次のコマンドを実行すると、ユーザ「 iepubs\user1 」によって確立された SVM vs1 上のセッションのユーザタイプに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Windowsクライアントの過剰なリソース消費を制限する**ONTAP**コマンドオプション

コマンドのオプションを `vserver cifs options modify`使用すると、Windowsクライアントのリソース消費を制御できます。これは、ファイルオープン、セッションオープン、Change Notify要求が異常に多い場合など、通常の範囲を超えてリソースを消費するクライアントがある場合に役立ちます。

Windowsクライアントのリソース消費を制御するために、コマンドに次のオプション `vserver cifs options modify`が追加されました。いずれかのオプションの最大値を超えると、要求は拒否され、EMSメッセージが送信されます。これらのオプションに設定されている制限の80%に達したときにも、EMS警告メッセージが送信されます。

- `-max-opens-same-file-per-tree`

  CIFSツリーあたりの同一ファイルに対する最大オープン数

- `-max-same-user-sessions-per-connection`

  接続ごとに同じユーザが開いたセッションの最大数

- `-max-same-tree-connect-per-session`

  同じ共有に対するセッションあたりの最大ツリー接続数

- `-max-watches-set-per-tree`

  ツリーごとに確立されるウォッチの最大数（別名 *change notifier*）

の詳細については `vserver cifs options modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 9.4 以降では、 SMB バージョン 2 以降を実行しているサーバで、クライアントからサーバに SMB 接続で送信できる未処理要求（ _SMB クレジット _ ）の数を制限することができます。SMBクレジットの管理はクライアントによって開始され、サーバによって制御されます。

SMB接続で許可できる未処理要求の最大数は、オプションで制御され `-max-credits`ます。このオプションのデフォルト値は128です。

従来の**oplock**および**oplock**リースでクライアントパフォーマンスを向上

従来の**oplock**および**oplock**リースでの**ONTAP SMB**クライアントのパフォーマンスの向上

便宜的 oplock と oplock リースでは、先読み、あと書き、ロックの各情報を SMB クライアント側でキャッシングできるよう、特定のファイル共有シナリオでそのクライアントを有効にします。クライアントは、対象のファイルへのアクセスが必要であることをサーバに定期的に通知することなく、ファイルの読み取りや書き込みを行うことができます。これにより、ネットワークトラフィックが軽減され、パフォーマンスが向上します。

oplockリースはoplockを強化したもので、SMB 2.1以降のプロトコルで使用できます。oplockリースを使用すると、クライアントが自身を起点とする複数のSMBオープンでクライアントのキャッシュ状態を取得して保持できます。

oplock は次の 2 つの方法で制御できます。

- 共有プロパティ。共有の作成時にコマンドを使用するか、 `vserver share properties`作成後にコマンドを使用し `vserver cifs share create`ます。
- qtreeプロパティ。qtreeの作成時にコマンドを使用するか、 `volume qtree oplock`作成後にコマンドを使用し `volume qtree create`ます。

oplockを使用する場合の**ONTAP SMB**キャッシュデータ損失に関する考慮事項

状況によっては、あるプロセスがファイルに対して排他的なoplockを持っていて、別のプロセスがそのファイルを開こうとすると、最初のプロセスがキャッシュされたデータを無効にし、書き込みとロックをフラッシュしなければならないことがあります。その後、クライアントはoplockを放棄してファイルにアクセスする必要があります。このフラッシュ中にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われる可能性があります。

- データ損失の可能性

  データの書き込みがキャッシュされるアプリケーションでは、次の場合にそのデータを失う可能性があります。

  - 接続は SMB 1.0 を使用して確立されます。
  - ファイルに対して排他的な oplock を使用している場合
  - oplock を解除するか、ファイルを閉じるように指示された場合

- 書き込みキャッシュをフラッシュするプロセスで、ネットワークまたはターゲットシステムにエラーが発生した場合

- エラー処理および書き込みの完了

  キャッシュ自体にエラー処理機能はなく、アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行う場合、書き込みは必ず完了します。キャッシュがネットワークを介してターゲットシステムに書き込みを行う場合、書き込みが完了していないとデータが失われるため、書き込みが完了したと想定する必要があります。

ONTAP SMB共有の作成時にoplockを有効または無効にする

oplockを使用すると、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるため、ファイル操作のパフォーマンスが向上します。Storage Virtual Machine（SVM）上にあるSMB共有ではoplockが有効になります。場合によっては、oplockの無効化が必要になることがあります。oplockは共有ごとに有効または無効にできます。

タスクの内容

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームのoplock設定よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。

oplock共有プロパティに加えて、他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する操作を実行します。

状況	そしたら...。
共有の作成時に共有でoplockを有効にする	次のコマンドを入力します。 `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` 共有でデフォルトの共有プロパティ（、、、 `changenotify`）のみを有効にする場合 `oplocks`は、`browsable`SMB共有の作成時にパラメータを指定する必要はありません `-share-properties`。デフォルト以外の共有プロパティを組み合わせて使用する場合は、パラメータとその共有に使用する共有プロパティのリストを指定する必要があります `-share-properties`。

状況	そしたら...。
共有の作成時に共有でoplockを無効にする	次のコマンドを入力します。 `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` oplockを無効にする場合は、共有の作成時に共有プロパティのリストを指定する必要がありますが、プロパティは指定しないで `oplocks`ください。

関連情報

既存のSMB共有でoplocksを有効または無効にする

oplock ステータスを監視する

SMBボリュームおよび**qtree**で**oplock**を有効または無効にするための**ONTAP**コマンド

oplockを使用すると、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるため、ファイル操作のパフォーマンスが向上します。ここでは、ボリュームまたはqtreeでoplockを有効または無効にするコマンドについて説明します。また、ボリュームおよびqtreeでoplockを有効または無効にできるタイミングについても把握しておく必要があります。

- ボリュームでは、oplockがデフォルトで有効になっています。
- ボリュームの作成時にoplockを無効にすることはできません。
- 既存のSVMのボリュームでは、oplockをいつでも有効または無効にできます。
- SVMのqtreeではoplockを有効にできます。

  oplockモードの設定は、すべてのボリュームに含まれるデフォルトのqtreeであるqtree ID 0のプロパティです。qtreeの作成時にoplock設定を指定しない場合、qtreeは親ボリュームのoplock設定（デフォルトで有効）を継承します。ただし、新しいqtreeでoplock設定を指定した場合は、ボリュームのoplock設定よりも優先されます。

状況	使用するコマンド
ボリュームまたはqtreeでoplockを有効にする	`volume qtree oplocks`パラメータがに設定されている `enable`場合 `-oplock-mode`
ボリュームまたはqtreeでoplockを無効にする	`volume qtree oplocks`パラメータがに設定されている `disable`場合 `-oplock-mode`

関連情報

既存のONTAP SMB共有でのoplockの有効化または無効化

Storage Virtual Machine（SVM）上のSMB共有では、oplockがデフォルトで有効になっています。状況によっては、oplockの無効化が必要になることがあります。また、以前に共有でoplockを無効にしたことがある場合は、oplockを再度有効にすることもできます。

タスクの内容

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームでのoplockの有効化よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。既存の共有では、oplockをいつでも有効または無効にできます。

ステップ

1. 該当する操作を実行します。

状況	そしたら...。
既存の共有を変更して共有でoplockを有効にする	次のコマンドを入力します。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` 追加する共有プロパティをカンマで区切って追加指定できます。 新しく追加したプロパティは、既存の共有プロパティのリストに追加されます。以前に指定した共有プロパティは有効なままです。
既存の共有を変更して共有でoplockを無効にする	次のコマンドを入力します。 `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` 削除する共有プロパティをカンマで区切って追加指定できます。 削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しない設定済みの共有プロパティは有効なままです。

例

次のコマンドは、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 Engineering 」という名前の共有の oplock を有効にします。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

次のコマンドは、 SVM vs1 上の「 Engineering 」という名前の共有の oplock を無効にします。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

関連情報

- SMB共有を作成するときにoplocksを有効または無効にする
- oplock ステータスを監視する
- 既存の共有の共有プロパティを追加または削除する

ONTAP SMB oplockステータスの監視

oplockステータスに関する情報を監視および表示できます。この情報を使用して、oplockが設定されているファイル、oplockレベルとoplock状態レベル、およびoplockリースが使用されているかどうかを確認できます。また、手動での解除が必要になる可能性があるロックに関する情報を確認することもできます。

タスクの内容

すべてのoplockに関する情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、指定したクライアントIPアドレスまたは指定したパスを持つロックのみを出力に返すように指定できます。

従来のoplockおよびoplockリースについて、次の情報を表示できます。

- oplockが有効なSVM、ノード、ボリューム、LIF
- ロックUUID

- oplockが有効なクライアントのIPアドレス
- oplockが有効なパス
- ロックのプロトコル（SMB）とタイプ（oplock）
- ロックの状態
- oplockレベル
- 接続状態とSMBの有効期限
- oplockリースが許可されている場合のOpen Group ID

の詳細については `vserver oplocks show`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用して、oplockステータスを表示します `vserver locks show`。

例

次のコマンドは、すべてのロックに関するデフォルトの情報を表示します。表示されたファイルのoplockにはoplockレベルが設定されてい `read-batch`ます。

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF          Protocol  Lock Type   Client
-------- ------------------ ------------ --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                         cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                   op-lock     192.168.1.5
         Oplock Level: read-batch
```

次の例は、パスのファイルに対するロックに関する詳細情報を表示します `/data2/data2_2/intro.pptx`。このファイルでは、IPアドレスがのクライアントに対してoplockレベルで `10.3.1.3`oplockリースが許可されてい `batch`ます。

詳細情報を表示する場合は、oplockと共有ロックの情報を個別に出力します。この例は、oplockセクションの出力のみを示しています。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

関連情報

SMB共有を作成するときにoplocksを有効または無効にする

既存のSMB共有でoplocksを有効または無効にする

SMBボリュームおよびqtreeでoplockを有効または無効にするコマンド

SMBサーバへのグループポリシーオブジェクトの適用

ONTAP SMBサーバへのグループポリシーオブジェクトの適用について

SMBサーバは、グループポリシーオブジェクト（GPO）をサポートしています。GPOは、Active Directory環境のコンピュータに適用される_グループポリシー属性_と呼ばれる一連のルールです。GPOを使用して、同じActive Directoryドメインに属するクラスタ上のすべてのStorage Virtual Machine（SVM）の設定を一元管理できます。

SMBサーバでGPOが有効になっている場合、ONTAPはActive DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。SMBサーバに適用可能なGPO定義がある場合、Active Directoryサーバは次のGPO情報を

返します。

- GPO名
- 現在のGPOバージョン
- GPO定義の場所
- GPOポリシーセットのUUID（Universally Unique Identifier）のリスト

関連情報

- サーバーのファイルアクセスセキュリティについて学ぶ
- "SMBおよびNFSの監査とセキュリティトレース"

サポートされる**ONTAP SMB GPO**の詳細

すべてのグループポリシーオブジェクト（GPO）をCIFS対応のStorage Virtual Machine（SVM）に適用できるわけではありませんが、SVMでは関連するGPOを認識して処理することができます。

SVMで現在サポートされているGPOは次のとおりです。

- 監査ポリシーの詳細設定：

  オブジェクトへのアクセス：集約型アクセスポリシーのステージング

  次の設定を含む、集約型アクセスポリシー（CAP）のステージングで監査対象となるイベントのタイプを指定します。

  - 監査しないでください
  - 成功イベントのみ監査
  - 失敗イベントのみ監査
  - 成功イベントと失敗イベントの両方を監査します

  > 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

  GPOの設定 `Advanced Audit Policy Configuration/Audit Policies/Object Access`を使用して設定します `Audit Central Access Policy Staging`。

  > 高度な監査ポリシー構成GPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- レジストリ設定：

  - CIFS 対応の SVM のグループポリシーの更新間隔

    GPOを使用して設定し`Registry`ます。

- グループポリシーの更新間隔のランダムオフセット

  GPOを使用して設定し `Registry`ます。

- BranchCache のハッシュの発行

  BranchCacheのハッシュの発行GPOは、BranchCacheの動作モードに対応しています。次の3つの動作モードがサポートされています。

  - 共有ごと
  - all-shares
  - Disabled GPOを使用して設定します `Registry`。

- BranchCache のハッシュバージョンサポート

  次の3つのハッシュバージョン設定がサポートされています。

  - BranchCache バージョン 1.7
  - BranchCache バージョン 1.7
  - BranchCacheバージョン1および2 GPOを使用して設定されます `Registry`。

> BranchCache GPO設定を使用するには、その設定を適用するCIFS対応のSVMでBranchCacheを構成する必要があります。SVMでBranchCacheが構成されていない場合、GPO設定は適用されず、破棄されます。

- セキュリティ設定
  - 監査ポリシーとイベントログ
    - ログオンイベントを監査します

      次の設定を含む監査対象のログオンイベントのタイプを指定します。

      - 監査しないでください
      - 成功イベントのみ監査
      - 障害イベントの監査
      - GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit logon events`。

> 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

    - オブジェクトへのアクセスを監査する

      次の設定を含む、監査対象のオブジェクトアクセスのタイプを指定します。

      - 監査しないでください
      - 成功イベントのみ監査

- 障害イベントの監査
- GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit object access`。

> 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- ログの保持方法

  次の設定を含む監査ログの保持方法を指定します。

  - ログファイルのサイズが最大ログサイズを超えたら、イベントログを上書きします
  - GPOの設定を `Event Log`使用して設定されたイベントログを上書きしないでください（ログを手動でクリア） `Retention method for security log`。
- 最大ログサイズ

  監査ログの最大サイズを指定します。

  GPOの設定 `Event Log`を使用して設定します `Maximum security log size`。

> 監査ポリシーとイベントログGPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

◦ ファイルシステムのセキュリティ

GPOを介してファイルセキュリティが適用されるファイルまたはディレクトリのリストを指定します。

GPOを使用して設定し `File System`ます。

> SVM内にファイルシステムセキュリティGPOを設定するボリュームパスが存在している必要があります。

◦ Kerberos ポリシー

- 最大クロックスキュー

  コンピュータクロック同期の最大許容値を分単位で指定します。

  GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum tolerance for computer clock synchronization`。

- チケットの有効期間

  ユーザチケットの最大有効期間を時間単位で指定します。

  GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum lifetime for user ticket`。

- チケットの更新の有効期間

  ユーザチケット更新の最大有効期間を日数で指定します。

GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum lifetime for user ticket renewal`。

◦ ユーザ権限の割り当て（権限）

- 所有権の取得

  セキュリティ保護可能なオブジェクトの所有権を取得する権限を持つユーザおよびグループのリストを指定します。

  GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Take ownership of files or other objects`。

- セキュリティ権限

  ファイル、フォルダ、Active Directoryオブジェクトなど、個 々 のリソースのオブジェクトアクセスの監査オプションを指定できるユーザとグループのリストを指定します。

  GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Manage auditing and security log`。

- 通知権限の変更（トラバースチェックのバイパス）

  ユーザとグループにトラバースするディレクトリに対する権限がない場合でも、ディレクトリツリーをトラバースできるユーザとグループのリストを指定します。

ユーザがファイルおよびディレクトリの変更通知を受信するには、同じ権限が必要です。GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Bypass traverse checking`。

◦ レジストリ値

- 署名要求設定

  SMB署名要求が有効になっているか無効になっているかを示します。

GPOの設定 `Security Options`を使用して設定します `Microsoft network server: Digitally sign communications (always)`。

◦ restrict anonymous （匿名の制限

匿名ユーザに対する制限を指定します。次の3つのGPO設定が含まれます。

- Security Account Manager （ SAM ）アカウントを列挙しない：

  このセキュリティ設定は、コンピュータへの匿名接続に対して許可される追加の権限を決定します。このオプションが有効になっている場合は、ONTAPでと表示され`no-enumeration`ます。

GPOの設定 `Local Policies/Security Options`を使用して設定します `Network access: Do not allow anonymous enumeration of SAM accounts`。

- SAM アカウントと共有は列挙しません

  このセキュリティ設定では、SAMアカウントと共有の匿名列挙を許可するかどうかを指定します。このオプションが有効になっている場合は、ONTAPでと表示され `no-enumeration`ます。

  GPOの設定 `Local Policies/Security Options`を使用して設定します `Network access: Do not allow anonymous enumeration of SAM accounts and shares`。

- 共有と名前付きパイプへの匿名アクセスを制限します

  共有とパイプへの匿名アクセスを制限します。このオプションが有効になっている場合は、ONTAPでと表示され `no-access`ます。

  GPOの設定 `Local Policies/Security Options`を使用して設定します `Network access: Restrict anonymous access to Named Pipes and Shares`。

  定義済みおよび適用済みのグループポリシーに関する情報を表示する場合、出力フィールドには、3つのrestrict anonymous GPO設定による制限に関する情報が表示 `Resultant restriction for anonymous user`されます。考えられる制限は次のとおりです。

◦ `no-access`

匿名ユーザは、指定された共有と名前付きパイプへのアクセスを拒否され、SAMアカウントと共有を列挙できません。この制限は、GPOが有効になっている場合に発生し `Network access: Restrict anonymous access to Named Pipes and Shares`ます。

◦ `no-enumeration`

匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAMアカウントと共有を列挙することはできません。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- `Network access: Do not allow anonymous enumeration of SAM accounts`または `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPOが有効になっている。

◦ `no-restriction`

匿名ユーザにはフルアクセスが付与され、列挙を使用できます。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- GPOと `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPOの両方 `Network access: Do not allow anonymous enumeration of SAM accounts`が無効になっている。
  - 制限されたグループ

    制限されたグループを設定して、組み込みグループまたはユーザ定義グループのメンバーシッ

プを一元管理できます。グループポリシーを使用して制限されたグループを適用すると、CIFSサーバローカルグループのメンバーシップは、適用されたグループポリシーで定義されているメンバーシップリストの設定に一致するように自動的に設定されます。

GPOを使用して設定し `Restricted Groups`ます。

- 集約型アクセスポリシーの設定

  集約型アクセスポリシーのリストを指定します。集約型アクセスポリシーと関連付けられた集約型アクセスポリシールールによって、SVM上の複数のファイルに対するアクセス権限が決定されます。

関連情報

- サーバー上の GPO サポートを有効または無効にする
- サーバーのファイルアクセスセキュリティについて学ぶ
- "SMBおよびNFSの監査とセキュリティトレース"
- サーバーのセキュリティ設定を変更する
- BranchCache を使用してブランチ オフィスの共有コンテンツをキャッシュする方法について説明します。
- ONTAP署名を使用してネットワークセキュリティを強化する方法について学習します
- バイパストラバースチェックの設定について学ぶ
- 匿名ユーザに対するアクセス制限の設定

GPOのONTAP SMBサーバの要件

SMBサーバでグループポリシーオブジェクト（GPO）を使用するには、システムがいくつかの要件を満たしている必要があります。

- クラスタでSMBのライセンスが有効になっている必要があります。SMBライセンスはに含まれて い"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- SMBサーバが設定され、Windows Active Directoryドメインに追加されている必要があります。
- SMBサーバ管理ステータスがオンである必要があります。
- GPOが設定され、SMBサーバ コンピュータ オブジェクトを含むWindows Active Directoryの組織単位（OU）に適用されている必要があります。
- SMBサーバでGPOのサポートが有効になっている必要があります。

ONTAP SMBサーバでのGPOサポートの有効化または無効化

CIFSサーバでGroup Policy Object（GPO；グループポリシーオブジェクト）のサポートを有効または無効にすることができます。CIFSサーバでGPOのサポートを有効にすると、グループポリシー（CIFSサーバコンピュータオブジェクトを含む組織単位（OU）に適用されるポリシー）で定義されている該当するGPOがCIFSサーバに適用されます。

タスクの内容

GPOは、ワークグループモードのCIFSサーバでは有効にできません。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
GPOを有効にする	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOを無効にする	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. GPOサポートが目的の状態になっていることを確認します。 `vserver cifs group-policy show -vserver +vserver_name_`

   ワークグループモードの CIFS サーバのグループポリシーステータスは「 disabled 」と表示されます。

例

次の例では、Storage Virtual Machine（SVM）vs1でGPOサポートを有効にします。

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

関連情報

サポートされているGPOについて学ぶ

GPOのサーバー要件

SMBサーバー上のGPOの更新について学ぶ

SMBサーバーのGPO設定を手動で更新する

GPO構成に関する情報を表示する

SMBサアハテノ**GPO**ノコウシンホウホウ

ONTAP SMBサーバでの**GPO**の更新について

デフォルトでは、ONTAPはグループポリシーオブジェクト（GPO）の変更を90分ごとに取得して適用します。セキュリティ設定は16時間ごとに更新されます。ONTAPで自動

的に更新される前にGPOを更新して新しいGPOポリシー設定を適用する場合は、ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーできます。

- デフォルトでは、すべてのGPOが90分ごとに検証され、必要に応じて更新されます。

  この間隔は設定可能で、および `Random offset`GPO設定を使用して設定できます `Refresh interval`。

  ONTAPは、GPOの変更がないかどうかをActive Directoryに照会します。Active Directoryに記録されているGPOのバージョン番号がCIFSサーバ上のGPOのバージョン番号より大きい場合、ONTAPは新しいGPOを取得して適用します。バージョン番号が同じ場合、CIFSサーバ上のGPOは更新されません。

- セキュリティ設定のGPOは16時間ごとに更新されます。

  ONTAPは、変更の有無にかかわらず、16時間ごとにセキュリティ設定のGPOを取得して適用します。

  デフォルト値の16時間は、現在のONTAPバージョンでは変更できません。これはWindowsクライアントのデフォルト設定です。

- ONTAPコマンドを使用して、すべてのGPOを手動で更新できます。

  このコマンドは、Windowsの/force'コマンドをシミュレートし `gpupdate.exe``ます。

関連情報

SMBサーバーのGPO設定を手動で更新する

ONTAP SMBサーバでの**GPO**設定の手動更新

CIFSサーバのGroup Policy Object（GPO；グループポリシーオブジェクト）設定をすぐに更新する場合は、設定を手動で更新できます。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

ステップ

1. 適切な操作を実行します。

更新する項目	入力するコマンド
GPO設定が変更されました	`vserver cifs group-policy update -vserver vserver_name`
すべてのGPO設定	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

関連情報

SMBサーバー上のGPOの更新について学ぶ

Active Directoryで定義されているグループポリシーオブジェクト（GPO）設定、およびCIFSサーバに適用されているGPO設定に関する情報を表示できます。

タスクの内容

CIFSサーバが属しているドメインのActive Directoryで定義されているすべてのGPO設定に関する情報を表示することも、CIFSサーバに適用されているGPO設定に関する情報のみを表示することもできます。

手順

1. 次のいずれかの操作を実行して、GPO設定に関する情報を表示します。

情報を表示するグループポリシー設定	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy show-defined -vserver vserver_name`
CIFS対応のStorage Virtual Machine（SVM）に適用されている	`vserver cifs group-policy show-applied -vserver vserver_name`

例

次の例は、CIFS対応のvs1という名前のSVMが属するActive Directoryで定義されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
------------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
```

```
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
```

```
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

次の例は、CIFS対応のSVM vs1に適用されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
```

```
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
```

```
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
```

関連情報

サーバー上の GPO サポートを有効または無効にする

ONTAP SMB制限されたグループの**GPO**に関する情報を表示する

Active Directoryでグループポリシーオブジェクト（GPO）として定義されている制限されたグループ、およびCIFSサーバに適用されている制限されたグループに関する詳細情報を表示できます。

タスクの内容

デフォルトでは、次の情報が表示されます。

- グループポリシー名
- グループポリシーバージョン
- リンク

  グループポリシーが設定されているレベルを指定します。指定可能な出力値は次のとおりです。

  - `Local`グループポリシーがONTAPで設定されている状況
  - `Site`グループポリシーがドメインコントローラのサイトレベルで設定されている場合
  - `Domain`グループポリシーがドメインコントローラのドメインレベルで設定されている場合
  - `OrganizationalUnit`グループポリシーがドメインコントローラのOrganizational Unit（OU；組織単位）レベルで設定されている場合
  - `RSOP`さまざまなレベルで定義されたすべてのグループポリシーから派生した一連のポリシー
- 制限されたグループ名
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ

- 制限されたグループが追加されているグループのリスト

  グループは、ここにリストされているグループ以外のグループのメンバーになることができます。

ステップ

1. 次のいずれかの操作を実行して、制限されたグループのすべてのGPOに関する情報を表示します。

情報を表示する制限されたグループのすべての**GPO**	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

例

次の例は、CIFS対応のvs1という名前のSVMが属するActive Directoryドメインで定義されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

次の例では、CIFS対応のSVM vs1に適用されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

関連情報

GPO構成に関する情報を表示する

ONTAP SMB集約型アクセスポリシーに関する情報を表示する

Active Directoryで定義されている集約型アクセスポリシーに関する詳細情報を表示できます。また、Group Policy Object（GPO；グループポリシーオブジェクト）を介してCIFSサーバに適用されている集約型アクセスポリシーに関する情報も表示できます。

タスクの内容

デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセスポリシーの名前
- SID
- 説明
- 作成時間
- 更新日時
- メンバールール

ワークグループモードのCIFSサーバはGPOをサポートしていないため表示されません。

ステップ

1. 次のいずれかの操作を実行して、集約型アクセスポリシーに関する情報を表示します。

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
CIFSサアハニテキヨウ	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

例

次の例は、Active Directoryで定義されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

次の例は、クラスタ上のStorage Virtual Machine（SVM）に適用されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                  SID
-------- --------------------
-----------------------------------------------
vs1      p1                    S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                    S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

関連情報

- サーバーのファイルアクセスセキュリティについて学ぶ
- GPO構成に関する情報を表示する
- 集中アクセスポリシールールに関する情報を表示する

ONTAP SMB集約型アクセスポリシールールに関する情報を表示する

Active Directoryで定義されている集約型アクセスポリシーに関連付けられている集約型アクセスポリシールールに関する詳細情報を表示できます。また、集約型アクセスポリシーのGPO（グループポリシーオブジェクト）を介してCIFSサーバに適用されている集約型アクセスポリシールールに関する情報も表示できます。

タスクの内容

定義済みおよび適用されている集約型アクセスポリシールールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 更新日時
- 現在の権限

- 推奨される権限
- ターゲットリソース

集約型アクセスポリシーに関連付けられた、情報を表示するすべての集約型アクセスポリシールール	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

例

次の例は、Active Directoryで定義されている集約型アクセスポリシーに関連付けられているすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

次の例は、クラスタ上のStorage Virtual Machine（SVM）に適用されている集約型アクセスポリシーに関連付けられているすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

関連情報

- サーバーのファイルアクセスセキュリティについて学ぶ
- GPO構成に関する情報を表示する
- 集中アクセスポリシーに関する情報を表示する

SMBサーバコンピュータアカウントパスワードの管理用**ONTAP**コマンド

パスワードの変更、リセット、無効化、および自動更新スケジュールの設定に使用するコマンドについて説明します。SMBサーバでスケジュールを設定して自動的に更新することもできます。

状況	使用するコマンド
ONTAPがADサービスと同期されている場合のドメインアカウントパスワードの変更	`vserver cifs domain password change`
ONTAPがADサービスと同期されていない場合のドメインアカウントパスワードのリセット	`vserver cifs domain password reset`
SMBサーバでコンピュータアカウントパスワードの自動変更を設定する	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
SMBサーバでのコンピュータアカウントパスワードの自動変更の無効化	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

の詳細については `vserver cifs domain password`、を"ONTAPコマンド リファレンス"参照してください。

ドメインコントローラ接続の管理

ONTAP SMBで検出されたサーバに関する情報を表示する

CIFSサーバで検出されたLDAPサーバおよびドメインコントローラに関する情報を表示できます。

ステップ

1. 検出されたサーバに関する情報を表示するには、次のコマンドを入力します。 `vserver cifs domain discovered-servers show`

例

次の例は、SVM vs1で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

関連情報

- サーバのリセットと再検出
- サーバーの停止または起動

ONTAP SMBサーバのリセットと再検出

CIFSサーバでサーバをリセットおよび再検出すると、LDAPサーバおよびドメインコントローラに関するCIFSサーバに格納されている情報が破棄されます。サーバ情報を破棄したあと、CIFSサーバはこれらの外部サーバに関する最新の情報を再取得します。これは、接続されているサーバが適切に応答しない場合に役立ちます。

手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 再検出されたサーバに関する情報を表示します。 `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

例

次の例では、Storage Virtual Machine（SVM、旧Vserver）vs1のサーバをリセットして再検出します。

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

関連情報

- 検出されたサーバーに関する情報を表示する
- サーバーの停止または起動

ONTAP SMBドメインコントローラの検出を管理します。

ONTAP 9 .3以降では、ドメインコントローラ（DC）の検出に使用するデフォルトプロセスを変更できます。これにより、検出対象をサイトまたは優先DCのプールに限定できます。これにより、環境によってはパフォーマンスが向上する可能性があります。

タスクの内容

デフォルトでは、動的検出プロセスによって、使用可能なすべてのDC（優先DC、ローカルサイト内のすべてのDC、およびすべてのリモートDCを含む）が検出されます。そのため、一部の環境では、認証時および共有へのアクセス時にレイテンシが発生する可能性があります。使用するDCのプールが決まっている場合、またはリモートDCが不適切またはアクセスできない場合、検出方法を変更することができます。

ONTAP 9 .3以降のリリースでは `discovery-mode`、コマンドのパラメータを `cifs domain discovered-servers`使用して次の検出オプションのいずれかを選択できます。

- ドメイン内のすべてのDCが検出されます。
- ローカルサイトのDCだけが検出されます。

  SMBサーバのパラメータは、 `default-site`sites-and-servicesでサイトに割り当てられていないLIFでこのモードを使用するように定義できます。

- サーバ検出は実行されず、優先DCのみを使用してSMBサーバを設定します。

  このモードを使用するには、まずSMBサーバの優先DCを定義する必要があります。

開始する前に

advanced権限レベルが必要です。

ステップ

1. 目的の検出オプションを指定します。 `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   パラメータのオプション `mode`：

   - `all`

     使用可能なすべてのDCを検出します（デフォルト）。

   - `site`

     DC検出をサイトに限定します。

   - `none`

     優先DCのみを使用し、検出は実行しません。

優先ONTAP SMBドメインコントローラの追加

ONTAPは、DNSを介してドメインコントローラを自動的に検出します。必要に応じて、特定のドメインに対する優先ドメインコントローラのリストに1つ以上のドメインコントローラを追加できます。

タスクの内容

指定したドメインの優先ドメインコントローラリストがすでに存在する場合は、新しいリストが既存のリストにマージされます。

ステップ

1. 優先ドメインコントローラのリストに追加するには、次のコマンドを入力します。+
   `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver *vserver_name*`Storage Virtual Machine（SVM）名を示します。

   `-domain *domain_name*`指定したドメインコントローラが属するドメインの完全修飾Active Directory名を指定します。

   `-preferred-dc` *`IP_address`*、…には、優先ドメインコントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

例

次のコマンドでは、SVM vs1上のSMBサーバがcifs.lab.example.comドメインへの外部アクセスを管理するために使用する優先ドメインコントローラのリストに、ドメインコントローラ172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

関連情報

優先ドメインコントローラの管理用コマンド

優先**SMB**ドメインコントローラの管理用**ONTAP**コマンド

優先ドメインコントローラを追加、表示、削除するコマンドについて説明します。

状況	使用するコマンド
優先ドメインコントローラを追加する	`vserver cifs domain preferred-dc add`
優先ドメインコントローラを表示する	`vserver cifs domain preferred-dc show`
優先ドメインコントローラを削除する	`vserver cifs domain preferred-dc remove`

の詳細については `vserver cifs domain preferred-dc`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

優先ドメインコントローラを追加する

ONTAP SMBドメインコントローラへの暗号化された接続を有効にする

ONTAP 9 .8以降では、ドメインコントローラへの接続を暗号化するように指定できます。

タスクの内容

このオプションをに設定 `true`すると、`ONTAP`でドメインコントローラ（`DC`）通信の暗号化が必要になります `-encryption-required-for-dc-connection`。デフォルトはです。 `false`暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されます。

暗号化されたDC通信が必要な場合、ONTAPはSMB3接続のみをネゴシエートするため、この `-smb2-enabled-for-dc-connections`オプションは無視されます。DCがSMB3と暗号化をサポートしていない場合、ONTAPは接続しません。

ステップ

1. DCとの暗号化通信を有効にします。 `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

非**Kerberos**環境でストレージにアクセスするには**null**セッションを使用します。

null セッションアクセスは、ローカルシステムで稼働しているクライアントベースのサービスにストレージシステムデータなどのネットワークリソースへのアクセスを提供します。null セッションは、クライアントプロセスが「システム」アカウントを使用してネットワークリソースにアクセスするときに発生します。null セッション設定は非 Kerberos 認証に固有です。

ONTAP SMBストレージシステムがnullセッションアクセスを提供する方法

nullセッション共有は認証を必要としないため、nullセッションアクセスを必要とするクライアントは、ストレージシステム上でIPアドレスをマッピングする必要があります。

デフォルトでは、マッピングされていないnullセッションクライアントは、共有の列挙などの特定のONTAPシステムサービスにはアクセスできますが、ストレージシステムデータへのアクセスは制限されます。

> ONTAPでは、オプションを使用してWindows RestrictAnonymousレジストリ設定値をサポートしています `-restrict-anonymous`。これにより、マッピングされていないnullユーザがシステムリソースを表示またはアクセスできる範囲を制御できます。たとえば、共有の列挙とipc$共有（非表示の名前付きパイプ共有）へのアクセスを無効にすることができます。および `vserver cifs options show` `–restrict-anonymous`オプションの詳細については、を"ONTAPコマンド リファレンス"参照して `vserver cifs options modify`ください。

特に設定がないかぎり、 null セッションでストレージシステムアクセスを要求するローカルプロセスを実行しているクライアントは、「 everyone 」などの制限のないグループのみのメンバーとなります。nullセッションアクセスを選択したストレージシステムリソースに制限するには、すべてのnullセッションクライアントが属するグループを作成します。このグループを作成すると、ストレージシステムアクセスを制限し、nullセッションクライアントにのみ適用されるストレージシステムリソース権限を設定できます。

ONTAPのコマンドセットでは `vserver name-mapping`、nullユーザセッションを使用したストレージシステムリソースへのアクセスを許可するクライアントのIPアドレスを指定できます。nullユーザ用のグループを作成したら、nullセッションにのみ適用されるストレージシステムリソースおよびリソース権限に対するアクセス制限を指定できます。nullユーザは匿名ログオンとして識別されます。nullユーザはどのホームディレクトリにもアクセスできません。

マッピングされたIPアドレスからストレージシステムにアクセスするすべてのnullユーザには、マッピングされたユーザ権限が付与されます。nullユーザにマッピングされたストレージシステムへの不正アクセスを防止するために、適切な予防措置を検討してください。最大限の保護を実現するには、ストレージシステムと null ユーザによるストレージシステムアクセスが必要なすべてのクライアントを別のネットワークに配置し、 IP アドレス「 SVM 」の問題を解消します。

関連情報

匿名ユーザに対するアクセス制限の設定

ONTAP SMBファイルシステム共有へのアクセスをnullユーザに許可

nullセッションクライアントによるストレージシステムリソースへのアクセスを許可するには、nullセッションクライアントが使用するグループを割り当て、nullセッションクライアントのIPアドレスを記録して、ストレージシステム上の、nullセッションを使用したデータアクセスを許可するクライアントのリストに追加します。

手順

1. コマンドを使用し `vserver name-mapping create`て、IP修飾子を使用して、有効なWindowsユーザにnullユーザをマッピングします。

   次のコマンドは、有効なホスト名 google.com で user1 に null ユーザをマッピングします。

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   次のコマンドは、有効な IP アドレス 10.238.2.54/32 で user1 に null ユーザをマッピングします。

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. コマンドを使用し `vserver name-mapping show`て、ネームマッピングを確認します。

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. コマンドを使用し `vserver cifs options modify –win-name-for-null-user`て、nullユーザにWindowsメンバーシップを割り当てます。

   このオプションは、 null ユーザに有効なネームマッピングが設定されている場合にのみ使用できます。

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. コマンドを使用し `vserver cifs options show`て、nullユーザがWindowsユーザまたはグループにマッピングされていることを確認します。

   ```
   vserver cifs options show

   Vserver :vs1

   Map Null User to Windows User of Group: user1
   ```

SMBサーバのNetBIOSエイリアスを管理します。

ONTAP SMBサーバのNetBIOSエイリアスの管理について

NetBIOSエイリアスは、SMBクライアントがSMBサーバに接続するときに使用できるSMBサーバの別名です。SMBサーバのNetBIOSエイリアスを設定すると、他のファイルサーバのデータをSMBサーバに統合し、SMBサーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

NetBIOSエイリアスのリストは、SMBサーバの作成時、またはSMBサーバの作成後にいつでも指定できます。リストにNetBIOSエイリアスを追加または削除することはいつでもできます。SMBサーバには、NetBIOSエイリアスリスト内の任意の名前を使用して接続できます。

関連情報

NetBIOS over TCP接続に関する情報を表示する

ONTAP SMBサーバへのNetBIOSエイリアスリストの追加

エイリアスを使用してSMBサーバに接続できるようにするには、NetBIOSエイリアスのリストを作成するか、既存のNetBIOSエイリアスのリストにNetBIOSエイリアスを追加します。

タスクの内容

- NetBIOSエイリアス名は15文字以内で指定します。
- SMBサーバには最大200個のNetBIOSエイリアスを設定できます。
- 次の文字は使用できません。

  @ # * （） = +[] | ； ： " 、 <> \ / ？

手順

1. NetBIOSエイリアスを追加します。+
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - 1 つ以上の NetBIOS エイリアスをカンマで区切って指定します。
   - 指定した NetBIOS エイリアスが既存のリストに追加されます。
   - NetBIOSエイリアスのリストが現在空の場合は、新しいリストが作成されます。
2. NetBIOSエイリアスが正しく追加されたことを確認します。 `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

関連情報

- SMBサーバーのリストからNetBIOSエイリアスを削除します
- SMBサーバーのNetBIOSエイリアスリストを表示する

ONTAP SMBサーバのリストから**NetBIOS**エイリアスを削除する

CIFS サーバで特定の NetBIOS エイリアスが不要な場合、その NetBIOS エイリアスをリストから削除できます。リストからすべての NetBIOS エイリアスを削除することもできます。

タスクの内容

複数のNetBIOSエイリアスを削除するには、カンマで区切って指定します。パラメータの値に `-netbios -aliases`を指定すると、CIFSサーバ上のすべてのNetBIOSエイリアスを削除できます `-`。

手順

1. 次のいずれかを実行します。

削除する項目	入力するコマンド
リスト内の特定の NetBIOS エイリアス	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
リスト内のすべての NetBIOS エイリアス	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 指定したNetBIOSエイリアスが削除されたことを確認します。 `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_2, ALIAS_3
```

NetBIOSエイリアスのリストを表示できます。これは、SMBクライアントがCIFSサーバへの接続に使用できる名前のリストを確認する場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
CIFSサーバのNetBIOSエイリアス	`vserver cifs show -display-netbios -aliases`
NetBIOSエイリアスのリスト（CIFSサーバの詳細情報の一部）	`vserver cifs show -instance`

次の例は、CIFSサーバのNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

次の例は、NetBIOSエイリアスのリストを含む詳細なCIFSサーバ情報を表示します。

```
vserver cifs show -instance
```

```
                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

の詳細については `vserver cifs show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- NetBIOSエイリアスリストをサーバーに追加する

- サーバーを管理するためのコマンド

ONTAP SMBクライアントが**NetBIOS**エイリアスを使用して接続しているかどうかの確認

SMB クライアントが NetBIOS エイリアスを使用して接続しているかどうか、および使用している場合はその NetBIOS エイリアスを確認できます。これは、接続の問題をトラブルシューティングするときに役立ちます。

タスクの内容

SMB接続に関連付けられているNetBIOSエイリアス（ある場合）を表示するには、パラメータを使用する必要があります `-instance`。CIFSサーバの名前またはIPアドレスを使用してSMB接続を確立している場合、フィールドの出力 `NetBIOS Name`は（ハイフン）になります `-`。

ステップ

1. 必要な操作を実行します。

表示する **NetBIOS** 情報	入力するコマンド
SMBセツソク	`vserver cifs session show -instance`
指定した NetBIOS エイリアスを使用する接続：	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

次の例は、Session ID 1とのSMB接続に使用されるNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

その他の**SMB**サーバタスクの管理

ONTAP SMBサーバの停止と起動

ユーザがSMB共有を介してデータにアクセスしていない間にタスクを実行する場合は、SVM上のCIFSサーバを停止すると便利です。SMBアクセスを再開するには、CIFSサーバを起動します。CIFSサーバを停止することによって、Storage Virtual Machine（SVM）で許可されているプロトコルを変更することもできます。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
CIFSサーバを停止する	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	CIFSサーバを起動する
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground`コマンドをフォアグラウンドとバックグラウンドのどちらで実行するかを指定します。このパラメータを入力しない場合、このパラメータはに設定され `true`、フォアグラウンドでコマンドが

実行されます。

2. コマンドを使用して、CIFSサーバの管理ステータスが正しいことを確認します `vserver cifs show`。

例

次のコマンドは、SVM vs1でCIFSサーバを起動します。

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

関連情報

- 検出されたサーバーに関する情報を表示する
- サーバのリセットと再検出

別のOUへのONTAP SMBサーバの移動

CIFSサーバの作成プロセスでは、別のOUを指定しないかぎり、セットアップ時にデフォルトの組織単位（OU）CN=Computersが使用されます。CIFSサーバはセットアップ後に別のOUに移動できます。

手順

1. Windows サーバーで、 * Active Directory ユーザーとコンピューター * ツリーを開きます。
2. Storage Virtual Machine（SVM）のActive Directoryオブジェクトを探します。
3. オブジェクトを右クリックし、 * 移動 * （ * Move * ）を選択します。
4. SVMに関連付けるOUを選択します。

結果

選択したOUにSVMオブジェクトが配置されます。

ONTAP SMBサーバを移動する前の動的DNSドメインの変更

SMBサーバを別のドメインに移動するときに、Active Directory統合DNSサーバでSMBサーバのDNSレコードがDNSに動的に登録されるようにするには、SMBサーバを移動する前にStorage Virtual Machine（SVM）の動的DNS（DDNS）を変更する必要があります。

開始する前に

SMB サーバコンピュータアカウントを含む新しいドメインのサービスロケーションレコードを含む DNS ドメインを使用するには、 SVM で DNS ネームサービスを変更する必要があります。セキュアDDNSを使用している場合は、Active Directoryに統合されたDNSネームサーバを使用する必要があります。

タスクの内容

DDNS （ SVM 上で設定されている場合）はデータ LIF の DNS レコードを新しいドメインに自動的に追加しますが、元のドメインの DNS レコードは元の DNS サーバから自動的には削除されません。手動で削除する必要があります。

SMBサーバを移動する前にDDNSの変更を完了するには、次のトピックを参照してください。

"動的DNSサービスの設定"

Active DirectoryドメインへのONTAP SMB SVMの追加

コマンドを使用してドメインを変更すると、既存のSMBサーバを削除せずにStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify`。現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

開始する前に

- SVM の DNS 設定が完了している必要があります。
- SVM の DNS 設定がターゲットドメインを提供できる必要があります。

  DNSサーバには、ドメインLDAPサーバとドメインコントローラサーバのサービスロケーションレコード（SRV）が含まれている必要があります。

タスクの内容

- Active Directoryドメインを変更するには、CIFSサーバの管理ステータスがに設定されている必要があります `down`。
- コマンドが正常に完了すると、管理ステータスは自動的にに設定されます `up`。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。
- ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

手順

1. SVMをCIFSサーバドメインに追加します。 `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   の詳細については `vserver cifs modify`、を"ONTAPコマンド リファレンス"参照してください。新しいドメイン用にDNSを再設定する必要がある場合は、の詳細を参照して `vserver dns modify`"ONTAPコマンド リファレンス"ください。

   SMBサーバ用のActive Directoryマシンアカウントを作成するには、.comドメイン内のコンテナ *`example`* にコンピュータを追加するための十分な `Privileges`を備えた `Windows`アカウントの名前とパスワードを指定する必要があります `ou=` *`example`* `ou`。

   ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabフ

ァイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

2. CIFSサーバが目的のActive Directoryドメイン内にあることを確認します。 `vserver cifs show`

例

次の例では、 SVM vs1 上にある SMB サーバ「 CIFSSERVER1 」を keytab 認証を使用して example.com ドメインに追加します。

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

ONTAP SMB NetBIOS over TCP接続に関する情報を表示する

NetBIOS over TCP（NBT）接続に関する情報を表示できます。これは、NetBIOS関連の問題のトラブルシューティングに役立ちます。

ステップ

1. NetBIOS over TCP接続に関する情報を表示するには、コマンドを使用し `vserver cifs nbtstat`ます。

   IPv6経由のNetBIOSネームサービス（NBNS）はサポートされていません。

例

次の例は、「 cluster1 」について表示される NetBIOS ネームサービスの情報を示しています。

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

SMBサーバの管理用**ONTAP**コマンド

作成、表示、変更、停止、開始、 およびSMBサーバを削除しています。また、サーバのリセットと再検出、マシンアカウントパスワードの変更またはリセット、マシンアカウントパスワードのスケジュール変更、NetBIOSエイリアスの追加または削除を行うコマンドもあります。

状況	使用するコマンド
SMB サーバを作成	`vserver cifs create`
SMBサーバに関する情報を表示する	`vserver cifs show`
SMBサーバを変更する	`vserver cifs modify`
SMBサーバを別のドメインに移動する	`vserver cifs modify`

SMBサーバを停止する	`vserver cifs stop`
SMBサーバを起動する	`vserver cifs start`
SMBサーバを削除する	`vserver cifs delete`
SMBサーバ用のサーバのリセットと再検出	`vserver cifs domain discovered-servers reset-servers`
SMBサーバのマシンアカウントパスワードを変更する	`vserver cifs domain password change`
SMBサーバのマシンアカウントパスワードをリセットする	`vserver cifs domain password change`
SMBサーバのマシンアカウントの自動パスワード変更のスケジュールを設定する	`vserver cifs domain password schedule modify`
SMBサーバ用のNetBIOSエイリアスを追加する	`vserver cifs add-netbios-aliases`
SMBサーバのNetBIOSエイリアスを削除する	`vserver cifs remove-netbios-aliases`

の詳細については `vserver cifs`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

"SMBサーバを削除したときのローカルユーザとローカルグループへの影響"

ONTAP SMB NetBIOSネームサービスを有効にする

ONTAP 9以降では、NetBIOSネームサービス（NBNS、Windowsインターネットネームサービスまたは WINSと呼ばれることもあります）はデフォルトで無効になっています。以前は、WINSがネットワークで有効になっているかどうかに関係なく、CIFS対応Storage Virtual Machine（SVM）が名前登録のブロードキャストを送信していました。このようなブロードキャストをNBNSが必要な構成に限定するには、新しいCIFSサーバに対してNBNSを明示的に有効にする必要があります。

開始する前に

- すでにNBNSを使用していて、ONTAP 9にアップグレードする場合は、このタスクを実行する必要はありません。NBNSは以前と同様に機能します。
- NBNSはUDP（ポート137）でイネーブルになっています。
- IPv6経由のNBNSはサポートされていません。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. CIFSサーバでNBNSを有効にします。

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. admin権限レベルに戻ります。

```
set -privilege admin
```

SMBアクセスと**SMB**サービスに**IPv6**を使用する

IPv6の**ONTAP SMB**要件の詳細

SMBサーバでIPv6を使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとライセンスの要件について確認しておく必要があります。

ONTAPのライセンス要件

SMBのライセンスがある場合、IPv6に特別なライセンスは必要ありません。SMBライセンスはに含まれて"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMBプロトコルのバージョン

- SVMについては、ONTAPですべてのバージョンのSMBプロトコルでIPv6がサポートされます。

IPv6経由のNetBIOSネームサービス（NBNS）はサポートされていません。

ONTAPの**SMB**アクセスと**CIFS**サービスでの**IPv6**のサポートについて

CIFSサーバでIPv6を使用する場合は、ONTAPによるSMBアクセスやCIFSサービスとのネットワーク通信でのIPv6のサポートについて確認しておく必要があります。

Windowsクライアントおよびサーバのサポート

ONTAPは、IPv6をサポートするWindowsサーバおよびクライアントをサポートします。次に、Microsoft Windowsクライアントおよびサーバの IPv6サポートについて説明します。

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012以降では、SMBファイル共有とActive Directoryサービス（DNS、LDAP、CLDAP、Kerberosの各サービス）の両方でIPv6がサポートされます。

  IPv6アドレスが設定されている場合、Windows 7およびWindows Server 2008以降のリリースで

は、Active Directoryサービスにデフォルトで IPv6が使用されます。IPv6接続を介したNTLM認証とKerberos認証の両方がサポートされます。

ONTAPでサポートされるWindowsクライアントは、いずれもIPv6アドレスを使用してSMB共有に接続できます。

ONTAPがサポートするWindowsクライアントの最新情報については、を参照して"Interoperability Matrix"ください。

NTドメインはIPv6ではサポートされていません。

その他の**CIFS**サービスのサポート

ONTAPでは、SMBファイル共有とActive Directoryサービスに加えて、次の項目に対してもIPv6をサポートしています。

- クライアント側のサービス（オフラインフォルダ、移動プロファイル、フォルダリダイレクト、以前のバージョン機能など）
- サーバ側のサービス：動的ホームディレクトリ（ホームディレクトリ機能）、シンボリックリンクとワイドリンク、BranchCache、ODXコピーオフロード、自動ノードリファーラル、以前のバージョン機能など
- ファイルアクセス管理サービス（Windowsのローカルユーザおよびローカルグループを使用したアクセス制御と権限の管理、CLIを使用したファイル権限と監査ポリシーの設定、セキュリティトレース、ファイルロックの管理、SMBアクティビティの監視など）
- NASのマルチプロトコルの監査
- FPolicy
- 共有の継続的可用性、監視プロトコル、およびリモートVSS（Hyper-V over SMB構成で使用）

ネームサービスと認証サービスのサポート

IPv6では、次のネームサービスとの通信がサポートされます。

- ドメインコントローラ
- DNSサーバ
- LDAPサーバ
- KDCサーバ
- NISサーバ

ONTAP SMBサーバで**IPv6**を使用して外部サーバに接続する方法

要件に応じた設定を作成するには、CIFSサーバが外部サーバへの接続を確立する際にIPv6がどのように使用されるかを確認しておく必要があります。

- 送信元アドレスの選択

  外部サーバに接続しようとする場合、選択する送信元アドレスは宛先アドレスと同じタイプである必要があります。たとえば、IPv6アドレスに接続する場合、CIFSサーバをホストするStorage Virtual Machine（SVM）には、ソースアドレスとして使用するIPv6アドレスを持つデータLIFまたは管理LIFが必要です。

同様に、IPv4アドレスに接続する場合、SVMには、ソースアドレスとして使用するIPv4アドレスを持つデータLIFまたは管理LIFが必要です。

- DNSを使用して動的に検出されたサーバの場合、サーバ検出は次のように実行されます。
  - クラスタで IPv6 が無効になっている場合は、 IPv4 サーバアドレスのみが検出されます。
  - クラスタで IPv6 が有効になっている場合は、 IPv4 と IPv6 の両方のサーバアドレスが検出されます。アドレスが属するサーバが適切かどうか、およびIPv6またはIPv4のデータLIFまたは管理LIFが使用可能かどうかに応じて、どちらかのタイプが使用されます。動的サーバ検出は、ドメインコントローラとその関連サービス（LSA、NETLOGON、Kerberos、LDAPなど）の検出に使用されます。
- DNSサーバへの接続

  SVMがDNSサーバに接続するときにIPv6を使用するかどうかは、DNSネーム サービスの設定によって決まります。IPv6アドレスを使用するようにDNSサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、DNSサーバへの接続で引き続きIPv4アドレスを使用できるように、DNSネームサービスの設定でIPv4アドレスを使用できます。DNSネーム サービスの設定時には、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。
- LDAPサーバへの接続

  SVMがLDAPサーバに接続するときにIPv6を使用するかどうかは、LDAPクライアントの設定によって異なります。IPv6アドレスを使用するようにLDAPクライアントが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、LDAPサーバへの接続で引き続きIPv4アドレスを使用できるように、LDAPクライアント設定でIPv4アドレスを使用できます。LDAPクライアントの設定時に、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

  LDAPクライアント設定は、UNIXユーザ、グループ、およびネットグループのネームサービス用にLDAPを設定するときに使用されます。
- NISサーバへの接続

  SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネームサービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、NISサーバへの接続で引き続きIPv4アドレスを使用できるように、NISネームサービスの設定でIPv4アドレスを使用できます。NISネームサービスの設定時に、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

  NISネームサービスは、UNIXユーザ、グループ、ネットグループ、およびホスト名オブジェクトを格納および管理するために使用されます。

関連情報

- サーバーのIPv6を有効にする
- IPv6セッションに関する情報を監視および表示する

ONTAP SMBサーバでのIPv6の有効化

IPv6ネットワークはクラスタのセットアップ時に有効になりません。SMBでIPv6を使用するには、クラスタのセットアップ完了後にクラスタ管理者がIPv6を有効にする必要があります。クラスタ管理者がIPv6を有効にすると、IPv6はクラスタ全体で有効になります。

ステップ

1. IPv6を有効にします。 `network options ipv6 modify -enabled true`

   IPv6が有効になっています。SMBアクセス用のIPv6データLIFを設定できます。

関連情報

- IPv6セッションに関する情報を監視および表示する
- "System Managerを使用したネットワークの可視化"
- "クラスターで IPv6 を有効にする"
- "ネットワークオプションipv6 modify"

ONTAP SMBサーバでのIPv6の無効化について

クラスタでIPv6を有効にするにはネットワークオプションを使用しますが、同じコマンドを使用してSMBでIPv6を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後にIPv6を有効にしたインターフェイスを無効にすると、ONTAPはIPv6を無効にします。IPv6が有効なインターフェイスの管理については、クラスタ管理者に問い合わせてください。

関連情報

- "System Managerを使用したONTAPネットワークの可視化"

IPv6 ONTAP SMBセッションに関する情報を監視および表示する

IPv6ネットワークを使用して接続されているSMBセッションに関する情報を監視および表示できます。この情報は、IPv6 SMBセッションに関するその他の有用な情報と同様に、IPv6を使用して接続しているクライアントを特定する場合に役立ちます。

ステップ

1. 必要な操作を実行します。

確認する項目	入力するコマンド
Storage Virtual Machine（SVM）へのSMBセッションはIPv6を使用して接続される	`vserver cifs session show -vserver vserver_name -instance`
IPv6は、指定したLIFアドレスを介したSMBセッションに使用されます。	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` `LIF_IP_address`は、データLIFのIPv6アドレスです。

SMBを使用したファイルアクセスのセットアップ

セキュリティ形式の設定

セキュリティ形式がデータアクセスに与える影響

ONTAP SMBのセキュリティ形式とその影響

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式によって、データに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データ アクセスの制御にONTAPで使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームでUNIXセキュリティ形式を使用している場合でも、ONTAPはマルチプロトコルに対応しているため、SMBクライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAPでは、UNIXクライアントのみが標準のツールを使用して変更できるUNIX権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
UNIX	NFS	NFSv3モードビット	UNIX	NFSとSMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
mixed	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
unified （ Infinite Volume のみ、 ONTAP 9.4 以前のリリース）	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVolでは、UNIX、NTFS、およびmixedのセキュリティ形式がサポートされます。セキュリティ形式がmixedまたはunifiedの場合、ユーザはセキュリティ形式を個別に設定するため、権限を最後に変更したクライアントのタイプによって有効な権限が異なります。権限を最後に変更したクライアントがNFSv3クライアントの場合、権限はUNIX NFSv3モードビットになります。最後のクライアントがNFSv4クライアントの場合、権限はNFSv4 ACLになります。最後のクライアントがSMBクライアントの場合、権限はWindows NTFS ACLになります。

unifiedセキュリティ形式は、Infinite Volumeでのみ使用できます。Infinite Volumeは、ONTAP 9 .5以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

その `show-effective-permissions`パラメータを `vserver security file-directory`コマンドを使用すると、指定されたファイルまたはフォルダー パスで `Windows` または `UNIX` ユーザーに付与され

た有効な権限を表示できます。また、オプションのパラメータを `-share-name`使用すると、有効な共有権限を表示できます。の詳細については `vserver security file-directory show-effective-permissions`、を"ONTAPコマンド リファレンス"参照してください。

> ONTAPは、最初に一部のデフォルトのファイル権限を設定します。デフォルトでは、UNIX、mixed、およびunifiedのセキュリティ形式のボリュームにあるデータには、セキュリティ形式はUNIXになり、アクセス権のタイプはUNIXモードビット（特に指定がないかぎり0755）になります。これは、デフォルトのセキュリティ形式で許可されるようにクライアントによって設定されるまでの間です。デフォルトでは、NTFSセキュリティ形式のボリューム内のすべてのデータに対するセキュリティ形式はNTFSになり、すべてのユーザにフルコントロールを許可するACLが割り当てられます。

関連情報

- "ONTAPコマンド リファレンス"

ONTAP SMBセキュリティ形式を設定する場所とタイミングに関する詳細情報

セキュリティ形式は、 FlexVol （ルートボリュームとデータボリュームの両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

ONTAP SVMで使用する**SMB**セキュリティ形式の決定

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります。主な要因は、ファイルシステムを管理する管理者のタイプです。2番目の要因は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームでセキュリティ形式を設定する場合は、最適なセキュリティ形式を選択し、権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定には、次の考慮事項が役立ちます。

セキュリティ形式	以下の場合に選択
UNIX	• ファイルシステムはUNIX管理者によって管理されます。 • ユーザの大半がNFSクライアントである。 • データにアクセスするアプリケーションでは、UNIXユーザをサービスアカウントとして使用します。
NTFS	• ファイルシステムはWindows管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションでは、Windowsユーザをサービスアカウントとして使用します。

セキュリティ形式	以下の場合に選択
mixed	ファイルシステムはUNIX管理者とWindows管理者の両方によって管理され、ユーザはNFSクライアントとSMBクライアントの両方で構成されます。

ONTAPの**SMB**セキュリティ形式の継承について

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAP SMB FlexVolボリュームの**UNIX**アクセス権の保持に関する詳細

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

ONTAP SMBサーバ用の**Windows**の**[**セキュリティ**]**タブを使用した**UNIX**権限の管理について

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 Windows クライアントのセキュリティタブを使用できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

  モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータに

アカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

ONTAP SVMルートボリュームでの**SMB**セキュリティ形式の設定

Storage Virtual Machine（SVM）のルートボリューム上のデータに使用するアクセス権のタイプを決定するには、SVMルートボリュームのセキュリティ形式を設定します。

手順

1. セキュリティ形式を定義するには、コマンドで `-rootvolume-security-style`パラメータを使用し `vserver create`ます。

   ルートボリュームのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

2. 作成したSVMのルートボリュームセキュリティ形式を含む設定を表示して確認します。 `vserver show -vserver vserver_name`

ONTAP FlexVolボリュームでの**SMB**セキュリティ形式の設定

Storage Virtual Machine（SVM）のFlexVol上のデータに使用するアクセス権のタイプを決定するには、FlexVol volumeセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
まだ存在しません	`volume create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

FlexVol volumeセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

FlexVol volumeの作成時にセキュリティ形式を指定しない場合、ボリュームはルートボリュームのセキュリティ形式を継承します。

コマンドまたは `volume modify`コマンドの詳細については `volume create`、を参照してください"論理ストレージ管理"。

2. 作成したFlexVol volumeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume show -volume volume_name -instance
```

ONTAP qtreeでのSMBセキュリティ形式の設定

qtree上のデータに使用するアクセス権のタイプを決定するには、qtreeボリュームのセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
まだ存在しません	`volume qtree create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume qtree modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

qtreeのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

コマンドまたは `volume qtree modify`コマンドの詳細については `volume qtree create`、を参照してください"論理ストレージ管理"。

2. 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。 `volume qtree show -qtree qtree_name -instance`

NASネームスペースでのデータボリュームの作成と管理

NASネームスペースでのONTAP SMBデータボリュームの作成と管理について

NAS環境でファイルアクセスを管理するには、Storage Virtual Machine（SVM）上でデータボリュームとジャンクションポイントを管理する必要があります。これには、ネームスペースアーキテクチャの計画、ジャンクションポイントが設定されたボリュームまたはジャンクションポイントが設定されていないボリュームの作成、ボリュームのマウントまたはアンマウント、およびデータボリュームや NFS サーバまたは CIFS サーバの

ネームスペースに関する情報の表示が含まれます。

ジャンクションポイントを指定して**ONTAP SMB**データボリュームを作成する

ジャンクションポイントは、データボリュームの作成時に指定できます。作成したボリュームはジャンクションポイントに自動的にマウントされ、NASアクセス用の設定にすぐに使用できます。

開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

> ジャンクションパスに次の文字を使用することはできません。 * # <> < | ? \
>
> また、ジャンクションパスの長さは255文字以下にする必要があります。

手順

1. ジャンクションポイントを設定してボリュームを作成します。 `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   ジャンクションパスはルート（/）で始まる必要があり、ディレクトリと結合されたボリュームの両方を含めることができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリュームと同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームに適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   ジャンクションパスでは大文字と小文字が区別されません。はと同じ `/eng`です。 `/ENG`CIFS共有を作成する場合、Windowsではジャンクションパスは大文字と小文字が区別されるかのように扱われます。たとえば、ジャンクションがの場合、 `/ENG`CIFS共有のパスははではなくで `/eng`始まる必要があります `/ENG。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

例

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

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

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

ジャンクションポイントを指定せずに**ONTAP SMB**データボリュームを作成する

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にはマウントされず、NASアクセス用に設定することもできません。ボリュームに対してSMB共有またはNFSエクスポートを設定するには、ボリュームをマウントする必要があります。

開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

手順

1. 次のコマンドを使用して、ジャンクションポイントが設定されていないボリュームを作成します。
   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリュームと同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームに適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

2. ボリュームがジャンクションポイントなしで作成されたことを確認します。 `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

例

次の例は、ジャンクションポイントにマウントされない「 sales 」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NASネームスペースで既存の**ONTAP SMB**ボリュームをマウントまたはアンマウントする

Storage Virtual Machine（SVM）ボリュームに格納されたデータへのNASクライアントからのアクセスを設定するには、ボリュームがNASネームスペースにマウントされている必要があります。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームをアンマウントすることもできます。

タスクの内容

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、ジャンクションポイント内のすべてのデータにNASクライアントからアクセスできなくなります。

> ボリュームへのNASクライアントアクセスを中止するには、ボリュームをアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次のナレッジベースの記事を参照してください。 "ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"

ボリュームをアンマウントしてオフラインにしても、ボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーと、ボリュームまたはディレクトリに作成されたSMB共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすると、NASクライアントは既存のエクスポートポリシーとSMB共有を使用してボリュームに格納されているデータにアクセスできます。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームのマウント	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

状況	入力するコマンド

ボリュームのアンマウント	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例は、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ONTAP SMBボリュームのマウントポイントとジャンクションポイントの情報を表示します。

Storage Virtual Machine（SVM）のマウントボリューム、およびボリュームがマウントされているジャンクションポイントに関する情報を表示できます。ジャンクションポイ

ントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVMネームスペースを理解し、管理することができます。

手順

1. 必要な操作を実行します。

表示する項目	入力するコマンド
SVMのマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver vserver_name -junction`
SVMのマウントされたボリュームとマウントされていないボリュームに関する詳細情報	`volume show -vserver vserver_name -volume volume_name -instance`
SVMのマウントされたボリュームとマウントされていないボリュームに関する特定の情報	a. 必要に応じて、次のコマンドを使用してパラメータの有効なフィールドを表示できます `-fields。 volume show -fields ?` b. パラメータを使用して、必要な情報を表示し `-fields`ます。volume show -vserver vserver_name -fields fieldname、……

例

次の例では、SVM vs1のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

次の例は、SVM vs2上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

ネームマッピングの設定

ONTAP SMBネームマッピング設定の詳細

ONTAPでは、ネームマッピングを使用して、CIFS IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをCIFS IDにマッピングします。この情報は、NFSクライアントとCIFSクライアントのどちらから接続しているかに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要になります。

ネームマッピングを使用する必要がない例外が2つあります。

- 純粋なUNIX環境を構成し、ボリュームでCIFSアクセスまたはNTFSセキュリティ形式を使用する予定がない場合。
- 代わりにデフォルトユーザを使用するように設定します。

  このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。

ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できないことに注意してください。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、salesという語で開始または終了するすべてのADユーザを、特定のUNIXユーザおよびそのユーザのUIDにマッピングできます。

ONTAP SMBネームマッピングの詳細

ONTAPでユーザのクレデンシャルをマッピングする必要がある場合は、まずローカルのネームマッピングデータベースとLDAPサーバで既存のマッピングの有無を確認します。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVMのネームサービスの設定で決まります。

- WindowsからUNIXへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPは小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。見つからない場合は、デフォルトのUNIXユーザを使用します（設定済みの場合）。デフォルトのUNIXユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIXからWindowsへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPはSMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合は、デフォルトのSMBユーザを使用します（設定済みの場合）。デフォルトのCIFSユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトで指定されたデフォルトのUNIXユーザにマッピングされます。デフォルトのUNIXユーザが指定されていない場合、マシンアカウントのマッピングは失敗します。

- ONTAP 9 .5以降では、マシンアカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9 .4以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントのネームマッピングが定義されていても、それらのマッピングは無視されます。

UNIXユーザからWindowsユーザへのネームマッピング用のONTAP SMBマルチドメイン検索について

ONTAPは、UNIXユーザをWindowsユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性がUNIXユーザからWindowsユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性がONTAPとどのように連携するかを理解しておく必要があります。CIFSサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、SVMのCIFSサーバが属しているドメインです。

- _ 双方向の信頼 _

双方向の信頼では、両方のドメインが相互に信頼されます。CIFSサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

UNIXユーザからWindowsユーザへのネームマッピング検索は、ホームドメインともう一方のドメイン間で双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼 _

  アウトバウンドの信頼では、ホームドメインはもう一方のドメインを信頼します。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属するユーザを認証および許可できます。

  ホームドメインとアウトバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

- インバウンドの信頼 _

  インバウンドの信頼では、もう一方のドメインがCIFSサーバのホームドメインを信頼します。この場合、ホームドメインはインバウンドの信頼できるドメインに属するユーザを認証または許可できません。

  ホームドメインとインバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

ワイルドカード（*）を使用したネームマッピング用のマルチドメイン検索の設定方法

マルチドメインネームマッピングの検索は、Windowsユーザ名のドメインセクションにワイルドカードを使用することで簡単に実行できます。次の表に、ネームマッピングエントリのドメイン部分でワイルドカードを使用してマルチドメイン検索を有効にする方法を示します。

パターン	交換	結果
root	*\\administrator	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。

パターン	交換	結果
*	\ * \\ *	有効なUNIXユーザが対応するWindowsユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。 パターン「 \ * \\ * 」は、 UNIX から Windows へのネームマッピングでのみ有効であり、反対方向では無効です。

マルチドメインの名前検索の実行方法

マルチドメイン名の検索に使用する信頼できるドメインのリストを決定するには、次の2つの方法のいずれかを選択します。

- ONTAPによってコンパイルされた自動検出双方向信頼リストを使用する
- コンパイルした信頼できるドメインの優先リストを使用する

ユーザ名のドメインセクションにワイルドカードを使用してUNIXユーザがWindowsユーザにマッピングされている場合、Windowsユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピングされたWindowsユーザはこの検索リストでのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係が確立されたすべてのドメインでWindowsユーザの検索が行われます。
- ホームドメインに双方向の信頼関係が確立されたドメインがない場合は、ホームドメインでユーザの検索が行われます。

UNIXユーザがユーザ名にドメインセクションのないWindowsユーザにマッピングされている場合、ホームドメインでWindowsユーザの検索が行われます。

ONTAP SMBネームマッピングの変換ルールについて

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIXプログラムのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed`。

ONTAP SMBネームマッピングの作成

コマンドを使用すると、ネームマッピングを作成できます `vserver name-mapping`

`create`。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

タスクの内容

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`

   および `-replacement`ステートメントは、 `-pattern`正規表現として記述できます。また、ステートメントを使用して、`null`の置換文字列（スペース文字）を使用してユーザへのマッピングを明示的に拒否する `" "`こともできます `-replacement`。の詳細については `vserver name-mapping create`、を"ONTAPコマンド リファレンス"参照してください。

   Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、 vs1 という名前の SVM 上にネームマッピングを作成します。このマッピングは、UNIXからWindowsへのマッピングで、優先順位リストの1番目にあります。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン ENG 内のすべての CIFS ユーザが、 SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

デフォルトの**ONTAP SMB**ユーザを設定する

ユーザに対する他のマッピング試行がすべて失敗した場合や、UNIXとWindowsの間で個々 のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。または、マッピングされていないユーザの認証を失敗させる場合は、デフォルトユーザを設定しないでください。

タスクの内容

CIFS認証で、各Windowsユーザを個 々 のUNIXユーザにマッピングしない場合は、代わりにデフォルトのUNIXユーザを指定できます。

NFS認証で、各UNIXユーザを個 々 のWindowsユーザにマッピングしない場合は、代わりにデフォルトのWindowsユーザを指定できます。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトのUNIXユーザを設定する	`vserver cifs options modify -default -unix-user` *`user_name`*
デフォルトのWindowsユーザを設定する	`vserver nfs modify -default-win-user` *`user_name`*

SMBネームマッピングを管理するための**ONTAP**コマンド

ONTAPには、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
名前マッピングを作成する	`vserver name-mapping create`
特定の位置に名前マッピングを挿入する	`vserver name-mapping insert`
表示名のマッピング	`vserver name-mapping show`

2つのネームマッピングの位置を交換する注：ネームマッピングがIP修飾子エントリで設定されている場合はスワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`
ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

の詳細については `vserver name-mapping`、を"ONTAPコマンド リファレンス"参照してください。

マルチドメインネームマッピング検索の設定

ONTAP SMBマルチドメインネームマッピングの検索を有効または無効にする

マルチドメインネームマッピングの検索では、 UNIX ユーザから Windows ユーザへのネームマッピングを設定するときに、 Windows 名のドメイン部分にワイルドカード（ * ）を使用できます。名前のドメイン部分にワイルドカード（ * ）を使用すると、 ONTAP で、 CIFS サーバのコンピュータアカウントが含まれるドメインと双方向の信頼関係が確立されているすべてのドメインを検索できるようになります。

タスクの内容

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。信頼できるドメインのリストを設定すると、ONTAPは双方向の信頼関係が確立された検出ドメインの代わりに、信頼できるドメインのリストを使用してマルチドメインネームマッピングの検索を実行します。

- マルチドメインネームマッピングの検索は、デフォルトで有効になっています。
- このオプションは、advanced権限レベルで使用できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

マルチドメインネームマッピングの検索の設定	入力するコマンド
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`

マルチドメインネームマッピングの検索の設定	入力するコマンド
無効にする	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

利用可能なサーバーオプション

信頼できるONTAP SMBドメインのリセットと再検出

すべての信頼できるドメインを強制的に再検出することができます。これは、信頼できるドメインサーバが適切に応答しない場合や、信頼関係が変更された場合に役立ちます。ホームドメイン（CIFSサーバのコンピュータアカウントを含むドメイン）と双方向の信頼関係が確立されたドメインのみが検出されます。

ステップ

1. コマンドを使用して、信頼できるドメインをリセットして再検出し `vserver cifs domain trusts rediscover` ます。

```
vserver cifs domain trusts rediscover -vserver vs1
```

関連情報

検出された信頼できるドメインに関する情報を表示する

検出された信頼できるONTAP SMBドメインに関する情報を表示する

CIFSサーバのホームドメイン（CIFSサーバのコンピュータアカウントが含まれているドメイン）で検出された信頼できるドメインに関する情報を表示できます。この情報は、検出された信頼できるドメインと、検出された信頼できるドメインのリスト内でのそれらの順序を確認する場合に役立ちます。

タスクの内容

ホームドメインと双方向の信頼関係が確立されたドメインのみが検出されます。ホームドメインのドメインコントローラ（DC）は、信頼できるドメインのリストをDCが決定した順序で返すため、リスト内のドメインの順序を予測することはできません。信頼できるドメインのリストを表示することで、マルチドメインネームマッピングの検索での検索順序を確認できます。

表示される信頼できるドメインの情報は、ノードおよびStorage Virtual Machine（SVM）別にグループ化されます。

ステップ

1. コマンドを使用して、検出された信頼できるドメインに関する情報を表示します `vserver cifs domain trusts show`。

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

関連情報

信頼できるドメインのリセットと再検出

優先リスト内の信頼できる**ONTAP SMB**ドメインの追加、削除、交換

SMBサーバの信頼できるドメインの優先リストに対して信頼できるドメインを追加または削除したり、現在のリストを変更したりできます。信頼できるドメインの優先リストを設定すると、マルチドメインネームマッピングの検索を実行するときに、検出された双方向の信頼できるドメインの代わりにこのリストが使用されます。

タスクの内容

- 信頼できるドメインを既存のリストに追加する場合は、新しいリストが既存のリストにマージされ、新しいエントリが末尾に追加されます。信頼できるドメインは、リスト内の順序で検索されます。
- 信頼できるドメインを既存のリストから削除する際にリストを指定しないと、指定したStorage Virtual Machine（SVM）の信頼できるドメインのリスト全体が削除されます。
- 信頼できるドメインの既存のリストを変更すると、新しいリストで上書きされます。

> 信頼できるドメインのリストには、双方向の信頼関係が確立されたドメインだけを入力してください。アウトバウンドまたはインバウンドの信頼ドメインを優先ドメインリストに入力することはできますが、マルチドメインネームマッピングの検索では使用されません。ONTAPは単方向ドメインのエントリをスキップし、リスト内の次の双方向の信頼関係が確立されたドメインに移動します。

ステップ

1. 次のいずれかを実行します。

信頼できるドメインのリストに対して行う操作	使用するコマンド
信頼できるドメインをリストに追加する	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
信頼できるドメインをリストから削除する	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
既存のリストを変更する	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

例

次のコマンドは、SVM vs1で使用される信頼できるドメインの優先リストに2つの信頼できるドメイン（cifs1.example.comおよびcifs2.example.com）を追加します。

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1で使用されるリストから信頼できるドメインを2つ削除します。

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1で使用される信頼できるドメインのリストを変更します。元のリストが新しいリストに置き換えられます。

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

関連情報

優先信頼ドメインリストに関する情報を表示する

信頼できる**ONTAP**の優先**SMB**ドメインリストに関する情報を表示する

信頼できるドメインの優先リストに含まれている信頼できるドメインに関する情報、およびマルチドメインネームマッピングの検索が有効な場合の信頼できるドメインの検索順序に関する情報を表示できます。自動検出された信頼できるドメインの優先リストを使用する代わりに、信頼できるドメインの優先リストを設定することもできます。

手順

1. 次のいずれかを実行します。

表示する情報	使用するコマンド
Storage Virtual Machine（SVM）別にグループ化されたクラスタ内のすべての信頼できる優先ドメイン	`vserver cifs domain name-mapping-search show`
指定したSVMのすべての信頼できる優先ドメイン	`vserver cifs domain name-mapping-search show -vserver vserver_name`

次のコマンドは、クラスタ上のすべての信頼できる優先ドメインに関する情報を表示します。

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
--------------  ---------------------------------
vs1              CIFS1.EXAMPLE.COM
```

関連情報

優先リスト内の信頼できるドメインを追加、削除、または置換する

SMB共有の作成と設定

ONTAP SMB共有の作成と設定の詳細

ユーザやアプリケーションがSMB経由でCIFSサーバ上のデータにアクセスできるようにするには、SMB共有を作成して設定する必要があります。SMB共有は、ボリューム内の指定されたアクセスポイントです。共有をカスタマイズするには、共有パラメータと共有プロパティを指定します。既存の共有はいつでも変更できます。

SMB共有を作成すると、すべてのメンバーにフルコントロール権限が設定されたACLがONTAPによってデフォルトで作成されます。

SMB共有は、Storage Virtual Machine（SVM）上のCIFSサーバに関連付けられます。SVMが削除された場合、または関連付けられているCIFSサーバがSVMから削除された場合、SMB共有は削除されます。SVMにCIFSサーバを再作成する場合は、SMB共有を再作成する必要があります。

関連情報

- ローカルユーザーとグループについて学ぶ
- "Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"
- ボリューム上のファイル名変換の文字マッピングを構成する

デフォルトの管理ONTAP SMB共有の詳細

Storage Virtual Machine（SVM）上にCIFSサーバを作成すると、デフォルトの管理共有が自動的に作成されます。これらのデフォルトの共有とその用途について理解しておく

必要があります。

CIFSサーバを作成すると、ONTAPによって次のデフォルトの管理共有が作成されます。

ONTAP 9 .8以降では、admin$共有はデフォルトで作成されなくなりました。

- IPC$
- admin$（ONTAP 9.7以前のみ）
- c$

$文字で終わる共有は非表示の共有であるため、デフォルトの管理共有は[マイコンピュータ]には表示されませんが、[共有フォルダ]を使用して表示できます。

ipc$**および**admin$デフォルト共有の使用方法

ipc$共有とadmin$共有はONTAPが使用するものであり、Windows管理者がSVM上のデータにアクセスするために使用することはできません。

- ipc$共有

  ipc$共有は、プログラム間の通信に不可欠な名前付きパイプを共有するリソースです。ipc$共有は、コンピュータのリモート管理中およびコンピュータの共有リソースを表示するときに使用されます。ipc$共有の共有設定、共有プロパティ、ACLは変更できません。また、ipc$共有の名前を変更したり削除したりすることもできません。

- admin$共有（ONTAP 9.7以前のみ）

  ONTAP 9 .8以降では、admin$共有はデフォルトで作成されなくなりました。

  admin$共有は、SVMのリモート管理に使用されます。このリソースのパスは、常にSVMルートへのパスです。admin$共有の共有設定、共有プロパティ、ACLは変更できません。また、admin$共有の名前変更や削除もできません。

c$テフオルトキヨウユウノシヨウホウホウ

c$共有は、クラスタ管理者またはSVM管理者がSVMルートボリュームへのアクセスと管理に使用できる管理共有です。

c$共有の特徴は次のとおりです。

- この共有のパスは、常にSVMルートボリュームへのパスであり、変更することはできません。
- c$共有のデフォルトのACLは、Administrator/Full Controlです。

  このユーザはBUILTIN\administratorです。デフォルトでは、BUILTIN\administratorを共有にマッピングし、マッピングされたルートディレクトリ内のファイルやフォルダを表示、作成、変更、削除できます。このディレクトリ内のファイルとフォルダを管理する場合は、注意が必要です。

- c$共有のACLは変更できます。
- c$共有設定と共有プロパティを変更できます。

- c$共有は削除できません。
- SVM管理者は、ネームスペースジャンクションを横断することで、マッピングされたc$共有から残りのSVMネームスペースにアクセスできます。
- c$共有には、Microsoft管理コンソールを使用してアクセスできます。

関連情報

Windows セキュリティ タブを使用して詳細なファイル権限を構成する

ONTAP SMB共有の命名要件の詳細

SMBサーバでSMB共有を作成するときは、ONTAP共有の命名要件に注意してください。

ONTAPの共有の命名規則はWindowsの命名規則と同じで、次の要件があります。

- 各共有名はSMBサーバで一意である必要があります。
- 共有名では大文字と小文字は区別されません。
- 共有名の最大文字数は80文字です。
- 共有名はUnicodeに対応しています。
- $文字で終わる共有名は非表示の共有です。
- ONTAP 9 .7以前の場合、admin$、ipc$、およびc$管理共有はすべてのCIFSサーバで自動的に作成され、共有名が予約されています。ONTAP 9 .8以降では、admin$共有は自動的に作成されなくなりました。
- 共有の作成時に共有名ONTAP _ ADMIN$を使用することはできません。
- 共有名ではスペースの使用がサポートされます。
  - 共有名の先頭または末尾の文字をスペースにすることはできません。
  - スペースを含む共有名は引用符で囲む必要があります。

    単一引用符は共有名の一部とみなされ、引用符の代わりに使用することはできません。

- SMB共有の名前では次の特殊文字がサポートされます。

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- SMB共有の名前では、次の特殊文字はサポートされません。

```
** [ ] " / \ : ; | < > , ? * =
```

マルチプロトコル環境で共有を作成する際の**ONTAP SMB**ディレクトリの大文字と小文字の区別に関する要件

名前に大文字と小文字の違いしかないディレクトリ名を区別するために 8.3 の命名方法が使用されている SVM に共有を作成する場合は、クライアントが必要なディレクトリ

パスに接続できるように共有パスに 8.3 の名前を使用する必要があります。

次の例では、 Linux クライアント上に「 testdir 」と「 testdir 」という名前の 2 つのディレクトリが作成されています。ディレクトリを含むボリュームのジャンクションパスは、です `/home`。最初の出力は Linux クライアントで、 2 番目の出力は SMB クライアントで行います。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

2 番目のディレクトリへの共有を作成する場合、共有パスに 8.3 の名前を使用する必要があります。この例では、最初のディレクトリの共有パスはで `/home/testdir`、2番目のディレクトリの共有パスはです `/home/TESTDI~1`。

SMB共有プロパティを使用する

ONTAP SMB共有プロパティの使用方法

SMB 共有のプロパティをカスタマイズすることができます。

使用可能な共有プロパティは次のとおりです。

共有プロパティ	説明
`oplocks`	共有で便宜的ロック（クライアント側キャッシュ）を使用することを指定します。
`browsable`	Windowsクライアントが共有を参照することを許可します。
`showsnapshot`	クライアントがスナップショットを表示およびトラバースできることを指定します。
`changenotify`	共有が変更通知要求をサポートすることを指定します。SVM 上の共有では、これはデフォルトの初期プロパティです。

共有プロパティ	説明
attributecache	属性にすばやくアクセスできるように SMB 共有でのファイル属性のキャッシュを有効にします。デフォルトでは、属性のキャッシュは無効になっています。このプロパティは、 SMB 1.0 経由で共有に接続するクライアントがある場合にのみ有効にしてください。クライアントが SMB 2.x または SMB 3.0 経由で共有に接続している場合、この共有プロパティは適用されません。
continuously-available	このプロパティは、サポートするSMBクライアントが永続的な方法でファイルを開くことを許可します。この方法で開いたファイルは、フェイルオーバーやギブバックなど、システムを停止させるイベントから保護されます。
branchcache	共有内のファイルに対するBranchCacheハッシュの要求をクライアントに許可します。このオプションが役立つのは、 CIFS の BranchCache 設定で動作モードとして「共有ごと」を指定した場合だけです。
access-based-enumeration	このプロパティは、この共有で _ アクセスベースの列挙 _ （ ABE ）を有効にするように指定します。ABEでフィルタリングされた共有フォルダは、個 々 のユーザのアクセス権に基づいてユーザに表示されるため、ユーザがアクセス権を持っていないフォルダやその他の共有リソースは表示されません。
namespace-caching	共有に接続するSMBクライアントが、CIFSサーバから返されるディレクトリの列挙結果をキャッシュできることを指定します。これにより、パフォーマンスが向上します。デフォルトでは、 SMB 1 のクライアントはディレクトリの列挙結果をキャッシュしません。SMB 2 および SMB 3 クライアントはデフォルトでディレクトリ列挙結果をキャッシュするため、この共有プロパティを指定してパフォーマンスが向上するのは SMB 1 クライアント接続のみです。
encrypt-data	この共有へのアクセス時にSMB暗号化を使用する必要があることを指定します。SMB データへのアクセスで暗号化をサポートしていない SMB クライアントは、この共有にアクセスできません。

既存の**ONTAP SMB**共有に対する共有プロパティの追加または削除

共有プロパティを追加または削除することで、既存のSMB共有をカスタマイズできます。これは、環境内の要件の変化に合わせて共有設定を変更する場合に便利です。

開始する前に

プロパティを変更する共有が存在している必要があります。

タスクの内容

共有プロパティの追加に関するガイドラインは次のとおりです。

- カンマで区切って1つ以上の共有プロパティを追加できます。
- 以前に指定した共有プロパティは有効なままです。

  新しく追加したプロパティは、既存の共有プロパティのリストに追加されます。

- 共有にすでに適用されている共有プロパティに新しい値を指定した場合は、元の値が新たに指定した値に置き換えられます。
- コマンドを使用して共有プロパティを削除することはできません `vserver cifs share properties add`。

  共有プロパティを削除するには、コマンドを使用し `vserver cifs share properties remove`ます。

共有プロパティの削除に関するガイドラインは次のとおりです。

- カンマで区切って1つ以上の共有プロパティを削除できます。
- 以前に指定した共有プロパティは、削除しないかぎり有効なままです。

手順

1. 該当するコマンドを入力します。

状況	入力するコマンド
共有プロパティを追加する	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
共有プロパティを削除する	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 共有プロパティの設定を確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドを実行すると、SVM vs1上の「`share1`」という名前の共有に共有プロパティが追加され `showsnapshot`ます。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share1   /share1    oplocks      -          Everyone / Full
Control
                               browsable
                               changenotify
                               showsnapshot
```

次のコマンドは、SVM vs1上の「`share2'」という名前の共有から共有プロパティを削除し`browsable`ます。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share2   /share2    oplocks      -          Everyone / Full
Control
                               changenotify
```

関連情報

共有を管理するためのコマンド

force-group共有設定を使用した**ONTAP SMB**ユーザアクセスの最適化

ONTAP コマンドラインから、 UNIX 対応のセキュリティを使用するデータへの共有を作成するときに、 SMB ユーザがその共有内に作成するすべてのファイルが、 *force-group* と呼ばれる同じグループに属するように指定できます。このグループは、 UNIX グループデータベースで事前に定義されている必要があります。force-groupを使用すると、さまざまなグループに属するSMBユーザがファイルにアクセスできるようになります。

force-groupの指定が意味を持つのは、共有がUNIXまたはmixed qtree内にある場合のみです。NTFSボリュームまたはqtreeの共有内のファイルへのアクセスはUNIXのGIDではなくWindows権限によって決定されるため、これらの共有にforce-groupを設定する必要はありません。

共有にforce-groupが指定されている場合、共有は次のようになります。

- この共有にアクセスするforce-group内のSMBユーザは、force-groupのGIDに一時的に変更されます。

  このGIDを使用すると、プライマリGIDまたはUIDでは通常アクセスできない共有内のファイルにアクセスできます。

- SMBユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリGIDに関係なく、同じforce-groupに属します。

SMBユーザがNFSで作成されたファイルにアクセスしようとすると、SMBユーザのプライマリGIDによってアクセス権が決定されます。

force-groupは、NFSユーザがこの共有内のファイルにアクセスする方法には影響しません。NFSで作成されたファイルは、ファイル所有者からGIDを取得します。アクセス権限は、ファイルにアクセスしようとしているNFSユーザのUIDとプライマリGIDに基づいて決定されます。

force-groupを使用すると、さまざまなグループに属するSMBユーザがファイルにアクセスできるようになります。たとえば、会社の Web ページを保存する共有を作成し、 Engineering グループと Marketing グループのユーザに書き込みアクセス権を付与する必要がある場合、共有を作成して、「 webgroup1 」という名前の force-group に書き込み権限を与えます。force-group が指定されているため、 SMB ユーザがこの共有内に作成するすべてのファイルは「 webgroup1 」グループによって所有されます。また、ユーザが共有にアクセスするときは、「 webgroup1 」グループの GID が自動的に割り当てられます。その結果、すべてのユーザがこの共有に書き込むことができます。エンジニアリング部門とマーケティング部門のユーザのアクセス権を管理する必要はありません。

関連情報

強制グループ共有設定で共有を作成する

force-group共有設定を使用して**ONTAP SMB**共有を作成する

UNIXファイルセキュリティ形式のボリュームまたはqtree上のデータにアクセスするSMBユーザが、ONTAPで同じUNIXグループに属しているとみなされるようにするには、force-group共有設定を使用してSMB共有を作成します。

ステップ

1. SMB共有を作成します。 `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   (`\\servername\sharename\filepath`共有のUNCパスの文字数が256文字を超えている場合（UNCパスの先頭の""は除く\\）、Windowsの[プロパティ]ボックスの*[セキュリティ]*タブは使用できません。これは、ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないでください。

   共有の作成後にforce-groupを削除する場合は、いつでも共有を変更し、パラメータの値として空の文字列（""）を指定でき`-force-group-for-create`ます。共有を変更してforce-groupを削除した場合、この共有への既存のすべての接続には、引き続き以前に設定されたforce-groupがプライマリGIDとして使用されます。

例

次のコマンドは、SMBユーザが作成するすべてのファイルがwebgroup1グループに割り当てられるディレクトリに、Webからアクセス可能な「webpages」共有を作成し`/corp/companyinfo`ます。

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

関連情報

強制グループ共有設定でユーザーアクセスを最適化する

Microsoft 管理コンソール（ MMC ）を使用して SVM の SMB 共有情報を表示し、いくつかの管理タスクを実行できます。共有を表示する前に、 MMC を SVM に接続する必要があります。

タスクの内容

MMC を使用すると、 SVM 内の共有に対して次のタスクを実行できます。

- 共有を表示します
- アクティブなセッションを表示します
- 開いているファイルを表示します
- システムのセッション、ファイル、およびツリー接続のリストを列挙します
- 開いているファイルを閉じます
- 開いているセッションを閉じます
- 共有を作成 / 管理します

> 上記の機能によって表示されるビューは、クラスタではなくノードに固有のものです。そのため、 MMC を使用して SMB サーバホスト名（ cifs01.domain.local ）に接続すると、 DNS の設定に基づいてクラスタ内の単一の LIF にルーティングされます。

次の機能は、 MMC for ONTAP ではサポートされていません。

- 新しいローカルユーザ / グループを作成しています
- 既存のローカルユーザ / グループの管理 / 表示
- イベントまたはパフォーマンスログを表示する
- ストレージ
- サービスとアプリケーション

サポートされていない処理では、エラーが発生することがあり `remote procedure call failed`ます。

"FAQ ： ONTAP で Windows MMC を使用する"

手順

1. 任意の Windows サーバーでコンピュータの管理 MMC を開くには、 [コントロールパネル] で、 [管理ツール *]>[コンピュータの管理 *] を選択します。
2. 「 * アクション * > * 別のコンピューターに接続 * 」を選択します。

   [コンピュータの選択] ダイアログボックスが表示されます。
3. ストレージ・システムの名前を入力するか、または * Browse * をクリックしてストレージ・システムを検索します。
4. [OK]*をクリックします。

   MMC が SVM に接続します。

5. ナビゲーションペインで、 * 共有フォルダ * > * 共有 * をクリックします。

   右側の表示ペインに SVM の共有のリストが表示されます。

6. 共有の共有プロパティを表示するには、共有をダブルクリックして * プロパティ * ダイアログボックスを開きます。
7. MMC を使用してストレージシステムに接続できない場合は、ストレージシステムで次のいずれかのコマンドを使用して、 BUILTIN\Administrators グループまたは BUILTIN\Power Users グループにユーザを追加できます。

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

SMB共有の管理用ONTAPコマンド

SMB共有を管理するには、コマンドと `vserver cifs share properties`コマンドを使用し `vserver cifs share`ます。

状況	使用するコマンド
SMB共有を作成する	`vserver cifs share create`
SMB共有を表示する	`vserver cifs share show`
SMB共有を変更する	`vserver cifs share modify`
SMB共有を削除する	`vserver cifs share delete`
既存の共有に共有プロパティを追加する	`vserver cifs share properties add`
既存の共有から共有プロパティを削除する	`vserver cifs share properties remove`
共有プロパティに関する情報を表示する	`vserver cifs share properties show`

の詳細については `vserver cifs`、を"ONTAPコマンド リファレンス"参照してください。

SMB共有のACLを使用したファイルアクセスの保護

ONTAP SMB共有レベルACLの管理について

共有レベルの ACL を変更すると、共有に設定するアクセス権を強化したり、軽減したりできます。Windows のユーザとグループまたは UNIX のユーザとグループのいずれかを

使用して共有レベルの ACL を設定できます。

デフォルトでは、共有レベルのACLはEveryoneという標準グループにフルコントロールを付与します。ACLでフルコントロールが付与されているということは、ドメイン内のすべてのユーザーとすべての信頼ドメインに共有へのフルアクセス権限が付与されることを意味します。共有レベルのACLのアクセスレベルは、WindowsクライアントのMicrosoft管理コンソール（MMC）またはONTAPコマンドラインを使用して制御できます。"共有アクセス制御リストを作成する"です。

MMC を使用する際には、次の点に留意してください。

- 指定するユーザ名およびグループ名はWindows名である必要があります。
- Windows の権限だけを指定できます。

ONTAP コマンドラインを使用する際には、次の点に留意してください。

- ユーザ名およびグループ名には、 Windows 名または UNIX 名を使用できます。

  ACL の作成時または変更時に指定されない場合、デフォルトのタイプは Windows のユーザとグループです。

- Windows の権限だけを指定できます。

ONTAP SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List（ACL；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前、またはUNIXユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があり `Everyone / Full Control`ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。'vserver cifs share access-control delete -vserver <vserver_name>-share <share_name>-user-or-group everyone'
2. 新しいACLを設定します。

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIXユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIXグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com」SVM上の「sales」共有に対するWindowsグループ「sales Team」に権限を付与します `Change`。

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

次のコマンドは `Read`、「vs2.example.com」SVM上の「eng」共有に対して「engineering」UNIXグループに権限を付与します。

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

次のコマンドは `Change Full_Control`、SVM「vs1」上の「datavol5」共有に対して「Tiger Team」という名前のローカルWindowsグループに権限と「Sue Chang」という名前のローカルWindowsユーザに権限を付与します。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

SMB共有アクセス制御リストを管理するための**ONTAP**コマンド

Access Control List（ACL；アクセス制御リスト）の作成、表示、変更、削除など、SMBのAccess Control List（ACL；アクセス制御リスト）を管理するためのコマンドについて説明します。

状況	使用するコマンド
新しいACLを作成する	`vserver cifs share access-control create`
ACL を表示します	`vserver cifs share access-control show`
ACL を変更します	`vserver cifs share access-control modify`
ACL を削除します	`vserver cifs share access-control delete`

ファイル権限を使用したファイルアクセスの保護

ONTAP SMB SVMの**Windows**セキュリティタブを使用して、高度な**NTFS**ファイル権限を設定します。

Windows の [プロパティ] ウィンドウの [Windows セキュリティ *] タブを使用して、ファイルおよびフォルダの標準 NTFS ファイルアクセス権を構成できます。

開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

タスクの内容

NTFSファイル権限を設定するには、Windowsホストで、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。これらのタスクはWindows GUIで自動的に処理されます。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
2. [* ネットワークドライブの割り当て *] ダイアログボックスに入力します。
   a. ドライブ文字を選択します。
   b. [* フォルダ *] ボックスに、権限を適用するデータと共有名を含む共有を含む CIFS サーバー名を入力します。

      CIFSサーバ名が「CIFS_SERVER」で、共有の名前が「'share1'」の場合は、と入力します。
      `\\CIFS_SERVER\share1`

      CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

   c. [完了] をクリックします。

選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

3. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
5. [* セキュリティ *] タブを選択します。

   Security タブには、 NTFS アクセス権が設定されているユーザーおよびグループのリストが表示されます。[* アクセス許可の対象 *] ボックスには、選択した各ユーザーまたはグループに対して有効な [許可] と [拒否] のアクセス許可のリストが表示されます。

6. 「 * 詳細設定 * 」をクリックします。

   Windowsの[プロパティ]ウィンドウには、ユーザおよびグループに割り当てられている既存のファイル権限に関する情報が表示されます。

7. [権限の変更 *] をクリックします。

   [権限]ウィンドウが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループの詳細なNTFS権限を設定する	a. [追加]*をクリックします。 b. [* 選択するオブジェクト名を入力してください *] ボックスに、追加するユーザーまたはグループの名前を入力します。 c. [OK]*をクリックします。
ユーザまたはグループの詳細なNTFS権限を変更する	a. [* アクセス権エントリ： *] ボックスで、詳細なアクセス権を変更するユーザーまたはグループを選択します。 b. [編集（ Edit ）] をクリックします。
ユーザまたはグループの詳細なNTFS権限を削除する	a. [* アクセス許可エントリ： *] ボックスで、削除するユーザーまたはグループを選択します。 b. [削除（ Remove ）] をクリックします。 c. 手順13に進みます。

   新しいユーザまたはグループに詳細な NTFS 権限を追加する場合、または既存のユーザまたはグループの NTFS 詳細権限を変更する場合は、 <Object> の権限エントリボックスが開きます。

9. [* 適用先 *] ボックスで、この NTFS ファイル許可エントリを適用する方法を選択します。

   1 つのファイルに NTFS ファイル権限を設定する場合、 * Apply to * ボックスはアクティブになりません。[* 適用先 * （ Apply to * ）] 設定のデフォルトは、 * このオブジェクトのみ * です。

10. [* アクセス許可 *] ボックスで、このオブジェクトに設定する詳細なアクセス許可の [* 許可 *] または [* 拒否 *] ボックスを選択します。

- 指定したアクセスを許可するには、 * 許可 * ボックスを選択します。
- 指定されたアクセスを許可しない場合は、 * Deny * ボックスを選択します。次の詳細な権限に対して権限を設定できます。
- * フルコントロール *

  この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます（それらの権限が許可または拒否されます）。

- * フォルダの移動 / ファイルの実行 *
- * フォルダのリスト / データの読み取り *
- * 属性の読み取り *
- * 拡張属性の読み取り *
- * ファイルの作成 / データの書き込み *
- * フォルダの作成 / データの追加 *
- * 属性の書き込み *
- * 拡張属性の書き込み *
- * サブフォルダとファイルの削除 *
- * 削除 *
- * 読み取り許可 *
- * 権限の変更 *
- * 所有権を取りなさい *

  いずれかの詳細な権限ボックスが選択できない場合は、権限が親オブジェクトから継承されるためです。

11. このオブジェクトのサブフォルダとファイルにこれらのアクセス権を継承させる場合は、 [このコンテナ内のオブジェクトまたはコンテナにこれらのアクセス権を適用する *] ボックスをオンにします。
12. [OK]*をクリックします。
13. NTFS権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。
    - [このオブジェクトの親から継承可能な権限を含める *] ボックスをオンにします。

      これがデフォルトです。

    - [このオブジェクトから継承可能な権限ですべての子オブジェクトを置換する *] ボックスをオンにします。

      この設定は、単一ファイルに対してNTFSファイル権限を設定する場合は[権限]ボックスに表示されません。

この設定を選択する場合は注意が必要です。この設定では、すべての子オブジェクトに対する既存の権限がすべて削除され、このオブジェクトの権限設定に置き換えられます。削除したくない権限を誤って削除する可能性があります。これは、mixedセキュリティ形式のボリュームまたはqtreeで権限を設定する場合に特に重要です。子オブジェクトがUNIX対応のセキュリティ形式を使用している場合に、これらの子オブジェクトにNTFSアクセス権を適用すると、ONTAPによってこれらのオブジェクトがUNIXセキュリティ形式からNTFSセキュリティ形式に変更され、これらの子オブジェクトのすべてのUNIXアクセス権がNTFSアクセス権に置き換えられます。

- 両方のボックスを選択します。
- どちらのボックスも選択しない。

14. **OK** をクリックして、 *Permissions * ボックスを閉じます。
15. OK * をクリックして、 * <Object>* の高度なセキュリティ設定ボックスを閉じます。

詳細なNTFS権限の設定方法の詳細については、Windowsのマニュアルを参照してください。

関連情報

- サーバーにNTFSセキュリティ記述子を作成する
- NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示
- mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示
- UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

SMB NTFSファイル権限用の**ONTAP**コマンド

ONTAP CLIを使用して、ファイルおよびディレクトリに対してNTFSファイル権限を設定できます。これにより、WindowsクライアントでSMB共有を使用してデータに接続することなくNTFSファイル権限を設定できます。

NTFSファイル権限を設定するには、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。

コマンドラインを使用して設定できるのはNTFSファイル権限のみです。CLIを使用してNFSv4 ACLを設定することはできません。

手順

1. NTFSセキュリティ記述子を作成します。

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. NTFSセキュリティ記述子にDACLを追加します。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
```

```
{this-folder|sub-folders|files}
```

3. ファイルやディレクトリのセキュリティポリシーを作成します。

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

ONTAP SMBサーバ経由でファイルにアクセスする際のアクセス制御を提供する**UNIX**ファイル権限について学習します。

FlexVol ボリュームのセキュリティ形式は、 NTFS 、 UNIX 、 mixed の 3 種類のいずれかにすることができます。セキュリティ形式に関係なく SMB 経由でデータにアクセスできますが、 UNIX 対応のセキュリティを使用するデータにアクセスするには、適切な UNIX ファイル権限が必要になります。

SMB 経由でのデータへのアクセス時には、いくつかのアクセス制御を使用して、要求した操作を実行する権限がユーザにあるかどうかが判断されます。

- エクスポート権限

  SMB アクセスに関するエクスポート権限の設定はオプションです。

- 共有権限
- ファイル権限

  ユーザが操作を実行するデータには、次のタイプのファイル権限を適用できます。

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX モードビット

NFSv4 ACL または UNIX モードビットが設定されたデータの場合は、 UNIX 形式のアクセス権を使用してデータへのファイルアクセス権が決定されます。SVM 管理者は、適切なファイル権限を設定して、ユーザに目的のアクションを実行する権限が付与されるようにする必要があります。

mixed セキュリティ形式のボリューム内のデータでは、 NTFS または UNIX 対応のセキュリティ形式を使用できます。UNIX 対応のセキュリティ形式を使用するデータの場合は、データに対するファイル権限を判断するときに NFSv4 権限または UNIX モードビットが使用されます。

ダイナミックアクセス制御（**DAC**）を使用したファイルアクセスの保護

ONTAP SMBサーバの**DAC**ファイルアクセスセキュリティについて学ぶ

ダイナミックアクセス制御を使用してアクセスを保護できます。Active Directoryで集約型アクセスポリシーを作成し、適用されたGPOを使用してSVM上のファイルとフォルダにそのポリシーを適用します。集約型アクセスポリシーのステージングイベントを使用するように監査を設定すると、集約型アクセスポリシーの変更を適用する前にその影響を確認できます。

CIFSクレデンシャルへの追加

ダイナミックアクセス制御が導入される前は、CIFSクレデンシャルにセキュリティプリンシパル（ユーザ）のIDとWindowsグループメンバーシップが含まれていました。ダイナミックアクセス制御では、さらに3種類の情報（デバイスID、デバイス要求、およびユーザ要求）がクレデンシャルに追加されます。

- デバイスID

  ユーザーのID情報と類似していますが、ユーザーがログインしているデバイスのIDとグループメンバーシップが異なります。

- デバイスの信頼性

  デバイスセキュリティプリンシパルに関するアサーション。たとえば、デバイスが特定のOUのメンバーであることが要求される場合があります。

- ユーザの信頼性

  ユーザセキュリティプリンシパルに関するアサーション。たとえば、ADアカウントが特定のOUのメンバーであることをユーザが要求する場合があります。

集約型アクセスポリシー

ファイルの集約型アクセスポリシーを使用すると、ユーザグループ、ユーザ要求、デバイス要求、およびリソースプロパティを使用した条件式を含む許可ポリシーを一元的に導入および管理できます。

たとえば、ビジネスに影響の大きいデータにアクセスするには、フルタイムの従業員であり、管理対象デバイスからのみデータにアクセスできる必要があります。集約型アクセスポリシーはActive Directoryで定義され、GPOメカニズムを介してファイルサーバに配布されます。

高度な監査を使用した集約型アクセスポリシーのステージング

集約型アクセスポリシーは「集約型」にすることができます。この場合、ファイルアクセスチェック時に「what if 」方式で評価されます。ポリシーが有効になっていた場合に発生した結果、および現在の設定とどのように異なるかが監査イベントとして記録されます。このようにして、管理者は、実際にポリシーを有効にする前に、監査イベントログを使用してアクセスポリシーの変更による影響を調べることができます。アクセスポリシーの変更による影響を評価したら、GPOを使用して目的のSVMにポリシーを導入できます。

関連情報

- サポートされているGPOについて学ぶ
- SMBサーバーにグループポリシーオブジェクトを適用する方法について学習します
- サーバー上の GPO サポートを有効または無効にする
- GPO構成に関する情報を表示する
- 集中アクセスポリシーに関する情報を表示する
- 集中アクセスポリシールールに関する情報を表示する
- サーバー上のデータを保護するための集中アクセスポリシーを構成する
- サーバーのセキュリティに関する情報を表示する
- "SMBおよびNFSの監査とセキュリティトレース"

CIFSサーバでダイナミックアクセス制御（DAC）を使用する場合は、ONTAPがActive Directory環境でどのようにダイナミックアクセス制御機能をサポートするかを理解しておく必要があります。

ダイナミックアクセス制御でサポート

CIFSサーバでダイナミックアクセス制御が有効になっている場合、ONTAPは次の機能をサポートします。

機能	コメント
ファイルシステムへの要求	クレームは単純な名前と値のペアで、ユーザーについての真実を記述します。ユーザクレデンシャルにはクレーム情報が含まれており、ファイルのセキュリティ記述子はクレームチェックを含むアクセスチェックを実行できます。これにより、管理者は誰がファイルにアクセスできるかをより細かく制御できます。
ファイルアクセスチェック用の条件式	ファイルのセキュリティパラメータを変更する場合、ユーザは任意に複雑な条件式をファイルのセキュリティ記述子に追加できます。条件式には、クレームのチェックを含めることができます。
集約型アクセスポリシーによるファイルアクセスの一元管理	集約型アクセスポリシーは、Active Directoryに格納されるACLの一種で、ファイルへのタグ付けが可能です。ファイルへのアクセスは、ディスクのセキュリティ記述子とタグ付けされた集約型アクセスポリシーの両方のアクセスチェックでアクセスが許可されている場合にのみ許可されます。これにより、管理者は、ディスクのセキュリティ記述子を変更することなく、一元的な場所（AD）からファイルへのアクセスを制御できます。
集約型アクセスポリシーのステージング	集約型アクセスポリシーへの変更を「集約型アクセスポリシー」し、監査レポートで変更の影響を確認することで、実際のファイルアクセスに影響を与えずにセキュリティの変更を試す機能を追加します。
ONTAP CLIを使用した集約型アクセスポリシーセキュリティに関する情報の表示のサポート	コマンドを拡張し `vserver security file-directory show`て、適用されている集約型アクセスポリシーに関する情報を表示します。
集約型アクセスポリシーを含むセキュリティトレース	コマンドファミリーを拡張し、 `vserver security trace`適用されている集約型アクセスポリシーに関する情報を含む結果を表示します。

ダイナミックアクセス制御でサポートされない

CIFSサーバでダイナミックアクセス制御が有効になっている場合、ONTAPは次の機能をサポートしません。

機能	コメント
NTFSファイルシステムオブジェクトの自動分類	これは、ONTAPでサポートされていないWindowsファイル分類インフラストラクチャの拡張機能です。
集約型アクセスポリシーのステージング以外の高度な監査	高度な監査では、集約型アクセスポリシーのステージングのみがサポートされます。

ONTAP SMBサーバーで**DAC**と集中アクセスポリシーを使用する方法について学習します

CIFS サーバ上のファイルとフォルダを保護するために Dynamic Access Control （ DAC ；ダイナミックアクセス制御）と集約型アクセスポリシーを使用する際は、一定の考慮事項に注意する必要があります。

ポリシールール「環境 **domain\administrator user** 」の場合、 **root** に対して **NFS** アクセスが拒否されることがあります

特定の状況では、 root ユーザがアクセスしようとしているデータに集約型アクセスポリシーセキュリティが適用されていると、 root に対して NFS アクセスが拒否されることがあります。問題は、集約型アクセスポリシーに domain\administrator に適用されるルールが含まれており、 root アカウントが domain\administrator アカウントにマッピングされている場合に実行されます。

domain\administrator ユーザにルールを適用する代わりに、 domain\administrators グループなど、管理者権限を持つグループにルールを適用してください。これにより、 root を domain\administrator アカウントにマッピングしても、 root はこの問題の影響を受けなくなります。

適用された集約型アクセスポリシーが**Active Directory**に見つからないと、**CIFS**サーバの**BUILTIN\Administrators**グループにリソースへのアクセスが許可されます

CIFS サーバに格納されたリソースに集約型アクセスポリシーが適用されている場合に、 CIFS サーバが集約型アクセスポリシーの SID を使用して Active Directory から情報を取得しようとしても、 SID が Active Directory 内の既存の集約型アクセスポリシーの SID と一致しないことがあります。このような場合、 CIFS サーバはそのリソースにローカルのデフォルトのリカバリポリシーを適用します。

ローカルのデフォルトのリカバリポリシーでは、 CIFS サーバの BUILTIN\Administrators グループにそのリソースへのアクセスが許可されます。

ONTAP SMBサーバの**DAC**を有効または無効にする

ダイナミックアクセス制御（DAC）を使用してCIFSサーバ上のオブジェクトを保護できるオプションは、デフォルトでは無効になっています。CIFSサーバでダイナミックアクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFSサーバに格納されたオブジェクトの保護にダイナミックアクセス制御を使用しない場合は、オプションを無効にすることができます。

Active Directoryでのダイナミックアクセス制御の設定方法については、Microsoft TechNetライブラリを参照し

てください。

"Microsoft TechNet ：「ダイナミックアクセス制御のシナリオの概要"

タスクの内容

ダイナミックアクセス制御を有効にすると、ダイナミックアクセス制御関連のエントリを含むACLをファイルシステムに含めることができます。ダイナミックアクセス制御を無効にすると、現在のダイナミックアクセス制御エントリは無視され、新しいエントリは許可されません。

このオプションは、advanced権限レベルでのみ使用できます。

ステップ

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ダイナミックアクセス制御の設定	入力するコマンド
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
無効にする	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 管理者権限レベルに戻ります。 `set -privilege admin`

関連情報

サーバー上のデータを保護するための集中アクセスポリシーを構成する

ONTAP SMBサーバで**DAC**が無効になっている場合に**DAC ACE**を含む**ACL**を管理する

ダイナミックアクセス制御ACEが適用されたACLが設定されたリソースがある場合にStorage Virtual Machine（SVM）でダイナミックアクセス制御を無効にすると、ダイナミックアクセス制御ACEを削除してから、そのリソースの非ダイナミックアクセス制御ACEを管理する必要があります。

タスクの内容

ダイナミックアクセス制御を無効にした場合、既存のダイナミックアクセス制御 ACE を削除するまでは、既存の非ダイナミックアクセス制御 ACE の削除や新しい非ダイナミックアクセス制御 ACE の追加はできません。

これらの手順は、通常 ACL の管理に使用している任意のツールを使用して実行できます。

手順

1. リソースに適用されているダイナミックアクセス制御 ACE を確認します。
2. リソースからダイナミックアクセス制御 ACE を削除します。
3. 必要に応じて、リソースに対して非ダイナミックアクセス制御 ACE を追加または削除します。

集約型アクセスポリシーを使用してCIFSサーバ上のデータへのアクセスを保護するには、CIFSサーバでのダイナミックアクセス制御（DAC）の有効化、Active Directoryでの集約型アクセスポリシーの設定、GPOを含むActive Directoryコンテナへの集約型アクセスポリシーの適用、CIFSサーバでのGPOの有効化など、いくつかの手順を実行する必要があります。

開始する前に

- 集約型アクセスポリシーを使用するようにActive Directoryを設定する必要があります。
- 集約型アクセスポリシーを作成し、CIFSサーバを含むコンテナにGPOを作成して適用するには、Active Directoryドメインコントローラに対する十分なアクセスが必要です。
- 必要なコマンドを実行するには、Storage Virtual Machine（SVM）に対する十分な管理アクセスが必要です。

タスクの内容

集約型アクセスポリシーは、Active Directoryのグループポリシーオブジェクト（GPO）に定義されて適用されます。Active Directoryで集約型アクセスポリシーを設定する方法については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNet ：「集約型アクセスポリシーのシナリオ"

手順

1. コマンドを使用して、SVMのダイナミックアクセス制御を有効にしていない場合は有効にし `vserver cifs options modify`ます。

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. コマンドを使用して、CIFSサーバでグループポリシーオブジェクト（GPO）を有効にしていない場合は有効にし `vserver cifs group-policy modify`ます。

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Active Directoryで集約型アクセスルールと集約型アクセスポリシーを作成します。
4. グループポリシーオブジェクト（GPO）を作成して、Active Directoryに集約型アクセスポリシーを導入します。
5. CIFSサーバのコンピュータアカウントが配置されているコンテナにGPOを適用します。
6. コマンドを使用して、CIFSサーバに適用されたGPOを手動で更新します `vserver cifs group-policy update`。

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. コマンドを使用して、CIFSサーバ上のリソースにGPO集約型アクセスポリシーが適用されていることを確認します `vserver cifs group-policy show-applied`。

   次の例は、デフォルトのドメインポリシーに2つの集約型アクセスポリシーがあり、それらがCIFSサーバに適用されていることを示しています。

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

```
    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

関連情報

- SMBサーバーにグループポリシーオブジェクトを適用する方法について学習します
- GPO構成に関する情報を表示する

- 集中アクセスポリシーに関する情報を表示する
- 集中アクセスポリシールールに関する情報を表示する
- サーバーのDACを有効または無効にする

ONTAP SMBサーバの**DAC**セキュリティに関する情報を表示する

NTFSボリューム、およびmixedセキュリティ形式のボリューム上のNTFS対応セキュリティを使用するデータのダイナミックアクセス制御（DAC）セキュリティに関する情報を表示できます。これには、条件付きACE、リソースACE、集約型アクセスポリシーACEに関する情報が含まれます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
出力にはグループSIDとユーザSIDが表示されます。	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
16進数のビットマスクがテキスト形式に変換されるファイルおよびディレクトリのファイルおよびディレクトリのセキュリティについて	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

例

次の例では、SVM vs1のパスに関するダイナミックアクセス制御セキュリティの情報を表示します `/vol1`。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

関連情報

- GPO構成に関する情報を表示する
- 集中アクセスポリシーに関する情報を表示する
- 集中アクセスポリシールールに関する情報を表示する

ONTAP SMBサーバ上の**DAC**の復元に関する考慮事項

ダイナミックアクセス制御（ DAC ）をサポートしないバージョンの ONTAP にリバートする場合に発生する状況と、リバートの前後に必要な処理を把握しておく必要があります。

ダイナミックアクセス制御がサポートされていないバージョンの ONTAP にクラスタをリバートし、 1 つ以上の Storage Virtual Machine （ SVM ）でダイナミックアクセス制御が有効になっている場合、リバート前に次の処理を実行する必要があります。

- クラスタでダイナミックアクセス制御が有効になっているすべての SVM で、ダイナミックアクセス制御を無効にする必要があります。
- イベントタイプを含むクラスタでは、イベントタイプのみを使用するように `file-op`監査の設定を変更する必要があります `cap-staging`。

ダイナミックアクセス制御 ACE が設定されているファイルやフォルダについて、リバートに関する重要な考慮事項を理解し、対応する必要があります。

- クラスタをリバートした場合、既存のダイナミックアクセス制御 ACE は削除されませんが、ファイルアクセスチェックで無視されます。
- リバート後はダイナミックアクセス制御 ACE は無視されるため、ダイナミックアクセス制御 ACE が設定されたファイルへのアクセスには変更が発生します。

  これにより、ユーザは以前にアクセスできなかったファイルにアクセスできるようになり、以前にアクセスできたファイルにアクセスできなくなる可能性があります。

- 以前のセキュリティレベルに戻すには、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する必要があります。

  この処理は、リバート前またはリバート完了直後に実行できます。

> リバート後はダイナミックアクセス制御 ACE は無視されるため、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する際にダイナミックアクセス制御 ACE を削除する必要はありません。ただし、必要に応じて手動で削除することもできます。

エクスポートポリシーを使用した**SMB**アクセスの保護

ONTAP SMBアクセスでエクスポートポリシーを使用する方法について学習します

SMBサーバでSMBアクセスのエクスポートポリシーが有効になっている場合は、SMBクライアントによるSVMボリュームへのアクセスを制御する際にエクスポートポリシーが使用されます。データにアクセスするには、SMBアクセスを許可するエクスポートポリシーを作成し、SMB共有を含むボリュームにそのポリシーを関連付けます。

エクスポートポリシーには、データへのアクセスを許可するクライアント、および読み取り専用アクセスと読み取り/書き込みアクセスでサポートされる認証プロトコルを指定するルールが1つ以上適用されます。エクスポートポリシーを設定して、すべてのクライアント、クライアントのサブネット、または特定のクライアントにSMB経由のアクセスを許可し、データへの読み取り専用アクセスと読み取り/書き込みアクセスを決定する際にKerberos認証、NTLM認証、またはKerberosとNTLMの両方を使用した認証を許可できます。

ONTAPは、エクスポートポリシーに適用されたすべてのエクスポートルールを処理したあと、クライアントにアクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポートルールは、Windowsのユーザおよびグループではなく、クライアントマシンに適用されます。エクスポートルールは、Windowsのユーザおよびグループベースの認証および許可に代わるものではありません。エクスポートルールは、共有権限とファイルアクセス権限に加えて、アクセスセキュリティのもう1つのレイヤを提供します。

ボリュームへのクライアントアクセスを設定するには、ボリュームごとにエクスポートポリシーを1つ関連付けます。各 SVM には複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームを備えた SVM に対して次の操作を実行できます。

- SVM のボリュームごとに異なるエクスポートポリシーを割り当て、 SVM の各ボリュームへのクライアントアクセスを個別に制御する。
- SVM の複数のボリュームに同じエクスポートポリシーを割り当て、同一のクライアントアクセス制御を実行する。ボリュームごとに新しいエクスポートポリシーを作成する必要はありません。

各 SVM には、「デフォルト」という名前のエクスポートポリシーが少なくとも 1 つあります。これにはルールは含まれません。このエクスポートポリシーは削除できませんが、名前や変更は可能です。デフォルトでは、 SVM 上の各ボリュームはデフォルトのエクスポートポリシーに関連付けられています。SVM で SMB アクセスのエクスポートポリシーが無効になっている場合、「 default 」エクスポートポリシーは SMB アクセスには影響しません。

NFSホストとSMBホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポートポリシーに関連付けることができます。エクスポートポリシーを、NFSホストとSMBホストの両方がアクセスする必要があるデータが格納されたボリュームに関連付けることができます。または、SMBクライアントのみがアクセスを必要とするボリュームがある場合は、SMBプロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証にKerberosまたはNTLMのみ（またはその両方）を使用するルールを含むエクスポートポリシーを設定できます。その後、このエクスポートポリシーをSMBアクセスのみが必要なボリュームに関連付けます。

SMBのエクスポートポリシーが有効になっている場合に、クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示されて要求は失敗します。クライアントがボリュームのエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポートポリシーが空の場合、すべてのアクセスが暗黙的に拒否されます。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、SMB共有を含むボリュームで少なくとも以下を許可するようにエクスポートポリシーを設定する必要があります。

- すべてのクライアントまたは適切なクライアントサブセットへのアクセスを許可する
- SMB経由のアクセスを許可する
- Kerberos認証またはNTLM認証（またはその両方）を使用して、適切な読み取り専用アクセスと書き込みアクセスを許可する

詳細はこちらをご覧ください "エクスポートポリシーの設定と管理"。

ONTAP SMBエクスポートルールについて学ぶ

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポートルールでは、ボリュームへのクライアントアクセス要求が設定した特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順序で処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致した場合、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用してクライアントアクセス権限を決定するようにエクスポートルールを設定できます。

- クライアントが要求の送信に使用するファイルアクセスプロトコル（NFSv4やSMBなど）。
- クライアント識別子（ホスト名やIPアドレスなど）。

  フィールドの最大サイズ `-clientmatch`は4096文字です。

- クライアントが認証に使用するセキュリティタイプ（Kerberos v5、NTLM、AUTH_SYSなど）。

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv3プロトコルを使用して送信され、クライアントのIPアドレスは10.1.17.37です。

クライアントアクセスプロトコルが一致していても、クライアントのIPアドレスがエクスポートルールで指定されているサブネットとは異なるサブネットに属しています。そのため、クライアント一致は失敗し、このルールはこのクライアントには適用されません。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントのIPアドレスが指定したサブネットにあります。したがって、クライアント一致は成功し、このルールはこのクライアントに適用されます。セキュリティタイプに関係なく、クライアントは読み取り/書き込みアクセス権を取得します。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule krb5,ntlm`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されます。

両方のクライアントでクライアントアクセスプロトコルとIPアドレスが一致している。読み取り専用パラメータでは、認証に使用したセキュリティタイプに関係なく、すべてのクライアントに読み取り専用アクセスが許可されます。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

SMB経由のアクセスを制限または許可するONTAPエクスポートポリシールールの例

以下の例は、 SMB アクセスのエクスポートポリシーが有効になっている SVM で SMB 経由のアクセスを制限または許可するエクスポートポリシールールを作成する方法を示しています。

SMB アクセスに関するエクスポートポリシーは、デフォルトでは無効になっています。SMB 経由のアクセスを制限または許可するエクスポートポリシールールは、 SMB アクセスのエクスポートポリシーを有効にしている場合にのみ設定する必要があります。

SMB アクセスのみのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifs1
- インデックス番号： 1.
- クライアント一致： 192.168.1.0/24 ネットワーク上のクライアントにのみ一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM 認証または Kerberos 認証を使用するクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証を使用するクライアントに許可します

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB および NFS アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifsnfs1
- インデックス番号： 2.
- クライアント一致：すべてのクライアントに一致します

- プロトコル： SMB アクセスと NFS アクセス
- 読み取り専用アクセス：すべてのクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証（ NFS および SMB ）または NTLM 認証（ SMB ）を使用するクライアントに許可
- UNIX ユーザ ID 0 （ゼロ）のマッピング：ユーザ ID 65534 （通常ユーザ名 nobody にマッピングされる）にマッピング
- suid と sgid のアクセス：許可しています

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

NTLM のみを使用する **SMB** アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：ntlm1
- インデックス番号： 1.
- クライアント一致：すべてのクライアントに一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM を使用するクライアントにのみ許可されます
- 読み取り / 書き込みアクセス： NTLM を使用するクライアントにのみ許可されます

> NTLM のみを使用するアクセスに読み取り専用オプションまたは読み取り / 書き込みオプションを設定する場合は、クライアント一致オプションで IP アドレスベースのエントリを使用する必要があります。そうしないと、エラーが発生し `access denied`ます。これは、 ONTAP がホスト名を使用してクライアントの権限を確認するときに、 Kerberos Service Principal Name （ SPN ；サービスプリンシパル名）を使用するためです。NTLM 認証では、 SPN 名はサポートされません。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

SMBアクセスの**ONTAP**エクスポートポリシーを有効または無効にする

Storage Virtual Machine （ SVM ）での SMB アクセスに関するエクスポートポリシーを有効または無効にすることができます。エクスポートポリシーを使用したリソースへの SMB アクセスの制御はオプションです。

開始する前に

SMB のエクスポートポリシーを有効にするための要件は次のとおりです。

- クライアントのエクスポートルールを作成する前に、そのクライアントのDNSに「PTR」レコードが必要です。
- SVMがNFSクライアントにアクセスを提供し、NFSアクセスに使用するホスト名がCIFSサーバ名と異なる場合は、ホスト名の「A」レコードと「PTR」レコードのセットを追加する必要があります。

タスクの内容

SVM に新しい CIFS サーバをセットアップするとき、 SMB アクセスに関するエクスポートポリシーの使用はデフォルトで無効になります。認証プロトコル、クライアント IP アドレス、またはホスト名に基づいてアクセスを制御する場合は、 SMB アクセスのエクスポートポリシーを有効にできます。SMB アクセスに関するエクスポートポリシーはいつでも有効または無効にできます。

NFS対応のSVMでCIFS / SMBのエクスポートポリシーを有効にすると、Linuxクライアントは、SVMでコマンドを使用して、関連付けられているエクスポートポリシールールとすべてのSMBボリュームのジャンクションパスを表示でき `showmount -e`ます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. エクスポートポリシーを有効または無効にします。
   - エクスポートポリシーを有効にします。 `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
   - エクスポートポリシーを無効にします。 `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、エクスポートポリシーを使用したSVM vs1上のリソースへのSMBクライアントアクセスの制御を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

ストレージレベルのアクセス保護を使用したファイルアクセスの保護

ストレージレベルのアクセスガードを使用した安全な **ONTAP SMB** ファイルアクセスについて学習します。

ネイティブファイルレベルのセキュリティとエクスポートおよび共有のセキュリティを使用したアクセスの保護に加えて、ボリュームレベルで ONTAP によって適用される第 3 のセキュリティレイヤとしてストレージレベルのアクセス保護を設定できます。スト

レージレベルのアクセス保護：すべての NAS プロトコルから適用されるストレージオブジェクトへの環境アクセスを保護します。

NTFSのアクセス権限のみがサポートされます。ONTAPがストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスするUNIXユーザのセキュリティチェックを実行するには、UNIXユーザがボリュームを所有するSVM上のWindowsユーザにマッピングされている必要があります。

ストレージレベルのアクセス保護の動作

- ストレージレベル環境のアクセス保護：ストレージオブジェクト内のすべてのファイルまたはすべてのディレクトリを保護します。

  ボリューム内のすべてのファイルまたはディレクトリがストレージレベルのアクセス保護設定の影響を受けるため、伝播による継承は必要ありません。

- ストレージレベルのアクセス保護は、ボリューム内のファイルのみ、ディレクトリのみ、またはファイルとディレクトリの両方に適用されるように設定できます。
  - ファイルとディレクトリのセキュリティ

    ストレージオブジェクト内のすべてのディレクトリとファイルを環境に格納します。これがデフォルト設定です。

  - ファイルセキュリティ

    ストレージオブジェクト内のすべてのファイルを環境します。このセキュリティを適用しても、ディレクトリへのアクセスとディレクトリの監査には影響しません。

  - ディレクトリセキュリティ

    ストレージオブジェクト内のすべてのディレクトリを環境します。このセキュリティを適用しても、ファイルへのアクセスとファイルの監査には影響しません。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

- NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。

  有効な権限を決定するために、ストレージオブジェクトレベルで適用され、メタデータに格納されます。

- システム（ Windows または UNIX ）管理者であっても、ストレージレベルのセキュリティをクライアントから取り消すことはできません。

  このセキュリティは、ストレージ管理者のみが変更できるように設計されています。

- ストレージレベルのアクセス保護は、 NTFS または mixed セキュリティ形式のボリュームに適用できます。
- ストレージレベルのアクセス保護を UNIX セキュリティ形式のボリュームに適用できるのは、そのボリュームが含まれている SVM で CIFS サーバが設定されている場合に限られます。
- ボリュームがボリュームジャンクションパス以下にマウントされていて、そのパスにストレージレベルの

アクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。

- ストレージレベルのアクセス保護のセキュリティ記述子は、 SnapMirror データレプリケーションおよび SVM レプリケーションによってレプリケートされます。
- ウィルススキャンについては特別な免除があります。

  ファイルやディレクトリのスクリーニングを行うこれらのサーバに対しては、ストレージレベルのアクセス保護によってオブジェクトへのアクセスが拒否されていても、例外的なアクセスが許可されます。

- ストレージレベルのアクセス保護によってアクセスが拒否された場合、 FPolicy 通知は送信されません。

アクセスチェックの順序

ファイルまたはディレクトリへのアクセスは、エクスポートまたは共有の権限、ボリュームで設定されているストレージレベルのアクセス保護権限、ファイルやディレクトリに適用されるネイティブのファイル権限の各影響の組み合わせによって決まります。すべてのレベルのセキュリティが評価されて、ファイルまたはディレクトリの有効な権限が決定されます。セキュリティアクセスチェックは、次の順序で実行されます。

1. SMB 共有または NFS エクスポートレベルの権限
2. ストレージレベルのアクセス保護
3. NTFSのファイル/フォルダのAccess Control List（ACL；アクセス制御リスト）、NFSv4 ACL、またはUNIXモードビット

ストレージレベルのアクセス保護の使用のユースケース

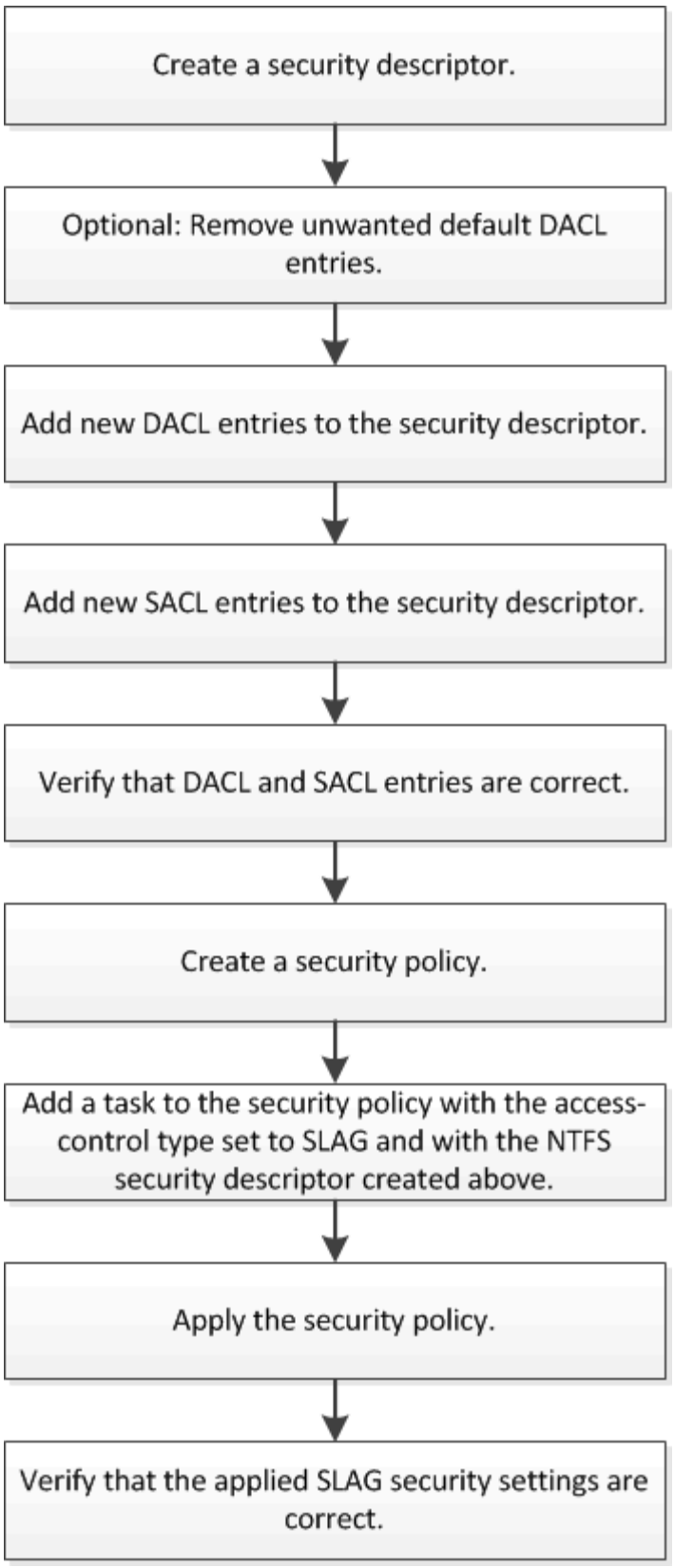
ストレージレベルのアクセス保護は、ストレージレベルでの追加セキュリティを提供します。このセキュリティはクライアント側からは見えないため、ユーザや管理者がデスクトップから取り消すことはできません。一部のユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

この機能の一般的なユースケースとしては、次のようなシナリオがあります。

- すべてのユーザーのアクセスをストレージ・レベルで監査および制御することにより ' 知的財産を保護します
- 銀行や証券会社など、金融サービス企業のストレージの場合
- 部門ごとに個別のファイルストレージを使用する行政サービス
- すべての学生のファイルを保護する大学

ONTAP SMBサーバにおけるストレージレベルアクセスガードの設定ワークフロー

ストレージレベルのアクセス保護（SLAG）を設定するワークフローでは、NTFSファイル権限と監査ポリシーの設定に使用するONTAP CLIコマンドと同じコマンドを使用します。対象のファイルやディレクトリのアクセスを設定する代わりに、対象のStorage Virtual Machine（SVM）ボリュームのSLAGを設定します。



関連情報

サーバー上でストレージレベルのアクセスガードを構成する

ボリュームまたはqtreeにストレージレベルのアクセス保護を設定するには、いくつかの手順に従う必要があります。ストレージレベルのアクセス保護は、ストレージレベルで設定されるアクセスセキュリティのレベルを提供します。すべてのNASプロトコルから適用先のストレージオブジェクトへのすべてのアクセスに適用されるセキュリティを提供します。

手順

1. コマンドを使用して、セキュリティ記述子を作成し `vserver security file-directory ntfs create`ます。

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver
security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1

   NTFS Security    Owner Name
   Descriptor Name
   ------------     --------------
   sd1              -
```

セキュリティ記述子は、次の4つのデフォルトDACL Access Control Entry（ACE；アクセス制御エントリ）で作成されます。

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    BUILTIN\Administrators
                     allow    full-control   this-folder, sub-folders,
files
    BUILTIN\Users    allow    full-control   this-folder, sub-folders,
files
    CREATOR OWNER    allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

ストレージレベルのアクセス保護の設定時にデフォルトのエントリを使用しない場合は、セキュリティ記述子に独自のACEを作成して追加する前に、デフォルトのエントリを削除できます。

2. セキュリティ記述子から、ストレージレベルのアクセス保護セキュリティで設定したくないデフォルト

のDACL ACEを削除します。

a. コマンドを使用して、不要なDACL ACEを削除します `vserver security file-directory ntfs dacl remove`。

   この例では、セキュリティ記述子から BUILTIN\Administrators 、 BUILTIN\Users 、 CREATOR OWNER の 3 つのデフォルト DACL ACE を削除しています。

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. コマンドを使用して、ストレージレベルのアクセス保護セキュリティに使用しないDACL ACEがセキュリティ記述子から削除されたことを確認します `vserver security file-directory ntfs dacl show`。

   この例では、コマンドの出力によって、3つのデフォルトDACL ACEがセキュリティ記述子から削除され、NT AUTHORITY\SYSTEMデフォルトDACL ACEエントリのみが残されていることが確認されます。

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access           Apply To
                     Type     Rights
    --------------   -------  -------          -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. コマンドを使用して、セキュリティ記述子に1つ以上のDACLエントリを追加します `vserver security file-directory ntfs dacl add`。

   この例では、セキュリティ記述子に2つのDACL ACEを追加しています。

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. コマンドを使用して、セキュリティ記述子に1つ以上のSACLエントリを追加します `vserver security file-directory ntfs sacl add`。

   この例では、セキュリティ記述子に2つのSACL ACEを追加しています。

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. コマンドと `vserver security file-directory ntfs sacl show`コマンドを使用して、DACL ACEとSACL ACEがそれぞれ正しく設定されていることを確認します `vserver security file-directory ntfs dacl show。

   この例では、次のコマンドを実行すると、セキュリティ記述子「`d1"」の DACL エントリに関する情報が表示されます。

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   この例では、次のコマンドを実行すると、セキュリティ記述子「`d1"」の SACL エントリに関する情報が表示されます。

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. コマンドを使用して、セキュリティポリシーを作成し `vserver security file-directory policy create`ます。

   次に、「 policy1 」という名前のポリシーを作成する例を示します。

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. コマンドを使用して、ポリシーが正しく設定されていることを確認します `vserver security file-directory policy show`。

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. コマンドでパラメータをに設定 `slag`して `-access-control`、セキュリティ記述子が関連付けられたタスクをセキュリティポリシーに追加します `vserver security file-directory policy task add`。

   ポリシーには複数のストレージレベルのアクセス保護タスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

   この例では ' セキュリティー記述子 "`d1" に割り当てられている "policy1 " という名前のポリシーにタスクが追加されますアクセス制御タイプが「`slag」に設定されたパスに割り当てられ `/datavol1`ます。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. コマンドを使用して、タスクが正しく設定されていることを確認します `vserver security file-directory policy task show`。

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. コマンドを使用して、ストレージレベルのアクセス保護セキュリティポリシーを適用し `vserver security file-directory apply`ます。

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    セキュリティポリシーを適用するジョブがスケジュールされます。

11. コマンドを使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認し `vserver security file-directory show`ます。

    この例では、コマンドの出力から、ストレージレベルのアクセス保護セキュリティがNTFSボリュームに適用されていることがわかります `/datavol1`。Everyoneにフルコントロールを許可するデフォルトのDACLは残っていますが、ストレージレベルのアクセス保護セキュリティは、ストレージレベルのアクセス保護設定で定義されたグループへのアクセスを制限（および監査）します。

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

関連情報

- NTFS ファイル セキュリティ、NTFS 監査ポリシー、ストレージ レベルのアクセス ガードを管理するためのコマンド
- サーバー上のストレージレベルのアクセスガードの構成ワークフロー
- サーバー上のストレージレベルのアクセスガードに関する情報を表示する
- サーバーのストレージレベルのアクセスガードを削除する

ONTAP SMBサーバにおける有効な**SLAG**マトリックス

SLAG は、ボリューム、 qtree 、またはその両方に対して設定できます。次の表に、さまざまな状況について、ボリュームまたは qtree に SLAG 構成を適用できるかどうかを示します。

	AFS 内のボリューム **SLAG**	**Snapshot**内のボリューム**SLAG**	**AFS** 内の **qtree SLAG**	**Snapshot**内の**qtree SLAG**
AFS 内のボリュームへのアクセス	はい	いいえ	N/A	N/A
Snapshot内のボリュームへのアクセス	はい	いいえ	N/A	N/A
AFS 内の qtree へのアクセス（ qtree に SLAG が設定されている場合）	いいえ	いいえ	はい	いいえ
AFS 内の qtree へのアクセス（ qtree に SLAG が設定されていない場合）	はい	いいえ	いいえ	いいえ
Snapshot内のqtreeへのアクセス（qtreeにSLAGが設定されている場合）	いいえ	いいえ	はい	いいえ
Snapshot内のqtreeへのアクセス（qtreeにSLAGが設定されていない場合）	はい	いいえ	いいえ	いいえ

ONTAP SMBサーバ上のストレージレベルアクセスガードに関する情報を表示する

ストレージレベルのアクセス保護は、ボリュームまたは qtree に適用される 3 番目のセキュリティレイヤです。ストレージレベルのアクセス保護設定は、 Windows のプロパティウィンドウでは表示できません。ストレージレベルのアクセス保護セキュリティに関する情報を表示するには、 ONTAP CLI を使用する必要があります。この情報を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine （ SVM ）の名前、およびストレージレベルのアクセス保護セキュリティ情報を表示するボリュームまたは qtree のパスを入力する必要があります。出力は要約形式で表示することも、詳細なリ

ストとして表示することもできます。

ステップ

1. ストレージレベルのアクセス保護セキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細を表示	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1のパスにあるNTFSセキュリティ形式のボリュームのストレージレベルのアクセス保護セキュリティ情報を表示します `/datavol1`。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

次の例では、SVM vs1のパスにあるmixedセキュリティ形式のボリュームに関するストレージレベルのアクセス保護の情報を表示します `/datavol5`。このボリュームの最上位には、 UNIX 対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP SMBサーバのストレージレベルアクセスガードを削除する

ストレージレベルのアクセスセキュリティの設定が不要になった場合は、ボリュームや qtree からストレージレベルのアクセス保護を削除できます。ストレージレベルのアクセス保護を削除しても、通常の NTFS のファイルやディレクトリのセキュリティは変更されたり削除されたりしません。

手順

1. コマンドを使用して、ボリュームまたはqtreeにストレージレベルのアクセス保護が設定されていることを確認します `vserver security file-directory show`。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. コマンドを使用して、ストレージレベルのアクセス保護を削除します `vserver security file-directory remove-slag`。

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. コマンドを使用して、ボリュームまたはqtreeからストレージレベルのアクセス保護が削除されたことを確認します `vserver security file-directory show`。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

SMBを使用したファイルアクセスの管理

ローカルユーザとローカルグループを認証と許可に使用する

ONTAPでのローカルユーザとローカルグループの使用方法

ローカル ONTAP SMB ユーザーとグループについて学ぶ

環境でローカルユーザとローカルグループを設定して使用するかどうかを決定する前に、ローカルユーザとローカルグループとは何か、およびそれらに関するいくつかの基本情報を把握しておく必要があります。

- * ローカルユーザー *

  一意のSecurity Identifier（SID；セキュリティ識別子）を持つユーザアカウント。そのユーザアカウントを作成したStorage Virtual Machine（SVM）上でのみ認識されます。ローカルユーザアカウントには、ユーザ名やSIDなどの一連の属性があります。ローカルユーザアカウントは、NTLM認証を使用してCIFSサーバ上でローカルに認証されます。

  ユーザアカウントには次のような用途があります。

  - ユーザに _ ユーザ権限の管理 _ 権限を付与するために使用します。
  - SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

- * ローカルグループ *

  一意のSIDを持つグループは、そのグループを作成したSVM上でのみ認識されます。グループには一連のメンバーが含まれます。メンバーには、ローカルユーザ、ドメインユーザ、ドメイングループ、およびドメインマシンアカウントを指定できます。グループは作成、変更、または削除できます。

  グループにはいくつかの用途があります。

  - メンバーに _User Rights Management_Privileges を付与するために使用します。
  - SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

- * ローカルドメイン *

  ローカルスコープを持つドメイン。SVMでバインドされています。ローカルドメインの名前はCIFSサーバの名前です。ローカルユーザとローカルグループはローカルドメイン内に格納されます。

- * Security Identifier （ SID ；セキュリティ識別子） *

  SIDは可変長の数値で、Windows形式のセキュリティプリンシパルを識別します。たとえば、通常の SID の場合は、次のような形式になります。 S-1-5-21-3139654847-1303905135-2517279418-123456 。

- * NTLM 認証 *

  CIFSサーバでユーザを認証するために使用されるMicrosoft Windowsのセキュリティ方式。

- * 複製されたクラスタデータベース（ RDB ） *

  クラスタ内の各ノードにインスタンスがあるレプリケートされたデータベース。ローカルユーザオブジェクトとローカルグループオブジェクトはRDBに格納されます。

ローカル **ONTAP SMB** ユーザーとローカル グループを作成する理由

Storage Virtual Machine（SVM）でローカルユーザやローカルグループを作成する理由はいくつかあります。たとえば、ドメインコントローラ（DC）を使用できない場合でも、ローカルユーザアカウントを使用してSMBサーバにアクセスできます。また、ローカルグループを使用してPrivilegesを割り当てたり、SMBサーバがワークグループに含まれている場合もあります。

ローカルユーザアカウントを作成する理由は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメインユーザを使用できません。

  ワークグループを設定するにはローカルユーザが必要です。

- ドメインコントローラを使用できない場合に、SMBサーバで認証してログインできるようにする。

  ドメインコントローラがダウンしている場合や、ネットワークの問題によってSMBサーバからドメインコントローラに接続できない場合は、ローカルユーザはNTLM認証を使用してSMBサーバに認証できます。

- ローカル・ユーザに _ ユーザ権限の管理 _ 権限を割り当てる

User Rights Management は、ユーザとグループに付与する SVM の権限を SMB サーバ管理者が制御できる機能です。ユーザにPrivilegesを割り当てるには、ユーザのアカウントにPrivilegesを割り当てるか、ユーザをそのPrivilegesを含むローカルグループのメンバーにします。

ローカルグループを作成する理由は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメイングループを使用できません。

  ローカルグループはワークグループ構成では必要ありませんが、ローカルワークグループユーザのアクセスPrivilegesの管理に役立ちます。

- 共有とファイルアクセスの制御にローカルグループを使用して、ファイルおよびフォルダリソースへのアクセスを制御する。
- カスタマイズした _ ユーザ権限の管理 _ 権限を持つローカルグループを作成する。

  一部の組み込みユーザグループには、Privilegesが事前に定義されています。カスタマイズしたPrivilegesセットを割り当てるには、ローカルグループを作成し、そのグループに必要なPrivilegesを割り当てます。その後、ローカルユーザ、ドメインユーザ、およびドメイングループをそのローカルグループに追加できます。

関連情報

- ローカルユーザー認証について学ぶ
- サポートされるPrivilegesのリスト

ローカル **ONTAP SMB** ユーザー認証について学ぶ

ローカルユーザがCIFSサーバ上のデータにアクセスする前に、認証されたセッションを作成する必要があります。

SMBはセッションベースであるため、ユーザのIDはセッションの最初のセットアップ時に1回だけ確認できます。CIFSサーバでは、ローカルユーザの認証時にNTLMベースの認証が使用されます。NTLMv1とNTLMv2の両方がサポートされています。

ONTAPは、3つのユースケースでローカル認証を使用します。それぞれのユースケースは、ユーザ名のドメイン部分（domain\user形式）がCIFSサーバのローカルドメイン名（CIFSサーバ名）と一致するかどうかによって異なります。

- ドメイン部分が一致する

  データへのアクセスを要求するときにローカルユーザクレデンシャルを指定したユーザは、CIFSサーバでローカルに認証されます。

- ドメイン部分が一致しません

  ONTAPは、CIFSサーバが属しているドメインのドメインコントローラでNTLM認証を試行します。認証に成功した場合は、ログインが完了します。成功しなかった場合、次に何が起こるかは、認証が成功しなかった理由によって異なります。

  たとえば、ユーザがActive Directoryに存在するにもかかわらず、パスワードが無効であるか期限切れになっている場合、ONTAPはCIFSサーバ上の対応するローカルユーザアカウントの使用を試みません。代わ

りに、認証は失敗します。NetBIOSドメイン名が一致しなくても、ONTAPがCIFSサーバ上の対応するローカルアカウント（存在する場合）を認証に使用するケースは他にもあります。たとえば、一致するドメインアカウントが存在するが無効になっている場合、ONTAPはCIFSサーバ上の対応するローカルアカウントを認証に使用します。

- ドメイン部分が指定されていません

  ONTAPは最初にローカルユーザとしての認証を試行します。ローカルユーザとしての認証に失敗した場合、ONTAPはCIFSサーバが属しているドメインのドメインコントローラでユーザを認証します。

ローカルユーザまたはドメインユーザの認証が完了すると、ONTAPはローカルグループメンバーシップとPrivilegesを考慮した完全なユーザアクセストークンを構築します。

ローカルユーザのNTLM認証の詳細については、Microsoft Windowsのマニュアルを参照してください。

関連情報

サーバー上のローカルユーザー認証を有効または無効にする

ONTAP SMBユーザーアクセストークンについて学ぶ

ユーザが共有をマッピングすると、認証された SMB セッションが確立され、ユーザアクセストークンが構成されます。このトークンには、ユーザ、ユーザのグループメンバーシップ、累積権限、マッピングされた UNIX ユーザのそれぞれについて、情報が格納されています。

この機能が無効になっていないかぎり、ローカルユーザとローカルグループの両方の情報がユーザアクセストークンに追加されます。アクセストークンの構成方法は、ローカルユーザのログインと Active Directory ドメインユーザのログインでは、方法が異なります。

- ローカルユーザログイン

  ローカルユーザは複数のローカルグループのメンバーになることができますが、ローカルグループを他のローカルグループのメンバーにすることはできません。ローカルユーザアクセストークンは、その特定のローカルユーザが属するグループに割り当てられたすべての権限の組み合わせから構成されます。

- ドメイン・ユーザ・ログイン

  ドメインユーザのログインでは、 ONTAP は、ユーザの SID と、そのユーザが属するすべてのドメイングループの SID が格納されたユーザアクセストークンを取得します。ONTAP は、ユーザドメイングループのローカルメンバーシップ（存在する場合）が提供するアクセストークンとドメインユーザアクセストークンとの組み合わせを使用します。また、ドメインユーザに割り当てられた直接権限や、ドメイングループメンバーシップの直接権限も使用します。

ローカルユーザとドメインユーザの両方のログインで、プライマリグループ RID もユーザアクセストークン用に設定されています。デフォルトのRIDは（RID 513）です `Domain Users`。デフォルトは変更できません。

Windows から UNIX へのネームマッピングと、 UNIX から Windows へのネームマッピングのプロセスでは、ローカルアカウントとドメインアカウントのどちらについても同じルールが適用されます。

UNIX ユーザがローカルアカウントに自動的にマッピングされることはありません。このマッピングが必要な場合は、既存のネームマッピングコマンドを使用して明示的なマッピングルールを指定する必要があります。

ローカルグループを含む **ONTAP SMB SVM** での **SnapMirror** の使用について学習します。

ローカルグループを含む SVM によって所有されているボリュームで SnapMirror を設定する際は、一定のガイドラインに注意する必要があります。

SnapMirror によって別の SVM にレプリケートされるファイル、ディレクトリ、または共有に適用する ACE ではローカルグループを使用できません。SnapMirror 機能を使用して別の SVM 上のボリュームに対する DR ミラーを作成する場合に、そのボリュームにローカルグループの ACE があるときは、ミラーには ACE は適用されません。データが別の SVM にレプリケートされる場合、実質的に、そのデータは別のローカルドメインに格納されることになります。ローカルユーザとローカルグループに付与されるアクセス権は、そのオブジェクトが最初に作成された SVM のスコープ内でのみ有効です。

ONTAP SMBサーバの削除がユーザーとグループに与える影響について学習します

CIFSサーバを作成するとデフォルトの一連のローカルユーザとローカルグループが作成され、CIFSサーバをホストするStorage Virtual Machine（SVM）に関連付けられます。SVM管理者は、ローカルユーザやローカルグループをいつでも作成できます。CIFSサーバを削除した場合のローカルユーザとローカルグループへの影響について理解しておく必要があります。

ローカルユーザとローカルグループはSVMに関連付けられます。そのため、セキュリティ上の理由から、CIFSサーバを削除してもそれらが削除されることはありません。CIFSサーバを削除してもローカルユーザとローカルグループは削除されませんが、表示されません。SVMでCIFSサーバを再作成するまで、表示したり管理したりすることはできません。

CIFSサーバの管理ステータスは、ローカルユーザやローカルグループの表示には影響しません。

ローカル **ONTAP SMB** ユーザーとグループで **Microsoft** 管理コンソールを使用する方法を学びます

Microsoft 管理コンソールを使用して、ローカルユーザとローカルグループのそれぞれの情報を表示できます。ONTAP の今回のリリースでは、 Microsoft 管理コンソールで、ローカルユーザとローカルグループに対する上記以外の管理タスクを実行することはできません。

ONTAP SMBクラスタの復元について学ぶ

ローカルユーザとグループを使用してファイルアクセスまたはユーザ権限を管理している場合に、ローカルユーザとグループをサポートしない ONTAP リリースにクラスタをリバートするときは、一定の考慮事項に注意する必要があります。

- セキュリティ上の理由から、 ONTAP をローカルユーザとグループの機能をサポートしないバージョンにリバートしても、設定されているローカルユーザ、グループ、および権限に関する情報は削除されません。

- ONTAP の以前のメジャーバージョンにリバートする際、 ONTAP では認証とクレデンシャルの作成時にローカルユーザとローカルグループは使用されません。
- ローカルユーザとローカルグループは、ファイルおよびフォルダの ACL からは削除されません。
- ローカルユーザまたはローカルグループに付与された権限に基づいて許可されるアクセスに依存するファイルアクセス要求は拒否されます。

  アクセスを許可するには、ローカルユーザとローカルグループオブジェクトではなく、ドメインオブジェクトに基づいてアクセスを許可するようにファイル権限を再設定する必要があります。

ローカル権限とは

サポートされている **ONTAP SMB** 権限のリスト

ONTAPには、サポートされるPrivilegesのセットがあらかじめ定義されています。一部の事前定義されたローカルグループには、これらのPrivilegesの一部がデフォルトで追加されています。また、事前定義されたグループに対してPrivilegesを追加または削除したり、新しいローカルユーザまたはローカルグループを作成して、作成したグループや既存のドメインユーザおよびグループにPrivilegesを追加したりすることもできます。

次の表に、Storage Virtual Machine（SVM）でサポートされるPrivilegesの一覧と、Privilegesが割り当てられているBUILTINグループの一覧を示します。

権限の名前	デフォルトのセキュリティ設定	説明
`SeTcbPrivilege`	なし	オペレーティングシステムの一部として機能
`SeBackupPrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	ACLを無視してファイルとディレクトリをバックアップ
`SeRestorePrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	ACLを無視してファイルとディレクトリをリストア有効なユーザまたはグループのSIDをファイル所有者として設定する
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	ファイルやその他のオブジェクトの所有権を取得する
`SeSecurityPrivilege`	`BUILTIN\Administrators`	監査の管理 セキュリティ ログの表示、ダンプ、消去など。

権限の名前	デフォルトのセキュリティ設定	説明
SeChangeNotifyPrivilege	BUILTIN\Administrators BUILTIN\Backup Operators、、 BUILTIN\Power Users、、 BUILTIN\Users Everyone	トラバースチェックのバイパス この権限を持つユーザには、フォルダ、シンボリックリンク、ジャンクションをトラバースするためのトラバース（x）権限は必要ありません。

関連情報

- 権限の割り当てについて学ぶ
- バイパストラバースチェックの設定について学ぶ

ONTAP SMB権限の割り当てについて学ぶ

Privilegesは、ローカルユーザまたはドメインユーザに直接割り当てることができます。また、ユーザに付与する機能と一致するPrivilegesが割り当てられているローカルグループにユーザを割り当てることもできます。

- 作成したグループに一連の権限を割り当てることができます。

  次に、そのユーザに割り当てるPrivilegesを含むグループにユーザを追加します。

- また、デフォルトのPrivilegesがユーザに付与するPrivilegesと一致する事前定義されたグループに、ローカルユーザとドメインユーザを割り当てることもできます。

関連情報

- ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加
- ローカルまたはドメインのユーザーまたはグループから権限を削除する
- ローカルまたはドメインのユーザーとグループの権限をリセットする
- バイパストラバースチェックの設定について学ぶ

ONTAP SMBサーバの**BUILTIN**グループとローカル管理者アカウントについて学習します

BUILTINグループとローカル管理者アカウントを使用する場合は、一定のガイドラインに注意する必要があります。たとえば、ローカル管理者アカウントは、名前の変更は可能ですが、削除はできません。

- Administratorアカウントの名前は変更できますが、削除することはできません。
- AdministratorアカウントはBUILTIN\Administratorsグループから削除できません。
- 組み込みグループの名前は変更できますが、削除することはできません。

  BUILTINグループの名前を変更すると、既知の名前を使用して別のローカルオブジェクトを作成できますが、そのオブジェクトには新しいRIDが割り当てられます。

- ローカルGuestアカウントはありません。

関連情報

事前定義のBUILTINグループとデフォルトのPrivileges

ローカル **ONTAP SMB** ユーザーパスワードの要件

デフォルトでは、ローカルユーザのパスワードは複雑さの要件を満たす必要があります。パスワードの複雑さの要件は、 Microsoft Windows_Local セキュリティポリシー _ で定義されている要件に似ています。

パスワードは次の基準を満たしている必要があります。

- 6文字以上にする必要があります
- ユーザアカウント名を含めることはできません
- 次の4つのカテゴリのうち、少なくとも3つの文字を含める必要があります。
  - 大文字のアルファベット（A~Z）
  - 小文字のアルファベット（a~z）
  - 10進数（0～9）
  - 特殊文字：

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

関連情報

- ローカルユーザーのパスワードの複雑さを構成する
- サーバーのセキュリティ設定に関する情報を表示する
- ローカルユーザアカウントのパスワードの変更

定義済みの**BUILTIN**グループとデフォルトの**ONTAP SMB**権限

ローカルユーザまたはドメインユーザのメンバーシップを、ONTAPの事前定義された一連のBUILTINグループに割り当てることができます。事前定義グループには事前定義Privilegesが割り当てられています。

次の表に、事前定義グループを示します。

事前定義の **BUILTIN** グループ	デフォルトの権限
BUILTIN\AdministratorsRID 544 最初に作成されたときに、RID 500のローカル Administrator`アカウントが自動的にこのグループのメンバーになります。Storage Virtual Machine（SVM）がドメインに参加すると、`domain\Domain Admins`グループがグループに追加されます。SVMがドメインから削除されると`domain\Domain Admins、グループはグループから削除されます。	• SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
BUILTIN\Power UsersRID 547 このグループには、最初に作成された時点ではメンバーがありません。このグループのメンバーには、次のような特徴があります。 • ローカルユーザとローカルグループを作成および管理できます。 • 自分自身や他のオブジェクトをグループに追加することはできません BUILTIN\Administrators。	SeChangeNotifyPrivilege
BUILTIN\Backup OperatorsRID 551 このグループには、最初に作成された時点ではメンバーがありません。このグループのメンバーは、バックアップ目的で開いたファイルやフォルダの読み取りおよび書き込み権限を上書きできます。	• SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
BUILTIN\UsersRID 545 最初に作成された時点では、このグループには（暗黙的な特殊グループ以外に）メンバーはありませ`Authenticated Users`ん。SVMがドメインに参加すると、`domain\Domain Users`グループがこのグループに追加されます。SVMがドメインから削除されると、`domain\Domain Users`グループはこのグループから削除されます。	SeChangeNotifyPrivilege
EveryoneSID S-1-1-0 このグループには、ゲストを含むすべてのユーザが含まれます（匿名ユーザは含まれません）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。	SeChangeNotifyPrivilege

関連情報

- サーバーのBUILTINグループとローカル管理者アカウントについて学習します
- サポートされるPrivilegesのリスト
- バイパストラバースチェックの設定について学ぶ

ローカルユーザとローカルグループ機能の有効化と無効化

ローカル **ONTAP SMB** ユーザーとグループの機能について学習します

NTFSセキュリティ形式データのアクセス制御にローカルユーザとローカルグループを使用する前に、ローカルユーザとローカルグループ機能を有効にする必要があります。また、SMB認証にローカルユーザを使用する場合は、ローカルユーザ認証機能を有効にする必要があります。

ローカルユーザとローカルグループ機能とローカルユーザ認証はデフォルトで有効になっています。有効になっていない場合は、ローカルユーザとローカルグループを設定して使用する前に有効にする必要があります。ローカルユーザとローカルグループ機能はいつでも無効にできます。

ローカルユーザとローカルグループ機能の明示的な無効化に加えて、ONTAPでは、クラスタ内のいずれかのノードがローカルユーザとローカルグループ機能をサポートしないONTAPリリースにリバートされた場合にローカルユーザとローカルグループ機能が無効になります。クラスタ内のすべてのノードでこの機能をサポートするバージョンのONTAPが実行されるまで、ローカルユーザとローカルグループ機能は有効になりません。

関連情報

- ローカルユーザアカウントを変更する
- ローカルグループの変更
- ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加

ONTAP SMBサーバ上のローカルユーザーとグループを有効または無効にする

Storage Virtual Machine（SVM）で、SMBアクセス用のローカルユーザとローカルグループを有効または無効にすることができます。ローカルユーザとローカルグループ機能はデフォルトで有効になっています。

タスクの内容

SMB共有およびNTFSファイル権限の設定時にローカルユーザとローカルグループを使用できます。必要に応じて、SMB接続の作成時の認証にローカルユーザを使用することもできます。認証にローカルユーザを使用するには、ローカルユーザとローカルグループ認証オプションも有効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ローカルユーザとローカルグループの設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、SVM vs1でローカルユーザとローカルグループ機能を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

関連情報

- サーバー上のローカルユーザー認証を有効または無効にする
- ローカルユーザアカウントの有効化または無効化

ONTAP SMBサーバ上でローカルユーザ認証を有効または無効にする

Storage Virtual Machine（SVM）でのSMBアクセスに関するローカルユーザ認証を有効または無効にすることができます。デフォルトでは、ローカルユーザ認証は許可されます。これは、SVMがドメインコントローラに接続できない場合や、ドメインレベルのアクセス制御を使用しない場合に役立ちます。

開始する前に

CIFSサーバでローカルユーザとローカルグループ機能を有効にする必要があります。

タスクの内容

ローカルユーザ認証はいつでも有効または無効にできます。SMB接続の作成時の認証にローカルユーザを使用する場合は、CIFSサーバのローカルユーザとローカルグループオプションも有効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`

2. 次のいずれかを実行します。

ローカル認証の設定	入力するコマンド
有効	`vserver cifs options modify -vserver *vserver_name* -is-local-auth-enabled true`
無効にする	`vserver cifs options modify -vserver *vserver_name* -is-local-auth-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、SVM vs1でローカルユーザ認証を有効にします。

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

関連情報

- ローカルユーザー認証について学ぶ
- サーバー上のローカルユーザーとグループを有効または無効にする

ローカルユーザアカウントを管理します。

ローカル **ONTAP SMB** ユーザー アカウントを変更する

既存のユーザのフルネームや概要を変更したり、ユーザアカウントを有効または無効にしたりする場合は、ローカルユーザアカウントを変更します。また、ユーザ名が侵害を受けたり、管理上の目的で名前の変更が必要になった場合にも、ローカルユーザアカウントの名前を変更できます。

状況	入力するコマンド
ローカルユーザのフルネームの変更	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -full-name text`フルネームにスペースが含まれている場合は、二重引用符で囲む必要があります。

状況	入力するコマンド
ローカルユーザの概要を変更します	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -description text`説明にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザアカウントを有効または無効にする	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	ローカルユーザアカウントの名前を変更する

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上のローカルユーザ「 CIFS_SERVER\sue 」の名前を「 CIFS_SERVER\sue_new 」に変更します。

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

ローカル **ONTAP SMB** ユーザー アカウントを有効または無効にする

ユーザがStorage Virtual Machine（SVM）に格納されたデータにSMB接続経由でアクセスできるようにするには、ローカルユーザアカウントを有効にします。また、そのユーザがSVMのデータにSMB経由でアクセスできないようにするには、ローカルユーザアカウントを無効にします。

タスクの内容

ローカルユーザを有効にするには、ユーザアカウントを変更します。

ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
ユーザアカウントを有効にする	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account -disabled false`
ユーザアカウントを無効にする	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account -disabled true`

ローカル **ONTAP SMB** ユーザー アカウントのパスワードを変更する

ローカルユーザのアカウントパスワードを変更できます。これは、ユーザのパスワードが侵害された場合や、ユーザがパスワードを忘れた場合に役立ちます。

ステップ

1. 適切な操作を実行してパスワードを変更します。 `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 に関連付けられたローカルユーザ「 CIFS_SERVER\sue 」のパスワードを設定します。

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

関連情報

ローカルユーザーのパスワードの複雑さを構成する

サーバーのセキュリティ設定に関する情報を表示する

ONTAP SMBローカルユーザーに関する情報を表示する

すべてのローカルユーザのリストを要約形式で表示できます。特定のユーザに対して設定されているアカウント設定を確認する場合は、そのユーザの詳細なアカウント情報だけでなく、複数のユーザのアカウント情報も表示できます。この情報は、ユーザの設定を変更する必要があるかどうかを判断するのに役立ちます。また、認証やファイルアクセスに関する問題のトラブルシューティングにも役立ちます。

タスクの内容

ユーザのパスワードに関する情報は表示されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
Storage Virtual Machine（SVM）上のすべてのユーザに関する情報を表示する	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
特定のユーザの詳細なアカウント情報を表示する	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

他にも、コマンドの実行時に選択できるオプションのパラメータがあります。の詳細については `vserver cifs`、を"ONTAPコマンド リファレンス"参照してください。

例

次の例では、SVM vs1のすべてのローカルユーザに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

ローカルユーザーの**ONTAP SMB**グループメンバーシップに関する情報を表示します。

ローカルユーザが属しているローカルグループに関する情報を表示できます。この情報を使用して、ファイルやフォルダに対するユーザのアクセス権を決定できます。この情報は、ファイルやフォルダに対するユーザのアクセス権を決定する場合や、ファイルアクセスに関する問題のトラブルシューティングを行う場合に役立ちます。

タスクの内容

コマンドをカスタマイズして、必要な情報のみを表示することができます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
指定したローカルユーザのローカルユーザメンバーシップ情報を表示する	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
このローカルユーザが属しているローカルグループのローカルユーザメンバーシップ情報を表示する	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
指定したStorage Virtual Machine（SVM）に関連付けられているローカルユーザのユーザメンバーシップ情報を表示する	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
指定したSVM上のすべてのローカルユーザに関する詳細情報を表示する	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

例

次の例は、 SVM vs1 上のすべてのローカルユーザのメンバーシップ情報を表示します。ユーザ「 CIFS_SERVER\Administrator 」は「 BUILTIN\Administrators 」グループのメンバーで、「 CIFS_SERVER\sue 」は「 CIFS_SERVER\g1 」グループのメンバーです。

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

ローカル **ONTAP SMB** ユーザー アカウントを削除する

Storage Virtual Machine（SVM）に対するローカルSMB認証やSVMに格納されたデータへのアクセス権の定義に使用するローカルユーザアカウントが不要になった場合は、SVMから削除することができます。

タスクの内容

ローカルユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

  このユーザーを参照するファイルおよびディレクトリのWindowsセキュリティ記述子は調整されません。

- ローカルユーザへの参照は、メンバーシップデータベースとPrivilegesデータベースからすべて削除されます。
- 一般的な標準ユーザ（Administratorなど）は削除できません。

手順

1. 削除するローカルユーザアカウントの名前を確認します。 `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. ローカルユーザを削除します。 `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. ユーザアカウントが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

例

次の例は、 SVM vs1 に関連付けられたローカルユーザ「 `CIFS_SERVER\su` 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

ローカルグループを管理します。

ローカル **ONTAP SMB** グループを変更する

既存のローカルグループの概要を変更するには、既存のローカルグループの名前を変更するか、グループの名前を変更します。

状況	使用するコマンド
ローカルグループの概要を変更します	`vserver cifs users-and-groups local-group modify -vserver *vserver_name* -group-name *group_name* -description text`説明にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルグループの名前を変更します	`vserver cifs users-and-groups local-group rename -vserver *vserver_name* -group-name *group_name* -new-group-name *new_group_name*`

例

次の例では ' ローカル・グループの名前を 'CIFS_server\engineering' から 'CIFS_server\engineering_new' に変更します

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

次の例では ' ローカル・グループの概要を変更します

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

ONTAP SMBローカルグループに関する情報を表示する

クラスタまたは指定したStorage Virtual Machine（SVM）で設定されているすべてのローカルグループの一覧を表示できます。この情報は、SVMに格納されているデータへのファイルアクセスに関する問題やSVMのユーザ権限に関する問題のトラブルシューティングに役立ちます。

ステップ

1. 次のいずれかを実行します。

必要な情報	入力するコマンド
クラスタのすべてのローカルグループ	`vserver cifs users-and-groups local-group show`
SVMのすべてのローカルグループ	`vserver cifs users-and-groups local-group show -vserver` *vserver_name*

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。の詳細については `vserver cifs`、を"ONTAPコマンド リファレンス"参照してください。

例

次の例では、SVM vs1のすべてのローカルグループに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- ---------------------------- ----------------------------
vs1      BUILTIN\Administrators       Built-in Administrators group
vs1      BUILTIN\Backup Operators     Backup Operators group
vs1      BUILTIN\Power Users          Restricted administrative privileges
vs1      BUILTIN\Users                All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

ローカルONTAP SMBグループメンバーシップを管理します。

ローカルグループメンバーシップの管理では、ローカルユーザまたはドメインユーザの追加と削除、またはドメイングループの追加と削除を行うことができます。これは、グループに設定されたアクセス制御に基づいてデータへのアクセスを制御する場合や、ユーザにそのグループにPrivilegesを関連付ける場合に便利です。

タスクの内容

ローカルグループへのメンバーの追加に関するガイドラインは次のとおりです。

- 特殊なグループ _Everyone にユーザーを追加することはできません。
- ユーザを追加するローカルグループが存在している必要があります。
- ローカルグループにユーザを追加する前に、そのユーザが存在している必要があります。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、Data ONTAPで名前をSIDに解決できる必要があります。

ローカルグループからのメンバーの削除に関するガイドラインは次のとおりです。

- 特殊なグループ _Everyone からメンバーを削除することはできません。
- メンバーを削除するグループが存在している必要があります。
- ONTAPは、グループから削除するメンバーの名前を対応するSIDに解決できる必要があります。

ステップ

1. グループのメンバーを追加または削除します。

状況	使用するコマンド
グループへのメンバーの追加	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]`ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループに追加できます。
グループからのメンバーの削除	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]`ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループから削除することができます。

次の例は、 SVM vs1 上のローカルグループ「 `S MB_server\sue` 」とドメイングループ「 AD_DOM\dom_eng 」をローカルグループ「 `S MB_server\engineering` 」に追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

次の例は、 SVM vs1 上のローカルグループ「 `S MB_server\sue` 」と「 S MB_server\james 」からローカルユーザ「 `S MB_server\engineering` 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

関連情報

ローカルグループのメンバーに関する情報を表示する

ローカルグループのメンバーに関する**ONTAP SMB**情報を表示する

クラスタまたは指定したStorage Virtual Machine（SVM）で設定されているローカルグループのすべてのメンバーの一覧を表示できます。この情報は、ファイルアクセスの問題やユーザ権限の問題のトラブルシューティングに役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
クラスタのすべてのローカルグループのメンバー	`vserver cifs users-and-groups local-group show-members`
SVMのすべてのローカルグループのメンバー	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

例

次の例では、SVM vs1のすべてのローカルグループのメンバーに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

ローカル **ONTAP SMB** グループを削除する

Storage Virtual Machine（SVM）に関連付けられたデータへのアクセス権を定義するためのローカルグループが不要になった場合や、グループメンバーへのSVMユーザ権限

（Privileges）の割り当てに必要なくなった場合は、SVMからローカルグループを削除できます。

タスクの内容

ローカルグループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

  このグループを参照するファイルおよびディレクトリのWindowsセキュリティ記述子は調整されません。

- グループが存在しない場合はエラーが返されます。
- special_every_group は削除できません。
- BUILTIN \ Administrators *BUILTIN\Users* などの組み込みのグループは削除できません。

手順

1. SVM上のローカルグループのリストを表示して、削除するローカルグループの名前を確認します。 `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. ローカルグループを削除します。 `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. グループが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

例

次の例は、 SVM vs1 に関連付けられたローカルグループ「 CIFS_SERVER\sales 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

ローカルデータベース内の**ONTAP SMB**ドメインユーザー名とグループ名を更新する

CIFSサーバのローカルグループにドメインユーザやドメイングループを追加できます。これらのドメインオブジェクトは、クラスタのローカルデータベースに登録されます。ドメインオブジェクトの名前を変更する場合は、ローカルデータベースを手動で更新する必要があります。

タスクの内容

ドメイン名を更新するStorage Virtual Machine（SVM）の名前を指定する必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 適切な操作を実行します。

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループのうち、正常に更新されたものと更新できなかったものを表示する	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループが正常に更新されたことを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
更新に失敗したドメインユーザとドメイングループのみを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
更新に関するすべてのステータス情報を非表示にする	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、Storage Virtual Machine（SVM、旧Vserver）vs1に関連付けられているドメインユーザとドメイングループの名前を更新します。最後の更新では、依存する一連の名前を更新する必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

ローカル**Privileges**を管理します。

ONTAP SMBのローカルまたはドメインユーザーまたはグループに権限を追加する

ローカルまたはドメインのユーザやグループのユーザ権限を管理できます。追加した権限は、これらのオブジェクトに割り当てられていたデフォルトの権限よりも優先されます。これにより、ユーザまたはグループに付与する権限をカスタマイズして、セキュリティを強化できます。

開始する前に

権限を追加する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

オブジェクトに権限を追加すると、そのユーザまたはグループのデフォルトの権限は無効になります。権限を追加しても、以前に追加した権限は削除されません。

ローカルまたはドメインのユーザまたはグループに権限を追加する場合は、次の点に注意する必要があります。

- 権限は 1 つ以上追加できます。
- Privilegesをドメインユーザまたはグループに追加するときに、ONTAPがドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。

  ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに1つ以上のPrivilegesを追加します。 `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or -group-name name -privileges _privilege_[,...]`
2. 目的のPrivilegesがオブジェクトに適用されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 CIFS_SERVER\suueo 」ユーザに「 ````eTcbPrivilege] 」権限と「 `seeOwnershipPrivilege 」権限を追加します。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

ONTAP SMBのローカルまたはドメインユーザーまたはグループから権限を削除します

ローカルまたはドメインのユーザやグループのユーザ権限を管理するには、権限を削除します。これにより、ユーザとグループに付与される最大権限をカスタマイズして、セキュリティを強化できます。

開始する前に

Privilegesを削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

ローカルまたはドメインのユーザやグループの権限を削除するときは、次の点に注意してください。

- 1 つ以上の権限を削除できます。
- ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続してドメインユーザまたはグループを検証することがあります。

  ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループから1つ以上のPrivilegesを削除します。 `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 目的のPrivilegesがオブジェクトから削除されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上のユーザ「 CIFS_SERVER\suueo 」から「 `s eTcbPrivilege 」および「 `s eTakeOwnershipPrivilege 」権限を削除します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

ローカルまたはドメインのユーザやグループの権限をリセットできます。これは、ローカルまたはドメインのユーザやグループの権限に対して行った変更が不要になった場合や必要がなくなった場合に役立ちます。

タスクの内容

ローカルまたはドメインのユーザまたはグループの権限をリセットすると、そのオブジェクトの権限のエントリがすべて削除されます。

手順

1. ローカルまたはドメインのユーザまたはグループのPrivilegesをリセットします。 `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. オブジェクトでPrivilegesがリセットされたことを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上のユーザ「 CIFS_SERVER\sue 」の権限をリセットしています。デフォルトでは、標準ユーザのアカウントには権限は関連付けられません。

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

次の例では ' グループ ""BUILTIN\Administrators "" の特権をリセットし ' 実質的に特権エントリを削除します

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

ONTAP SMB権限オーバーライドに関する情報を表示する

ドメインまたはローカルのユーザアカウントまたはグループに割り当てられているカスタムPrivilegesに関する情報を表示できます。この情報は、必要なユーザー権限が適用されているかどうかを判断するのに役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
Storage Virtual Machine（SVM）のすべてのドメインおよびローカルのユーザとグループ用のカスタムPrivileges	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
SVMの特定のドメインまたはローカルのユーザとグループのカスタムPrivileges	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。の詳細については `vserver cifs users-and-groups privilege show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドは、SVM vs1のローカルまたはドメインのユーザとグループに明示的に関連付けられているすべてのPrivilegesを表示します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

トラバースチェックのバイパスの設定

ONTAP SMBバイパストラバースチェックの設定について学ぶ

トラバースチェックのバイパスは、トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできるかどうかを判断するユーザ権限です。トラバースチェックのバイパスを許可または拒否した場合の動作と、Storage Virtual Machine（SVM）でのユーザに対するトラバースチェックのバイパスの設定方法を理解しておく必要があります。

トラバースチェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとすると、中間ディレクトリのトラバース権限がONTAPでチェックされず、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、ONTAPはファイルのパスにあるすべてのディレクトリでトラバース（実行）権限をチェックします。

  中間ディレクトリのいずれかに「 X 」（トラバース権限）がない場合、 ONTAP はファイルへのアクセスを拒否します。

トラバースチェックのバイパスの設定

トラバースチェックのバイパスを設定するには、ONTAP CLIを使用するか、Active Directoryグループポリシーにこのユーザ権限を設定します。

権限は `SeChangeNotifyPrivilege`、ユーザにトラバースチェックのバイパスを許可するかどうかを制御します。

- この権限をSVMのローカルSMBユーザまたはグループ、ドメインユーザまたはグループに追加すると、トラバースチェックのバイパスを許可できます。
- この権限をSVMのローカルSMBユーザまたはグループ、ドメインユーザまたはグループから削除すると、トラバースチェックのバイパスが拒否されます。

SVMの次のBUILTINグループには、デフォルトでトラバースチェックのバイパス権限があります。

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`

- `BUILTIN\Users`
- `Everyone`

これらのいずれかのグループのメンバーにトラバースチェックのバイパスを許可しない場合は、グループからこの権限を削除する必要があります。

CLIを使用してSVMのローカルSMBユーザおよびグループのトラバースチェックのバイパスを設定する場合は、次の点に注意する必要があります。

- カスタムのローカルグループまたはドメイングループのメンバーにトラバースチェックのバイパスを許可する場合は、そのグループに権限を追加する必要があります `SeChangeNotifyPrivilege`。
- ローカルユーザまたはドメインユーザにトラバースチェックのバイパスを個別に許可し、そのユーザがその権限を持つグループのメンバーでない場合は、そのユーザアカウントに権限を追加できます `SeChangeNotifyPrivilege`。
- ローカルまたはドメインのユーザやグループに対するトラバースチェックのバイパスをいつでも無効にするには、権限を削除し `SeChangeNotifyPrivilege`ます。

> ⓘ 特定のローカルまたはドメインのユーザまたはグループに対してトラバースチェックのバイパスを無効にするには、グループから権限 `Everyone`も削除する必要があります `SeChangeNotifyPrivilege`。

関連情報

- ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する
- ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する
- ボリューム上のファイル名変換の文字マッピングを構成する
- 共有アクセス制御リストを作成する
- ストレージレベルのアクセス保護を使用したファイルアクセスの保護
- サポートされるPrivilegesのリスト
- ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加

ユーザーまたはグループが **ONTAP SMB** ディレクトリ トラバース チェックをバイパスできるようにする

トラバースするディレクトリに対する権限がない場合でも、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできるようにするには、Storage Virtual Machine（SVM）のローカルSMBユーザまたはグループに権限を追加します `SeChangeNotifyPrivilege`。デフォルトでは、ユーザはディレクトリのトラバースチェックをバイパスできます。

開始する前に

- SVM上にSMBサーバが存在している必要があります。
- ローカルユーザとローカルグループのSMBサーバオプションが有効になっている必要があります。
- 権限を追加するローカルまたはドメインのユーザまたはグループ `SeChangeNotifyPrivilege`がすでに存在している必要があります。

タスクの内容

Privilegesをドメインユーザまたはグループに追加するときに、ONTAPがドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに権限を追加して、トラバースチェックのバイパスを有効にし `SeChangeNotifyPrivilege`ます。 `vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *name* -privileges SeChangeNotifyPrivilege`

   パラメータの値は `-user-or-group-name`、ローカルユーザまたはグループ、ドメインユーザまたはグループです。

2. 指定したユーザまたはグループでトラバースチェックのバイパスが有効になっていることを確認します。 `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

例

次のコマンドは、「example\eng'」グループに権限を追加することで、「example\eng'」グループに属するユーザがディレクトリのトラバースチェックをバイパスできるようにし `SeChangeNotifyPrivilege`ます。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

関連情報

ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する

ユーザーまたはグループが **ONTAP SMB** ディレクトリ トラバース チェックをバイパスすることを禁止します

トラバースするディレクトリに対する権限がないためにファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできないようにするには、Storage Virtual Machine（SVM）のローカルSMBユーザまたはグループから権限を削除します `SeChangeNotifyPrivilege`。

開始する前に

Privilegesを削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続してドメインユーザまたはグループを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. トラバースチェックのバイパスを禁止します。 `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   コマンドは、パラメータの値で指定したローカルまたはドメインのユーザまたはグループから権限を `-user-or-group-name name`削除します `SeChangeNotifyPrivilege`。

2. 指定したユーザまたはグループに対してトラバースチェックのバイパスが無効になっていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次のコマンドを実行すると、「 EXAMPLE\eng 」グループに属するユーザに対して、ディレクトリのトラバースチェックのバイパスが禁止されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ------------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ------------------------
vs1       EXAMPLE\eng          -
```

関連情報

ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する

ファイルセキュリティと監査ポリシーに関する情報を表示する

ONTAP SMBファイルセキュリティと監査ポリシーの表示について学習します

Storage Virtual Machine（SVM）のボリュームに格納されたファイルとディレクトリのファイルセキュリティに関する情報を表示できます。FlexVolの監査ポリシーに関する情報を表示できます。設定されている場合、FlexVolボリュームのストレージレベルのアクセス保護およびダイナミックアクセス制御セキュリティの設定に関する情報を表示できます。

ファイルセキュリティに関する情報の表示

次のセキュリティ形式のボリュームおよびqtree（FlexVolボリュームの場合）に格納されたデータに適用されているファイルセキュリティに関する情報を表示できます。

- NTFS
- UNIX
- mixed

監査ポリシーに関する情報の表示

次のNASプロトコルを介したFlexVolボリュームのアクセスイベントを監査する監査ポリシーに関する情報を表示できます。

- SMB（すべてのバージョン）
- NFSv4.x

ストレージレベルのアクセス保護（**SLAG**）セキュリティに関する情報の表示

ストレージレベルのアクセス保護セキュリティは、次のセキュリティ形式のFlexVolボリュームおよびqtreeオブジェクトに適用できます。

- NTFS
- mixed
- UNIX（ボリュームが格納されたSVMでCIFSサーバが設定されている場合）

ダイナミックアクセス制御（**DAC**）セキュリティに関する情報の表示

ダイナミックアクセス制御セキュリティは、次のセキュリティ形式のFlexVol volume内のオブジェクトに適用できます。

- NTFS
- mixed（オブジェクトにNTFS対応のセキュリティが設定されている場合）

関連情報

- ストレージレベルのアクセスガードを使用した安全なファイルアクセスについて学習します
- サーバー上のストレージレベルのアクセスガードに関する情報を表示する

NTFSセキュリティ形式のボリューム上の**ONTAP SMB**ファイルセキュリティに関する情報を表示します。

セキュリティ形式と有効なセキュリティ形式、適用されている権限、DOS属性に関する情報など、NTFSセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、ファイルアクセス権の決定時にNTFSファイル権限およびWindowsのユーザおよびグループのみが使用されるため、UNIX関連の出力フィールドには表示専用のUNIXファイル権限情報が表示されます。

- ACL出力は、NTFSセキュリティが適用されたファイルとフォルダについて表示されます。
- ストレージレベルのアクセス保護セキュリティはボリュームのルートまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルACLとストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- 指定したファイルまたはディレクトリパスにダイナミックアクセス制御が設定されている場合は、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例では、SVM vs1のパスに関するセキュリティ情報を表示し `/vol4`ます。

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                 Unix Mode Bits in Text: rwxrwxrwx
                                   ACLs: NTFS Security Descriptor
                                         Control:0x8004
                                         Owner:BUILTIN\Administrators
                                         Group:BUILTIN\Administrators
                                         DACL - ACEs
                                         ALLOW-Everyone-0x1f01ff
                                         ALLOW-Everyone-0x10000000-
OI|CI|IO
```

次の例では、マスクを展開して、SVM vs1のパスに関するセキュリティ情報を表示します `/data/engineering`。

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
     File Inode Number: 5544
        Security Style: ntfs
       Effective Style: ntfs
        DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
```

```
                        DACL - ACEs
                          ALLOW-Everyone-0x1f01ff
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...0 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
```

```
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...1 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...0 .... .... .... .... .... =
Synchronize
                           .... .... .... 0... .... .... .... .... =
Write Owner
                           .... .... .... .0.. .... .... .... .... =
Write DAC
                           .... .... .... ..0. .... .... .... .... =
Read Control
                           .... .... .... ...0 .... .... .... .... =
Delete
                           .... .... .... .... .... ...0 .... .... =
Write Attributes
                           .... .... .... .... .... .... 0... .... =
Read Attributes
                           .... .... .... .... .... .... .0.. .... =
Delete Child
                           .... .... .... .... .... .... ..0. .... =
Execute
                           .... .... .... .... .... .... ...0 .... =
Write EA
                           .... .... .... .... .... .... .... 0... =
Read EA
                           .... .... .... .... .... .... .... .0.. =
Append
                           .... .... .... .... .... .... .... ..0. =
Write
                           .... .... .... .... .... .... .... ...0 =
Read
```

次の例では、SVM vs1のパスにあるボリュームの、ストレージレベルのアクセス保護セキュリティ情報を含むセキュリティ情報を表示します `/datavol1`。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

関連情報

- mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示
- UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、mixedセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびフォルダと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。
- mixedセキュリティ形式のボリュームの最上位では、UNIX対応またはNTFS対応のセキュリティを設定できます。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、mixedセキュリティ形式のボリュームまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、UNIXファイル権限とストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例では、マスクを展開した形式で、SVM vs1のパスに関するセキュリティ情報を表示します

/projects。このmixedセキュリティ形式のパスには、UNIX対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

次の例は、SVM vs1のパスに関するセキュリティ情報を表示します /data。このmixedセキュリティ形式のパスには、NTFS対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                 Unix Mode Bits in Text: rwxrwxrwx
                                   ACLs: NTFS Security Descriptor
                                         Control:0x8004
                                         Owner:BUILTIN\Administrators
                                         Group:BUILTIN\Administrators
                                         DACL - ACEs
                                           ALLOW-Everyone-0x1f01ff
                                           ALLOW-Everyone-0x10000000-
OI|CI|IO
```

次の例では、SVM vs1のパスにあるボリュームに関するセキュリティ情報を表示します `/datavol5`。このmixedセキュリティ形式のボリュームの最上位には、UNIX対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

関連情報

- NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示
- UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

UNIXセキュリティ形式のボリューム上の**ONTAP SMB**ファイルセキュリティに関する情報を表示します。

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、UNIXセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリ

ティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを指定する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- ファイルアクセス権の決定時に、UNIXセキュリティ形式のボリュームおよびqtreeでは、UNIXファイル権限（モードビットまたはNFSv4 ACL）のみが使用されます。
- ACL出力は、NFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NFSv4セキュリティ記述子の場合は適用されません。

  NTFSセキュリティ記述子でのみ意味があります。

- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、パラメータで指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります `-path`。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細を表示	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1のパスに関するセキュリティ情報を表示し `/home`ます。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

次の例では、マスクを展開した形式で、SVM vs1のパスに関するセキュリティ情報を表示します `/home`。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                        Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

関連情報

- セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します
- mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

SMB FlexVol ボリューム上の **NTFS** 監査ポリシーに関する情報を表示する **ONTAP** コマンド

セキュリティ形式と有効なセキュリティ形式、適用されている権限、システムアクセス制御リストに関する情報など、FlexVolのNTFS監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、NTFSのシステムアクセス制御リスト（SACL）のみが監査ポリシーに使用されます。
- NTFS対応のセキュリティが有効なmixedセキュリティ形式のボリューム内のファイルやフォルダには、NTFS監査ポリシーを適用できます。

  mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixedセキュリティ形式のボリュームの最上位には、UNIX対応またはNTFS対応のセキュリティを設定でき、NTFS SACLが格納されている場合と格納されていない場合があります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、mixedセキュリティ形式のボリュームまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルおよびフォルダのNFSv4 SACLとストレージレベルのアクセス保護NTFS SACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。
- NTFS対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、UNIX関連の出力フィールドに表示専用のUNIXファイル権限情報が表示されます。

  ファイルアクセス権の決定時に、NTFSセキュリティ形式のファイルおよびフォルダでは、NTFSファイル権限とWindowsユーザおよびグループのみが使用されます。

- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルやフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。

ステップ

1. ファイルおよびディレクトリ監査ポリシーの設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリスト	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/corp`。パスにはNTFS対応のセキュリティが設定されています。NTFSセキュリティ記述子には、SUCCESSおよびSUCCESS / FAIL SACLエントリの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/datavol1`。このパスには、通常のファイルとフォルダのSACLとストレージレベルのアクセス保護のSACLの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

SMB FlexVol ボリューム上の **NFSv4** 監査ポリシーに関する情報を表示する **ONTAP** コマンド

セキュリティ形式と有効なセキュリティ形式、適用されている権限、システムアクセス制御リスト（ SACL ）に関する情報など、 ONTAP CLI を使用して FlexVol の NFSv4 監

査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine （ SVM ）の名前、および監査情報を表示するファイルまたはディレクトリのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- UNIX セキュリティ形式のボリュームおよび qtree では、監査ポリシーに NFSv4 SACL のみが使用されます。
- mixed セキュリティ形式のボリュームにある UNIX セキュリティ形式のファイルとディレクトリには、NFSv4 監査ポリシーを適用できます。

  mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixed セキュリティ形式のボリュームの最上位では、 UNIX または NTFS 対応のセキュリティを有効にすることができ、 NFSv4 SACL が含まれる場合と含まれない場合があります。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルやフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、 mixed セキュリティ形式のボリュームまたは qtree で設定できるため、 ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、標準の NFSv4 ファイルおよびディレクトリの SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、パラメータで指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります `-path`。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスに関するセキュリティ情報を表示します `/lab`。この UNIX セキュリティ形式のパスには NFSv4 SACL が設定されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

ONTAP SMBファイルのセキュリティと監査ポリシー情報を表示する方法を学びます

ワイルドカード文字（*）を使用すると、特定のパスまたはルートボリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関する情報を表示できます。

ワイルドカード文字（*）は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。「*」という名前の特定のファイルまたはディレクトリの情報を表示する場合は、二重引用符（「`」）で完全なパスを指定する必要があります。

例

次のコマンドでワイルドカード文字を使用すると、SVM vs1のパスの下にあるすべてのファイルとディレクトリに関する情報が表示され `/1/` ます。

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0x8514
                            Owner:BUILTIN\Administrators
                            Group:BUILTIN\Administrators
                            DACL - ACEs
                            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0x8404
                            Owner:BUILTIN\Administrators
                            Group:BUILTIN\Administrators
                            DACL - ACEs
                            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

次のコマンドは、SVM vs1のパスの下にある「*」という名前のファイルの情報を表示します `/vol1/a`。パスは二重引用符（ "" ）で囲まれます。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

CLIを使用して、**SVM**の**NTFS**ファイルセキュリティ、**NTFS**監査ポリシー、ストレージレベルのアクセス保護を管理します。

SMB NTFSファイルセキュリティ、**NTFS**監査ポリシー、ストレージレベルアクセスガードを管理するための**ONTAP**コマンド

CLIを使用して、Storage Virtual Machine（SVM）のNTFSファイルセキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護を管理できます。

NTFSファイルセキュリティと監査ポリシーは、SMBクライアントから、またはCLIを使用して管理できます。ただし、CLIを使用してファイルセキュリティと監査ポリシーを設定すると、リモートクライアントを使用してファイルセキュリティを管理する必要がなくなります。CLIを使用すると、1つのコマンドで多数のファイルやフォルダにセキュリティを適用する時間を大幅に短縮できます。

ONTAPがSVMボリュームに適用するもう1つのセキュリティレイヤであるストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護は、すべてのNASプロトコルからストレージレベルのアクセス保護が適用されるストレージオブジェクトへのアクセスに適用されます。

ストレージレベルのアクセス保護は、ONTAP CLIからのみ設定および管理できます。ストレージレベルのアクセス保護設定をSMBクライアントから管理することはできません。さらに、NFSまたはSMBクライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護セキュリティは表示されません。システム（WindowsまたはUNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が個別に設定および管理できる、データアクセスのセキュリティレイヤを強化します。

ストレージレベルのアクセス保護ではNTFSのアクセス権限のみがサポートされますが、ストレージレベルのアクセス保護が適用されているボリューム上のデータへのNFS経由のアクセスについては、そのボリュームを所有するSVM上のWindowsユーザにUNIXユーザがマッピングされている場合にONTAPでセキュリティチェックを実行できます。

NTFSセキュリティ形式のボリューム

NTFSセキュリティ形式のボリュームやqtreeに格納されているファイルやフォルダでは、すべてNTFS対応のセキュリティが有効になります。コマンドファミリーを使用すると、NTFSセキュリティ形式のボリュームに次の種類のセキュリティを実装でき `vserver security file-directory`ます。

- ボリュームに含まれるファイルとフォルダに対するファイル権限と監査ポリシー
- ボリュームに対するストレージレベルのアクセス保護セキュリティ

mixedセキュリティ形式のボリューム

mixedセキュリティ形式のボリュームやqtreeには、UNIX対応のセキュリティが有効で、UNIXファイル権限（モードビットまたはNFSv4.x ACL）とNFSv4.x監査ポリシーを使用するファイルやフォルダ、およびNTFS対応のセキュリティが有効でNTFSファイル権限と監査ポリシーを使用するファイルやフォルダを格納できます。コマンドファミリーを使用すると、mixedセキュリティ形式のデータに次の種類のセキュリティを適用でき `vserver security file-directory`ます。

- mixed形式のボリュームまたはqtreeにおけるNTFS対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- NTFS対応またはUNIX対応のセキュリティ形式のボリュームに対するストレージレベルのアクセス保護

UNIXセキュリティ形式のボリューム

UNIXセキュリティ形式のボリュームおよびqtreeには、UNIX対応のセキュリティ（モードビットまたはNFSv4.x ACL）が設定されたファイルおよびフォルダが格納されます。コマンドファミリーを使用してUNIXセキュリティ形式のボリュームにセキュリティを実装する場合は、次の点に注意する必要があり `vserver security file-directory`ます。

- UNIXセキュリティ形式のボリュームおよびqtreeでは、 `vserver security file-directory`コマンドファミリーを使用してUNIXファイルセキュリティおよび監査ポリシーを管理することはできません。
- ターゲットボリュームを含むSVMにCIFSサーバが含まれている場合は、コマンドファミリーを使用してUNIXセキュリティ形式のボリュームにストレージレベルのアクセス保護を設定できます `vserver security file-directory`。

関連情報

- ファイルのセキュリティと監査ポリシーの表示について学習します
- サーバーにNTFSセキュリティ記述子を作成する
- ファイルとフォルダに監査ポリシーを設定および適用するためのコマンド
- ストレージレベルのアクセスガードを使用した安全なファイルアクセスについて学習します

SMBファイルとフォルダのセキュリティを設定するための**ONTAP**コマンド

ファイルおよびフォルダのセキュリティは、リモートクライアントを使用せずにローカ

ルで適用および管理できるため、多数のファイルまたはフォルダに対して一括でセキュリティを設定する場合に比べて大幅に時間を短縮できます。

CLI を使用してファイルおよびフォルダのセキュリティを設定すると効果的な状況として、次のようなユースケースがあります。

- ホームディレクトリ内のファイルストレージなど、大規模なエンタープライズ環境のファイルの格納
- データの移行
- Windowsドメインの変更
- NTFS ファイルシステムのファイルセキュリティと監査ポリシーの標準化

ONTAPコマンドを使用して**SMB**ファイルとフォルダのセキュリティを設定する際の制限について学習します

CLIを使用してファイルおよびフォルダのセキュリティを設定する場合は、一定の制限事項に注意する必要があります。

- `vserver security file-directory`コマンドファミリーはNFSv4 ACLの設定をサポートしていません。

  NTFSセキュリティ記述子は、NTFSファイルおよびNTFSフォルダにのみ適用できます。

セキュリティ記述子を使用して **ONTAP SMB** ファイルおよびフォルダのセキュリティを適用する

セキュリティ記述子には、ユーザがファイルやフォルダに対して実行できる操作、およびユーザがファイルやフォルダにアクセスするときに監査される内容を決定するアクセス制御リストが含まれます。

- * 権限 *

  権限はオブジェクトの所有者によって許可または拒否され、オブジェクト（ユーザ、グループ、またはコンピュータオブジェクト）が指定されたファイルまたはフォルダに対して実行できる操作を決定します。

- * セキュリティ記述子 *

  セキュリティ記述子は、ファイルまたはフォルダに関連付けられた権限を定義するセキュリティ情報を含むデータ構造です。

- * アクセス制御リスト (ACL) *

  アクセス制御リストは、セキュリティ記述子内に含まれるリストで、セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータオブジェクトが実行できる操作に関する情報が含まれます。セキュリティ記述子には、次の2種類のACLを含めることができます。

  ◦ Discretionary Access Control List （ DACL ；随意アクセス制御リスト）

  ◦ システムアクセスセイギョリスト SACL

- * 随意アクセス制御リスト（ DACL ） *

  DACLには、ファイルまたはフォルダに対してアクションを実行するためのアクセスを許可または拒否するユーザ、グループ、およびコンピュータオブジェクトのSIDリストが含まれます。DACLには0個以上

のAccess Control Entry（ACE；アクセス制御エントリ）が含まれます。

- * システム・アクセス・コントロール・リスト（ SACL ） *

  SACLには、成功または失敗した監査イベントがログに記録されるユーザ、グループ、およびコンピュータオブジェクトのSIDリストが含まれます。SACLには0個以上のAccess Control Entry（ACE；アクセス制御エントリ）が含まれます。

- * アクセス制御エントリ (ACE) *

  ACEは、DACLまたはSACLの個 々 のエントリです。

  - DACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトに対して許可または拒否されるアクセス権を指定します。
  - SACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトによって実行される指定された操作の監査時にログに記録される成功または失敗イベントを指定します。

- * 権限の継承 *

  権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトにパーミッションを設定する際に、「適用先」、 `sub-folders`「ファイル」でフォルダ、サブフォルダ、およびファイルを継承できるかどうかを指定できます `this-folder`。

関連情報

- "SMBおよびNFSの監査とセキュリティトレース"
- ファイルとフォルダに監査ポリシーを設定および適用するためのコマンド

ONTAP SVMディザスタリカバリ先でローカル**SMB**ユーザーまたはグループを使用するファイルディレクトリポリシーを適用する方法について説明します。

ファイルとディレクトリのポリシー設定でセキュリティ記述子、DACL、SACLエントリのいずれかでローカルユーザまたはグループを使用する場合、ID破棄設定のStorage Virtual Machine（SVM）ディザスタリカバリデスティネーションでファイルとディレクトリのポリシーを適用する前に注意する必要がある一定のガイドラインがあります。

ソースクラスタのソース SVM が、ソース SVM からデスティネーションクラスタのデスティネーション SVM にデータと設定をレプリケートする SVM ディザスタリカバリ構成を設定できます。

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます

  この設定では、 SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

  この設定では、 SVM と CIFS サーバの ID が維持されません。このシナリオでは、デスティネーション SVM の SVM と CIFS サーバの名前は、ソース SVM の SVM と CIFS サーバの名前と異なります。

ID 破棄設定に関するガイドライン

ID 破棄設定では、ローカルユーザ、グループ、権限設定を含む SVM ソースを SVM デスティネーションの CIFS サーバ名に一致するようにローカルドメインの名前（ローカル CIFS サーバ名）を変更する必要があります。たとえば、ソース SVM 名が「 vs1 」で CIFS サーバ名が「 CIFS1 」、デスティネーション SVM 名が「 vs1_dst 」で CIFS サーバ名が「 CIFS1_DST` 」の場合、ローカルユーザ「 CIFS1\user1 」のローカルドメイン名は「 CIFS1_DST` デスティネーション SVM 」で自動的に「 CIFS1_DST\user1 」に変更されます。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                 Full Name      Description
------------ ------------------------- -------------- -------------
vs1          CIFS1\Administrator                      Built-in
administrator account
vs1          CIFS1\user1               -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                 Full Name      Description
------------ ------------------------- -------------- -------------
vs1_dst      CIFS1_DST\Administrator                  Built-in
administrator account
vs1_dst      CIFS1_DST\user1           -              -
```

ローカルユーザおよびグループデータベースでローカルユーザおよびグループ名が自動的に変更されても、ファイルとディレクトリのポリシー設定（コマンドファミリーを使用してCLIで設定するポリシー）のローカルユーザまたはグループ名は自動的に変更されません `vserver security file-directory`。

たとえば、「vs1」について、パラメータが「`CIFS1\user1`」に設定されたDACLエントリを設定している場合 `-account`、デスティネーションSVMで設定がデスティネーションのCIFSサーバ名を反映するように自動的に変更されることはありません。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

CIFSサーバ名を手動でデスティネーションCIFSサーバ名に変更するには、コマンドを使用する必要があります `vserver security file-directory modify`。

アカウントパラメータを含むファイルとディレクトリのポリシー設定コンポーネント

ローカルユーザまたはグループを含むパラメータ設定を使用できるファイルとディレクトリのポリシー設定コンポーネントは 3 つあります。

- セキュリティ記述子

  必要に応じて、セキュリティ記述子の所有者とセキュリティ記述子の所有者のプライマリグループを指定できます。セキュリティ記述子で所有者とプライマリグループのエントリにローカルユーザまたはグループを使用する場合、デスティネーション SVM にアカウント名を使用するようにセキュリティ記述子を変更する必要があります。アカウント名に必要な変更を加えるには、コマンドを使用し `vserver security file-directory ntfs modify`ます。

- DACLエントリ

  各DACLエントリは、アカウントに関連付ける必要があります。ローカルユーザまたはグループアカウントを使用する DACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存のDACLエントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべてのDACLエントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しいDACLエントリを作成し、それらの新しいDACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

- SACLエントリ

  各SACLエントリは、アカウントに関連付ける必要があります。ローカルユーザまたはグループアカウン

トを使用する SACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存のSACLエントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべてのSACLエントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しいSACLエントリを作成し、それらの新しいSACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

ポリシーを適用する前に、ファイルとディレクトリのポリシー設定で使用されているローカルユーザまたはグループに必要な変更を行う必要があります。そうしないと、適用ジョブは失敗します。

CLIを使用した**NTFS**ファイルおよびフォルダに対するファイルセキュリティの設定と適用

ONTAP SMBサーバーに**NTFS**セキュリティ記述子を作成する

NTFS セキュリティ記述子（ファイルセキュリティポリシー）の作成は、 Storage Virtual Machine （ SVM ）内のファイルやフォルダの NTFS Access Control List （ ACL ；アクセス制御リスト）を設定および適用するための最初のステップです。セキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けることができます。

タスクの内容

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4つのデフォルトACEは次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み\管理者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込み\ユーザ	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者所有者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、を

"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBサーバ上の**NTFS**セキュリティ記述子に**NTFS DACL**アクセス制御エントリを追加する

NTFS セキュリティ記述子への随意アクセス制御リスト（ DACL ）のアクセス制御エントリ（ ACE ）の追加は、ファイルまたはフォルダに対する NTFS ACL の設定および適用における 2 番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、 ACE で定義されているファイルまたはフォルダに対してオブジェクトが実行できる操作または実行できない操作が定義されます。

タスクの内容

セキュリティ記述子のDACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるDACLに既存のACEがある場合は、新しいACEがDACLに追加されます。セキュリティ記述子にDACLが含まれていない場合は、DACLが作成されて新しいACEが追加されます。

必要に応じて、パラメータで指定したアカウントに対して許可または拒否する権限を指定することで、DACLエントリをカスタマイズでき `-account`ます。権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権限
- 詳細な権限
- raw 権限（ advanced 権限）

DACLエントリの権限を指定しない場合、権限はデフォルトでに設定され `Full Control`ます。

必要に応じて、継承の適用方法を指定することで、 DACL エントリをカスタマイズできます。

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

手順

1. セキュリティ記述子にDACLエントリを追加します。 `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. DACLエントリが正しいことを確認します。 `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
          Account Name or SID: DOMAIN\joe
                Access Rights: full-control
        Advanced Access Rights: -
                     Apply To: this-folder
                Access Rights: full-control
```

の詳細については `vserver security file-directory ntfs dacl`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBセキュリティポリシーを作成する

SVM のファイルセキュリティポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

タスクの内容

セキュリティポリシーに追加するタスクには、 NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFSセキュリティ形式またはmixedセキュリティ形式のボリュームを含む各SVMに関連付ける必要があります。

手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

ONTAP SMBセキュリティポリシーにタスクを追加する

ACL を設定し、 SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、 1 つ以上のタスクエントリを追加できます。

タスクの内容

セキュリティポリシーはタスクのコンテナです。タスクとは、 NTFS または mixed セキュリティが設定されたファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

  指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10 、 000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

  ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

セキュリティポリシーにタスクを追加する際には、次の 4 つの必須パラメータを指定する必要があります。

- SVM名
- ポリシー名
- パス
- パスに関連付けるセキュリティ記述子

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード

- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory`は、パラメータのデフォルト値 `-access-control`です。ファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access            Security   NTFS        NTFS
   Security
            Path           Control           Type       Mode
   Descriptor Name
   -----    --------       -----------       --------   ------
   -----------------
   1        /home/dir1     file-directory    ntfs       propagate   sd2
   ```

の詳細については `vserver security file-directory policy task`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBセキュリティポリシーを適用する

SVM へのファイルセキュリティポリシーの適用は、ファイルまたはフォルダに対して NTFS ACL を作成および適用する最後のステップです。

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在するNTFSファイルおよびフォルダに適用できます。

監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

ONTAP SMBセキュリティポリシージョブを監視する

Storage Virtual Machine （ SVM ）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

タスクの内容

セキュリティポリシージョブに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

ONTAP SMBファイルのセキュリティを確認する

Storage Virtual Machine （ SVM ）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

タスクの内容

データが格納されている SVM の名前、およびセキュリティ設定を確認するファイルとフォルダのパスを指定する必要があります。オプションのパラメータを使用すると、セキュリティ設定に関する詳細情報を表示できます `-expand-mask`。

ステップ

1. ファイルとフォルダのセキュリティ設定を表示します。 `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

   ```
            Vserver: vs1
                 File Path: /data/engineering
         File Inode Number: 5544
            Security Style: ntfs
           Effective Style: ntfs
            DOS Attributes: 10
    DOS Attributes in Text: ----D---
   Expanded Dos Attributes: 0x10
        ...0 .... .... .... = Offline
        .... ..0. .... .... = Sparse
        .... .... 0... .... = Normal
        .... .... ..0. .... = Archive
        .... .... ...1 .... = Directory
        .... .... .... .0.. = System
        .... .... .... ..0. = Hidden
        .... .... .... ...0 = Read Only
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0x8004

                                1... .... .... .... = Self Relative
                                .0.. .... .... .... = RM Control Valid
                                ..0. .... .... .... = SACL Protected
                                ...0 .... .... .... = DACL Protected
                                .... 0... .... .... = SACL Inherited
                                .... .0.. .... .... = DACL Inherited
                                .... ..0. .... .... = SACL Inherit Required
                                .... ...0 .... .... = DACL Inherit Required
                                .... .... ..0. .... = SACL Defaulted
                                .... .... ...0 .... = SACL Present
                                .... .... .... 0... = DACL Defaulted
   ```

```
                            .... .... .... .1.. = DACL Present
                            .... .... .... ..0. = Group Defaulted
                            .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read
```

```
                           ALLOW-Everyone-0x10000000-OI|CI|IO
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...1 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...0 .... .... .... .... .... =
Synchronize
                             .... .... .... 0... .... .... .... .... =
Write Owner
                             .... .... .... .0.. .... .... .... .... =
Write DAC
                             .... .... .... ..0. .... .... .... .... =
Read Control
                             .... .... .... ...0 .... .... .... .... =
Delete
                             .... .... .... .... .... ...0 .... .... =
Write Attributes
                             .... .... .... .... .... .... 0... .... =
Read Attributes
                             .... .... .... .... .... .... .0.. .... =
Delete Child
                             .... .... .... .... .... .... ..0. .... =
Execute
                             .... .... .... .... .... .... ...0 .... =
Write EA
                             .... .... .... .... .... .... .... 0... =
Read EA
                             .... .... .... .... .... .... .... .0.. =
Append
                             .... .... .... .... .... .... .... ..0. =
Write
                             .... .... .... .... .... .... .... ...0 =
Read
```

CLIを使用した監査ポリシーの設定と**NTFS**ファイルおよびフォルダへの適用

SMB監査ポリシーをNTFSファイルとフォルダに設定して適用するためのONTAPコマンド

ONTAP CLIを使用してNTFSファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、NTFSセキュリティ記述子を作成し、そのセキュリティ記述子にSACLを追加します。次に、セキュリティポリシーを作成し、ポリシータスクを追加します。その後、そのセキュリティポリシーをStorage Virtual Machine（SVM）に適用します。

タスクの内容

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視し、適用した監査ポリシーの設定を確認できます。

> 監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

関連情報

- ストレージレベルのアクセスガードを使用した安全なファイルアクセスについて学習します
- SMBファイルとフォルダのセキュリティを設定するコマンドを使用する際の制限について学習します
- セキュリティ記述子を使用してファイルとフォルダのセキュリティを適用する
- "SMBおよびNFSの監査とセキュリティトレース"
- サーバーにNTFSセキュリティ記述子を作成する

ONTAP SMBサーバーにNTFSセキュリティ記述子を作成する

NTFS セキュリティ記述子監査ポリシーの作成は、 SVM 内のファイルやフォルダの NTFS Access Control List （ ACL ；アクセス制御リスト）を設定および適用するための最初のステップです。このセキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けます。

タスクの内容

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4つのデフォルトACEは次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み\管理者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込み\ユーザ	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
作成者所有者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

手順

1. advancedパラメータを使用する場合は、権限レベルをadvancedに設定します。 `set -privilege advanced`
2. セキュリティ記述子を作成します。 `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                        Security Descriptor Name: sd1
                  Owner of the Security Descriptor: DOMAIN\joe
   ```

4. advanced権限レベルの場合は、admin権限レベルに戻ります。 `set -privilege admin`

ONTAP SMBサーバ上の**NTFS**セキュリティ記述子に**NTFS SACL**アクセス制御エントリを追加する

NTFS セキュリティ記述子への SACL （システムアクセス制御リスト）アクセス制御エントリ（ ACE ）の追加は、 SVM 内のファイルやフォルダに対する NTFS 監査ポリシーを作成する 2 番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。SACL エントリは、成功したアクセス試行と失敗したアクセス試行のどちらを監査するかを定義します。

タスクの内容

セキュリティ記述子のSACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるSACLに既存のACEがある場合は、新しいACEがSACLに追加されます。セキュリティ記述子にSACLが含まれていない場合は、SACLが作成されて新しいACEが追加されます。

SACLエントリを設定するには、パラメータで指定したアカウントの成功イベントまたは失敗イベントについて監査する権限を指定し `-account`ます。権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権限
- 詳細な権限
- raw 権限（ advanced 権限）

SACLエントリの権限を指定しない場合のデフォルト設定はです `Full Control`。

必要に応じて、パラメータで継承を適用する方法を指定して、SACLエントリをカスタマイズでき `apply to`ます。このパラメータを指定しない場合、デフォルトでは、この SACL エントリがこのフォルダ、サブフォルダ、およびファイルに適用されます。

手順

1. SACLエントリをセキュリティ記述子に追加します。 `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. SACLエントリが正しいことを確認します。 `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                   Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                   Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

ONTAP SMBセキュリティポリシーを作成する

Storage Virtual Machine （ SVM ）の監査ポリシーの作成は、ファイルまたはフォルダに

対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

タスクの内容

セキュリティポリシーに追加するタスクには、 NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFSセキュリティ形式のボリュームまたはmixedセキュリティ形式のボリュームを含むStorage Virtual Machine（SVM）ごとに関連付ける必要があります。

手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver vs1
   ```

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

   ```
   vserver security file-directory policy show
      Vserver           Policy Name
    ------------      --------------
        vs1               policy1
   ```

ONTAP SMBセキュリティポリシーにタスクを追加する

ACL を設定し、 SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1 つ以上のタスクエントリを追加できます。

タスクの内容

セキュリティポリシーはタスクのコンテナです。タスクとは、 NTFS または mixed セキュリティが設定されたファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

  指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理で

きます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10 、 000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

  ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory`は、パラメータのデフォルト値 `-access-control`です。ファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

の詳細については `vserver security file-directory policy task`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBセキュリティポリシーを適用する

SVMへの監査ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在するNTFSファイルおよびフォルダに適用できます。

> ⓘ 監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

ONTAP SMBセキュリティポリシージョブを監視する

Storage Virtual Machine （ SVM ）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフ

ォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

タスクの内容

セキュリティポリシージョブに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

ONTAP SMB監査ポリシーを確認する

Storage Virtual Machine （ SVM ）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりになっているかを確認するには、監査ポリシーを確認します。

タスクの内容

監査ポリシーの情報を表示するには、コマンドを使用し `vserver security file-directory show`ます。データが格納されている SVM の名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

ステップ

1. 監査ポリシーの設定を表示します。 `vserver security file-directory show -vserver vserver_name -path path`

例

次のコマンドは、 SVM vs1 のパス「 `/corp` 」に適用されている監査ポリシーの情報を表示します。このパスには、 SUCCESS と SUCCESS/FAIL SACL の両方のエントリが適用されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

ONTAP SMBセキュリティポリシージョブの管理について学ぶ

セキュリティポリシージョブが存在する場合、特定の状況下では、そのセキュリティポリシーやポリシーに割り当てられたタスクを変更できません。セキュリティポリシーの変更が確実に成功するように、ポリシーを変更できる条件やできない条件を理解しておく必要があります。ポリシーの変更には、ポリシーに割り当てられたタスクの追加、削除、変更と、ポリシーの削除または変更が含まれます。

セキュリティポリシーにジョブが存在し、そのジョブが次の状態の場合、そのポリシーまたはポリシーに割り当てられたタスクは変更できません。

- ジョブが実行中または実行中です。
- ジョブが一時停止中の場合
- ジョブが再開され、実行中の状態になります。
- ジョブが別のノードへのフェイルオーバーを待機中の場合。

セキュリティポリシーにジョブが存在する場合、次の状況下では、そのセキュリティポリシーまたはポリシーに割り当てられたタスクを正常に変更できます。

- ポリシージョブが停止されました。
- ポリシージョブが正常に終了しました。

SMBサーバー上のNTFSセキュリティ記述子を管理するためのONTAPコマンド

ONTAP には、セキュリティ記述子を管理するためのコマンドが用意されています。セキュリティ記述子を作成、変更、削除、および表示できます。

状況	使用するコマンド
NTFS セキュリティ記述子を作成します	`vserver security file-directory ntfs create`
既存の NTFS セキュリティ記述子を変更します	`vserver security file-directory ntfs modify`
既存の NTFS セキュリティ記述子に関する情報を表示します	`vserver security file-directory ntfs show`
NTFS セキュリティ記述子を削除します	`vserver security file-directory ntfs delete`

の詳細については `vserver security file-directory ntfs`、を"ONTAPコマンド リファレンス"参照してください。

SMBサーバー上のNTFS DACLアクセス制御エントリを管理するためのONTAPコマンド

ONTAPには、DACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS DACL に追加できます。また、DACLのACEを変更、削除、および情報表示することで、既存のNTFS DACLを管理することもできます。

状況	使用するコマンド
ACE を作成して NTFS DACL に追加します	`vserver security file-directory ntfs dacl add`
NTFS DACL の既存の ACE の変更	`vserver security file-directory ntfs dacl modify`
NTFS DACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs dacl show`
NTFS DACL から既存の ACE を削除します	`vserver security file-directory ntfs dacl remove`

の詳細については `vserver security file-directory ntfs dacl`、を"ONTAPコマンド リファレン

ス"参照してください。

SMBサーバー上のNTFS SACLアクセス制御エントリを管理するためのONTAPコマンド

ONTAPには、SACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS SACL に追加できます。また、SACLのACEを変更、削除、および情報表示することで、既存のNTFS SACLを管理することもできます。

状況	使用するコマンド
ACE を作成して NTFS SACL に追加します	`vserver security file-directory ntfs sacl add`
NTFS SACL の既存の ACE の変更	`vserver security file-directory ntfs sacl modify`
NTFS SACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs sacl show`
NTFS SACL から既存の ACE を削除します	`vserver security file-directory ntfs sacl remove`

の詳細については `vserver security file-directory ntfs sacl`、を"ONTAPコマンド リファレンス"参照してください。

SMBセキュリティポリシーを管理するためのONTAPコマンド

ONTAP には、セキュリティポリシーを管理するためのコマンドが用意されています。ポリシーに関する情報を表示したり、ポリシーを削除したりできます。セキュリティポリシーは変更できません。

状況	使用するコマンド
セキュリティポリシーを作成する	`vserver security file-directory policy create`
セキュリティポリシーに関する情報を表示します	`vserver security file-directory policy show`
セキュリティポリシーを削除する	`vserver security file-directory policy delete`

の詳細については `vserver security file-directory policy`、を"ONTAPコマンド リファレンス"参照してください。

SMBセキュリティポリシータスクを管理するためのONTAPコマンド

セキュリティポリシータスクに関する情報を追加、変更、削除、および表示するためのONTAPコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシータスクを追加する	`vserver security file-directory policy task add`
セキュリティポリシータスクを変更する	`vserver security file-directory policy task modify`
セキュリティポリシータスクに関する情報を表示します	`vserver security file-directory policy task show`
セキュリティポリシータスクを削除する	`vserver security file-directory policy task remove`

の詳細については `vserver security file-directory policy task`、を"ONTAPコマンド リファレンス"参照してください。

SMBセキュリティポリシージョブを管理するためのONTAPコマンド

ONTAP には、セキュリティポリシージョブを一時停止、再開、停止、および関連する情報を表示するためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシージョブを一時停止します	`vserver security file-directory job pause -vserver vserver_name -id integer`
セキュリティポリシージョブを再開します	`vserver security file-directory job resume -vserver vserver_name -id integer`
セキュリティポリシージョブに関する情報を表示します	`vserver security file-directory job show -vserver vserver_name`このコマンドを使用して、ジョブのジョブIDを確認できます。
セキュリティポリシージョブを停止します	`vserver security file-directory job stop -vserver vserver_name -id integer`

の詳細については `vserver security file-directory job`、を"ONTAPコマンド リファレンス"参照してください。

SMB共有のメタデータキャッシュの設定

ONTAP SMBメタデータキャッシュについて学ぶ

メタデータのキャッシングにより、 SMB 1.0 クライアントでファイル属性をキャッシュして、ファイル属性およびフォルダ属性にすばやくアクセスできるようになります。属性のキャッシュは、共有ごとに有効または無効にすることができます。メタデータのキャッシングが有効な場合は、キャッシュされたエントリの TTL を設定することもできます。クライアントが SMB 2.x または SMB 3.0 で共有に接続している場合は、メタデータキャッシュの設定は必要ありません。

SMB メタデータのキャッシングを有効にすると、パスとファイルの属性データが一定期間保存されます。これにより、一般的なワークロードでの SMB 1.0 クライアントの SMB パフォーマンスを向上させることができます。

特定のタスクでは、 SMB によって大量のトラフィックが作成され、そのトラフィックにはパスとファイルのメタデータに対する複数の同一クエリが含まれることがあります。代わりに、 SMB メタデータのキャッシングを使用してキャッシュから情報を読み込むことで、重複するクエリの数を減らし、 SMB 1.0 クライアントのパフォーマンスを向上させることができます。

メタデータのキャッシングを使用すると、ごくまれに、古い情報が SMB 1.0 クライアントに提供されることがあります。ご使用の環境でこのリスクを回避する必要がある場合は、この機能を有効にしないでください。

ONTAP SMBメタデータキャッシュを有効にする

SMBメタデータのキャッシュを有効にすることで、SMB 1.0クライアントのSMBパフォーマンスを向上させることができます。デフォルトでは、SMBメタデータのキャッシングは無効になっています。

ステップ

1. 必要な操作を実行します。

状況	入力するコマンド
共有の作成時にSMBメタデータのキャッシングを有効にする	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
既存の共有でSMBメタデータのキャッシングを有効にする	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

関連情報

- メタデータキャッシュエントリの有効期間を構成する

- 既存の共有の共有プロパティを追加または削除する

ONTAP SMBメタデータキャッシュエントリの有効期間を設定する

SMB メタデータキャッシュエントリの有効期間を設定できます。これにより、環境内での SMB メタデータキャッシュのパフォーマンスを最適化できます。デフォルトは10秒です。

開始する前に

SMB メタデータキャッシュ機能を有効にしている必要があります。SMB メタデータのキャッシングが有効でない場合、 SMB キャッシュの TTL 設定は使用されません。

ステップ

1. 必要な操作を実行します。

SMB メタデータキャッシュエントリの有効期間を設定する際の方法	入力するコマンド
共有を作成する	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
既存の共有を変更する	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

共有を作成または変更するときに、追加の共有設定オプションおよび共有プロパティを指定できます。の詳細については `vserver cifs share`、を"ONTAPコマンド リファレンス"参照してください。

ファイルロックを管理します。

プロトコル間の **ONTAP SMB** ファイルロックについて学ぶ

ファイルロックは、別のユーザが以前に開いていたファイルにユーザがアクセスできないようにするためにクライアントアプリケーションで使用される方法です。ONTAPでファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントがNFSクライアントの場合はロックを推奨します。クライアントがSMBクライアントの場合はロックは必須です。

NFSファイルとSMBファイルのロックの違いのため、SMBアプリケーションで以前に開いたファイルにNFSクライアントからアクセスすると失敗することがあります。

NFSクライアントがSMBアプリケーションでロックされているファイルにアクセスしようとすると、次の状況が発生します。

- mixed形式またはNTFS形式のボリュームでは、、 `rmdir`などのファイル操作を `rm`mv`行うと、NFSアプリケーションが失敗することがあります。
- NFSの読み取り処理と書き込み処理は、SMBの読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- ファイルの書き込み範囲が排他的なSMBバイトロックでロックされている場合、NFSの書き込み処理が失敗します。
- リンク解除
  - NTFSファイルシステムでは、SMBとCIFSの削除処理がサポートされています。

    ファイルは最後に閉じたあとで削除されます。
  - NFSのリンク解除処理は、サポートされていません。

    サポートされていない理由は、NTFSとSMBのセマンティクスが必要であり、NFSではLast Delete-On-Close処理がサポートされていないためです。
  - UNIXファイルシステムでは、リンク解除操作がサポートされています。

    サポートされている理由は、NFSとUNIXのセマンティクスが必要だからです。
- 名前変更
  - NTFSファイルシステムでは、デスティネーション ファイルがSMBかCIFSから開かれている場合には、デスティネーション ファイルの名前を変更できます。
  - NFSの名前変更はサポートされていません。

    サポートされていない理由は、NTFSとSMBのセマンティクスが必要だからです。

UNIXセキュリティ形式のボリュームでは、NFSのリンク解除および名前変更処理でSMBのロック状態が無視され、ファイルへのアクセスが許可されます。UNIXセキュリティ形式のボリューム上の他のすべてのNFS処理では、SMBロック状態が維持されます。

ONTAP SMBの読み取り専用ビットについて学ぶ

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。 NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、 Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、 ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、 NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。 ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファ

イルとして扱います。

- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、 ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、 ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、 NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときにSMBクライアントがその読み取り専用ビットを無効にすると、ONTAPはそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、 root のみです。

読み取り専用ビットは、ACL および Unix モード ビットと次のように相互作用します。

ファイルに読み取り専用ビットが設定されている場合:

- そのファイルの ACL は変更されません。NFSクライアントには、読み取り専用ビットが設定される前と同じ ACL が表示されます。
- ファイルへの書き込みアクセスを許可する Unix モード ビットはすべて無視されます。
- NFS クライアントと SMB クライアントはどちらもファイルを読み取ることはできますが、変更することはできません。
- ACLとUNIXモードビットは、読み取り専用ビットが優先されるため無視されます。つまり、ACLが書き込みアクセスを許可していても、読み取り専用ビットによって変更は禁止されます。

ファイルに読み取り専用ビットが設定されていない場合:

- ONTAP は、ACL と UNIX モード ビットに基づいてアクセスを決定します。
  - ACL または UNIX モード ビットのいずれかが書き込みアクセスを拒否した場合、NFS および SMB クライアントはファイルを変更できません。
  - ACL も UNIX モード ビットも書き込みアクセスを拒否しない場合は、NFS および SMB クライアントはファイルを変更できます。

ファイル権限の変更は、 SMB クライアントではすぐに反映されますが、 NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理における**ONTAP**と**Windows**の違い

Windowsとは異なり、ONTAPはファイルが開いている間、開いているファイルへのパスの各コンポーネントをロックしません。この動作はSMB共有パスにも影響します。

ONTAPではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。その結果、共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、セキュリティ設定を適用して、ユーザやアプリケ

ーションが重要なディレクトリの名前を変更できないようにします。

ONTAP SMBロックに関する情報を表示する

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

タスクの内容

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定の Storage Virtual Machine （ SVM ）のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

`vserver locks show`このコマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。 SMB を使用してクライアント側キャッシュを制御します。
- 委譲。 NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。の詳細については `vserver locks show`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. コマンドを使用して、ロックに関する情報を表示します `vserver locks show`。

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。共有ロックのアクセスモードは write-deny_none であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------ ----------- --------- -----------
-------
vol1    /vol1/file1              lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                        delegation  -
               Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します

/data2/data2_2/intro.pptx。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを write-deny_none として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
```

```
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ONTAP SMBロックを解除する

ファイルロックによってクライアントがファイルにアクセスできない場合は、現在有効なロックに関する情報を表示して、特定のロックを解除できます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

タスクの内容

コマンドは `vserver locks break`、advanced権限レベル以上でのみ使用できます。の詳細については `vserver locks break`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. ロックを解除するために必要な情報を確認するには、コマンドを使用し `vserver locks show`ます。

   の詳細については `vserver locks show`、を"ONTAPコマンド リファレンス"参照してください。

2. 権限レベルをadvancedに設定します。 `set -privilege advanced`
3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM名、ボリューム名、LIF名、およびファイルパス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロックID	`vserver locks break -lockid UUID`

4. admin権限レベルに戻ります。 `set -privilege admin`

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

SMBアクティビティの監視

SMB接続、SMB Session ID、セッションを使用しているワークステーションのIPアドレスなど、確立されているSMBセッションに関する情報を表示できます。セッションのSMBプロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうかを確認するのに役立ちます。

タスクの内容

SVM上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのパラメータを使用すると、選択したフィールドに関する出力を表示できます `-fields`。

  と入力して、使用できるフィールドを指定できます `-fields ?`。

- パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます `-instance`。
- パラメータまたは `-instance`パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます `-fields`。

ステップ

1. 次のいずれかを実行します。

表示する **SMB** セッション情報	入力するコマンド
SVM上のすべてのセッション（要約形式）	`vserver cifs session show -vserver vserver_name`
指定した接続IDのファイル	`vserver cifs session show -vserver vserver_name -connection-id integer`
指定したワークステーションのIPアドレスから	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定したLIF IPアドレスのファイル	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
指定したノードのオブジェクト	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	指定したWindowsユーザからのセッション
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	指定した認証メカニズムを使用している場合

表示する **SMB** セッション情報	入力するコマンド
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
指定したプロトコルバージョンを使用している場合	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 継続的可用性を備えた保護とSMBマルチチャネルは、SMB 3.0以降のセッションでのみ使用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を以降に設定します。 `SMB3` ====
指定したレベルの継続的可用性を備えた保護を使用しているセッション	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== 継続的可用性のステータスがの場合は `Partial`、継続的可用性を備えた開いているファイルがセッションに少なくとも1つ含まれていますが、継続的可用性を備えた保護を使用して開かれていないファイルがセッションに含まれています。コマンドを使用すると、確立されたセッションのファイルのうち、継続的可用性を備えた保護を使用して開かれていないファイルを確認できます `vserver cifs sessions file show`。 ====
指定したSMB署名セッションステータスのセッション	`vserver cifs session show -vserver vserver_name -is-session-signed {true

例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。接続はドメインアカウントを使用して行われました。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

次のコマンドを実行すると、SVM vs1上のSMB 3.0とSMBマルチチャネルを使用しているセッションに関するセッション情報が表示されます。この例では、ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するには、Kerberos認証を使用して接続を確立する必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

関連情報

開いているSMBファイルに関する情報の表示

開いている **ONTAP SMB** ファイルに関する情報を表示します

SMB接続とSession ID、ホスティングボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうかを確認するのに役立ちます。

タスクの内容

確立されたSMBセッションで開いているファイルに関する情報を表示できます。表示される情報は、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと継続的可用性を備えた保護を使用して開かれていないファイルがある場合（コマンド出力のフィールド `vserver cifs session show`の値 `-continuously-available`は `Partial`）、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

オプションのパラメータを何も指定せずにコマンドを実行することで、Storage Virtual Machine（SVM）上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show`。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションのパラメータを使用すると、選択したフィールドの出力を表示できます `-fields`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

- パラメータを使用すると、開いているSMBファイルに関する詳細情報を表示できます `-instance`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

ステップ

1. 次のいずれかを実行します。

表示する開いている **SMB** ファイル	入力するコマンド
SVM上のファイル（要約形式）	`vserver cifs session file show -vserver vserver_name`
指定したノードのオブジェクト	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	指定したファイルIDのファイル
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定したSMB接続IDのファイル
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定したSMB Session IDのファイル
`vserver cifs session file show -vserver vserver_name -session-id integer`	指定したホストアグリゲートのファイル
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	指定したボリュームのファイル
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定したSMB共有のファイル

表示する開いている **SMB** ファイル	入力するコマンド
`vserver cifs session file show -vserver vserver_name -share share_name`	指定したSMBパスのファイル
`vserver cifs session file show -vserver vserver_name -path path`	指定したレベルの継続的可用性を備えた保護を使用している
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 継続的可用性のステータスがの場合は `No`、開いているファイルがテイクオーバーやギブバックからの無停止でのリカバリに対応していません。また、ハイアベイラビリティ関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。 ====
指定した再接続状態のファイル	`vserver cifs session file show -vserver vserver_name -reconnected {No

出力結果の絞り込みに使用できるオプションのパラメータがほかにもあります。の詳細については `vserver cifs session file show`、を"ONTAPコマンド リファレンス"参照してください。

例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

関連情報

セッション情報を表示する

ONTAP SMBサーバで利用可能な統計、オブジェクト、カウンタを特定する

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	`statistics catalog object show`
使用可能な特定のオブジェクト	`statistics catalog object show -object object_name`
使用可能なカウンタ	`statistics catalog counter show -object object_name`

使用可能なオブジェクトやカウンタなど、の詳細については `statistics catalog object show`、を参照し"ONTAPコマンド リファレンス"てください。

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次のコマンドを実行すると、advanced権限レベルで表示した場合の、クラスタ内のCIFSアクセスとSMBアクセスに関連する選択した統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

次のコマンドを実行すると、advanced権限レベルで表示したオブジェクトの一部のカウンタに関する情報が

表示され `cifs`ます。

この例で表示されているのはオブジェクトの使用可能なカウンタの一部ではありませ `cifs`ん。出力は省略されています。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

関連情報

- 統計情報を表示

- "統計カタログカウンタ表示オブジェクト"
- "statistics start"

ONTAP SMB統計を表示する

パフォーマンスの監視と問題の診断を行うために、CIFSとSMB、監査、BranchCacheハッシュに関する統計など、さまざまな統計を表示できます。

開始する前に

オブジェクトに関する情報を表示する前に、コマンドと `statistics stop`コマンドを使用してデータサンプルを収集しておく必要があり `statistics start`ます。

詳細はこちら `statistics start`そして `statistics stop`の中で"ONTAPコマンド リファレンス" 。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

統計を表示する対象	入力するコマンド
SMBのすべてのバージョン	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.xおよびSMB 3.0	`statistics show -object smb2`
ノードのCIFSサブシステム	`statistics show -object nblade_cifs`
マルチプロトコルの監査	`statistics show -object audit_ng`
BranchCacheハッシュサービス	`statistics show -object hashd`
動的DNS	`statistics show -object ddns_update`

   の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

3. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

- サーバー上で利用可能な統計、オブジェクト、カウンターを決定する
- SMB署名済みセッションの統計の監視
- BranchCache統計を表示する
- 統計を使用して自動ノード参照アクティビティを監視する
- "Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"

- "パフォーマンス監視のセットアップ"

SMBクライアントベースのサービスを導入する

オフラインファイルを使用してオフラインで使用するファイルをキャッシュできるようにする

オフラインファイルを使用して、オフラインで使用するために **ONTAP SMB** ファイルをキャッシュできるようにする方法について説明します。

ONTAP では、 Microsoft のオフラインファイル機能（ _ クライアント側キャッシュ _ ）をサポートしています。これにより、オフラインで使用するファイルをローカルホストにキャッシュできます。オフラインファイル機能を使用すると、ネットワークから切断されていてもファイルの処理を継続できます。

Windowsのユーザドキュメントやプログラムを共有に自動的にキャッシュするかどうか、またはキャッシュするファイルを手動で選択する必要があるかどうかを指定できます。新しい共有では手動キャッシュがデフォルトで有効になります。オフラインで使用可能になったファイルは、Windowsクライアントのローカルディスクと同期されます。同期は、特定のストレージシステム共有へのネットワーク接続がリストアされたときに実行されます。

オフラインのファイルやフォルダへのアクセス権は、CIFSサーバに保存されているファイルやフォルダと同じになるため、オフラインのファイルやフォルダに対して操作を実行するには、CIFSサーバに保存されているファイルやフォルダに対する十分な権限がユーザに必要です。

ユーザーとネットワーク上の他のユーザーが同じファイルに変更を加えた場合、ユーザーはファイルのローカルバージョンをネットワークに保存するか、他のバージョンを保持するか、またはその両方を保存できます。ユーザが両方のバージョンを保持している場合、ローカルユーザの変更を含む新しいファイルがローカルに保存され、キャッシュされたファイルはCIFSサーバに保存されているバージョンの変更で上書きされます。

共有ごとにオフラインファイルを設定するには、共有設定を使用します。共有を作成または変更するときに、次の4つのオフラインフォルダ設定のいずれかを選択できます。

- キャッシュなし

  共有のクライアント側キャッシュを無効にします。クライアントのローカルにファイルやフォルダが自動的にキャッシュされず、ユーザがファイルやフォルダをローカルにキャッシュすることもできません。

- 手動キャッシュ

  共有にキャッシュするファイルを手動で選択できるようにします。これがデフォルト設定です。デフォルトでは、ファイルやフォルダはローカルクライアントにキャッシュされません。オフラインで使用するためにローカルにキャッシュするファイルやフォルダをユーザが選択できます。

- ドキュメントの自動キャッシュ

  ユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイルとフォルダだけです。

- プログラムの自動キャッシュ

  プログラムとユーザのドキュメントを共有に自動的にキャッシュできるようにします。ローカルにキャッシュされるのは、アクセスしたファイル、フォルダ、およびプログラムだけです。さらに、この設定によ

り、クライアントはネットワークに接続されている場合でも、ローカルにキャッシュされた実行可能ファイルを実行できます。

Windowsサーバおよびクライアントでのオフラインファイルの設定の詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

- 移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザプロファイルの一元的な格納
- フォルダーリダイレクトを使用してサーバーにデータを保存する方法について学習します
- BranchCache を使用してブランチ オフィスの共有コンテンツをキャッシュする方法について説明します。
- "Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

オフラインの **ONTAP SMB** ファイルを使用するための要件について学習します

CIFS サーバで Microsoft のオフラインファイル機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAP の各リリースでオフラインファイルがサポートされます。

SMBプロトコルのバージョン

Storage Virtual Machine （ SVM ONTAP ）については、すべてのバージョンの SMB でオフラインファイルがサポートされます。

Windowsクライアントの要件

Windows クライアントでオフラインファイルがサポートされている必要があります。

オフラインファイル機能をサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

"mysupport.netapp.com/matrix"

オフライン **ONTAP SMB** ファイルの導入に関するガイドライン

ホームディレクトリに共有プロパティが設定されているホームディレクトリ共有にオフラインファイルを導入する場合は、いくつかの重要なガイドラインについて理解しておく必要があり `showsnapshot`ます。

オフラインファイルが設定されているホームディレクトリ共有で共有プロパティが設定されている場合、`showsnapshot`Windowsクライアントはすべての`Snapshot`をユーザのホームディレクトリ内のフォルダの下にキャッシュします `~snapshot`。

次のいずれかに該当する場合、Windowsクライアントでは、すべてのSnapshotがホームディレクトリの下にキャッシュされます。

- ユーザが、ホームディレクトリをクライアントからオフラインで利用できるようにしている。

  ホームディレクトリ内のフォルダの内容 `~snapshot`も含まれ、オフラインで使用できるようになります。

- ユーザが、などのフォルダをCIFSサーバ共有にあるホームディレクトリのルートにリダイレクトするようにフォルダリダイレクトを設定している `My Documents`。

  Windows クライアントによっては、リダイレクトされたフォルダが自動的にオフラインで利用できるようになる場合があります。フォルダがホームディレクトリのルートにリダイレクトされる場合、その `~snapshot`フォルダはキャッシュされたオフラインコンテンツに含まれます。

> フォルダがオフラインファイルに含まれているオフラインファイルの展開 `~snapshot`は避ける必要があります。フォルダ内の`Snapshot` `~snapshot`には、`ONTAP`が`Snapshot`を作成した時点のボリューム上のすべてのデータが含まれています。そのため、フォルダのオフラインコピーを作成すると `~snapshot`、クライアントのローカルストレージが大量に消費され、オフラインファイルの同期中にネットワーク帯域幅が消費され、オフラインファイルの同期にかかる時間が長くなります。

オフライン**SMB**ファイルサポートを設定するための**ONTAP**コマンド

ONTAP CLIを使用してオフラインファイルのサポートを設定するには、SMB共有の作成時に、または既存のSMB共有の変更時にいつでも、4つのオフラインファイル設定のいずれかを指定します。デフォルトの設定は、オフラインファイルの手動サポートです。

タスクの内容

オフラインファイルのサポートを設定する場合は、次の4つのオフラインファイル設定のいずれかを選択できます。

設定	説明
`none`	Windowsクライアントがこの共有のファイルをキャッシュすることを禁止します。
`manual`	Windowsクライアントのユーザが、キャッシュするファイルを手動で選択できるようにします。
`documents`	Windowsクライアントがオフラインアクセスのために使用するユーザドキュメントをキャッシュすることを許可します。
`programs`	Windowsクライアントがオフラインアクセスのために使用するプログラムをキャッシュすることを許可します。クライアントは、共有が使用可能な場合でも、キャッシュされたプログラムファイルをオフラインモードで使用できます。

選択できるオフラインファイル設定は1つだけです。既存のSMB共有でオフラインファイル設定を変更すると、元の設定が新しいオフラインファイル設定に置き換えられます。その他の既存のSMB共有設定および共

有プロパティは削除も置き換えもされません。これらは、明示的に削除または変更されるまで有効です。

手順

1. 適切な操作を実行します。

オフラインファイルを設定する対象	入力するコマンド
新しいSMB共有	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	既存のSMB共有
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. SMB共有の設定が正しいことを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

例

次のコマンドは、オフラインファイルをに設定して「data1」という名前のSMB共有を作成します `documents`。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

次のコマンドは、オフラインファイルの設定をに変更し、ファイルモードおよびディレクトリモードの作成マスクの値を追加することで、「data1」という名前の既存のSMB共有を変更します。 `manual`

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

関連情報

既存の共有の共有プロパティを追加または削除する

コンピュータ管理**MMC**を使用して、**ONTAP SMB**共有のオフラインファイルサポートを構成する

オフラインで使用するためにファイルをローカルにキャッシュすることをユーザに許可する場合は、コンピュータの管理 MMC （ Microsoft 管理コンソール）を使用してオフラインファイルのサポートを設定できます。

手順

1. Windows サーバー上の MMC を開くには、 Windows エクスプローラで、ローカルコンピューターのアイコンを右クリックし、 * 管理 * を選択します。
2. 左側のパネルで、「 * コンピュータの管理 * 」を選択します。
3. 「 * アクション * > * 別のコンピューターに接続 * 」を選択します。

   [コンピュータの選択] ダイアログボックスが表示されます。

4. CIFS サーバの名前を入力するか、 * Browse * をクリックして CIFS サーバを指定します。

   CIFSサーバの名前がStorage Virtual Machine（SVM）ホスト名と同じ場合は、SVM名を入力しま

す。CIFS サーバの名前が SVM ホスト名と異なる場合は、 CIFS サーバの名前を入力します。

5. [OK]*をクリックします。
6. コンソールツリーで、 * システムツール * > * 共有フォルダー * をクリックします。
7. [* 共有] をクリックします。
8. 結果ペインで、共有を右クリックします。
9. * プロパティ * をクリックします。

   選択した共有のプロパティが表示されます。

10. [一般 *] タブで、 [* オフライン設定 *] をクリックします。

    [オフライン設定] ダイアログボックスが表示されます。

11. 必要に応じて、オフラインの可用性オプションを設定します。
12. [OK]*をクリックします。

移動プロファイルを使用して、**SVM**に関連付けられた**SMB**サーバにユーザプロファイルを一元的に格納する

移動プロファイルを使用して **ONTAP SMB** ユーザー プロファイルを一元的に保存する方法について説明します。

ONTAPでは、Windowsの移動プロファイルの格納をサポートしており、Storage Virtual Machine（SVM）に関連付けられたCIFSサーバに格納できます。ユーザ移動プロファイルを設定すると、ユーザはどこでログインしても自動でリソースを利用できるようになります。また、ユーザ プロファイルの管理が簡単になり、管理者にとってもメリットがあります。

移動ユーザプロファイルには、次の利点があります。

- 自動でリソースを利用できる

  ユーザーがWindows 8、Windows 7、Windows 2000、またはWindows XPを実行しているネットワーク上のコンピュータにログインすると、ユーザーの一意のプロファイルが自動的に使用可能になります。ユーザは、ネットワーク上で使用する各コンピュータでプロファイルを作成する必要はありません。

- コンピュータの交換が簡単

  ユーザのプロファイル情報はすべてネットワーク上で個別に管理されるため、ユーザのプロファイルは新しい交換用コンピュータに簡単にダウンロードできます。ユーザが新しいコンピュータに初めてログインしたときに、サーバに保存されているユーザのプロファイルが新しいコンピュータにコピーされます。

関連情報

- オフラインファイルを使用して、オフラインで使用するためにファイルをキャッシュできるようにする方法について学習します。
- フォルダーリダイレクトを使用してサーバーにデータを保存する方法について学習します

CIFSサーバでMicrosoftの移動プロファイルを使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAPでは、移動プロファイルがサポートされます。

SMBプロトコルのバージョン

Storage Virtual Machine（SVM）についてはONTAP、すべてのバージョンのSMBで移動プロファイルがサポートされます。

Windowsクライアントの要件

移動プロファイルを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。

移動プロファイルをサポートするWindowsクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ユーザがネットワーク上の任意のコンピュータにログオンしたときにそのユーザのプロファイルを自動的に使用可能にするには、[Active Directoryユーザーとコンピュータ]MMCスナップインで移動プロファイルを設定します。Windows Serverで移動プロファイルを設定する場合は、Active Directory管理センターを使用します。

手順

1. Windowsサーバーで、Active DirectoryユーザーとコンピュータMMC（またはWindowsサーバーのActive Directory管理センター）を開きます。
2. 移動プロファイルを設定するユーザを見つけます。
3. ユーザーを右クリックし、 * プロパティ * をクリックします。
4. [プロファイル]*タブで、ユーザの移動プロファイルを保存する共有のプロファイルパスを入力し、続けてを入力します `%username%`。

   たとえば、プロファイルパスは次のようになります `\\vs1.example.com\profiles\%username%`。ユーザが初めてログインすると、 `%username%`はそのユーザの名前に置き換えられます。

   > パスの `\\vs1.example.com\profiles\%username%` `profiles`は、すべてのメンバーにフルコントロール権限が割り当てられているStorage Virtual Machine（SVM）vs1上の共有の共有名です。

5. [OK]*をクリックします。

フォルダリダイレクトを使用して**SMB**サーバにデータを格納する

フォルダリダイレクトを使用して **ONTAP SMB** サーバーにデータを保存する方法について説明します。

ONTAPでは、Microsoftのフォルダリダイレクトがサポートされています。ユーザや管理者は、この機能を使用して、ローカルフォルダのパスをCIFSサーバ上の場所にリダイレクトできます。リダイレクトされたフォルダは、データがSMB共有に格納されていても、ローカルのWindowsクライアントに格納されているように見えます。

フォルダリダイレクトは、主に、ホームディレクトリをすでに導入していて、既存のホームディレクトリ環境との互換性を維持したい組織を対象としています。

- `Documents`、 `Desktop`、および `Start Menu`は、リダイレクト可能なフォルダの例です。
- ユーザはWindowsクライアントからフォルダをリダイレクトできます。
- 管理者は、Active DirectoryでGPOを設定することで、フォルダリダイレクトを一元的に設定および管理できます。
- 管理者が移動プロファイルを設定している場合、フォルダリダイレクトを使用すると、管理者はユーザデータをプロファイルデータから分割できます。
- フォルダリダイレクトとオフラインファイルを使用して、ユーザがコンテンツをローカルにキャッシュしながら、ローカルフォルダのデータストレージをCIFSサーバにリダイレクトできます。

関連情報

- オフラインファイルを使用して、オフラインで使用するためにファイルをキャッシュできるようにする方法について学習します。
- 移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザプロファイルの一元的な格納

ONTAP SMBフォルダリダイレクトの使用要件について学習します

CIFS サーバで Microsoft のフォルダリダイレクトを使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAP は、 Microsoft のフォルダリダイレクトをサポートしています

SMBプロトコルのバージョン

Storage Virtual Machine （ SVM ）については、 ONTAP のすべてのバージョンの SMB で Microsoft のフォルダリダイレクトがサポートされます。

Windowsクライアントの要件

Microsoft のフォルダリダイレクトを使用するには、 Windows クライアントでこの機能がサポートされている必要があります。

フォルダリダイレクトをサポートする Windows クライアントに関する最新情報については、 Interoperability Matrix を参照してください。

"mysupport.netapp.com/matrix"

Windowsのプロパティを使用して**ONTAP SMB**フォルダのリダイレクトを構成する

Windowsの[プロパティ]ウィンドウを使用して、フォルダリダイレクトを設定できます。この方法を使用する利点は、WindowsユーザがSVM管理者の支援なしでフォルダリダイレクトを設定できることです。

手順

1. エクスプローラで、ネットワーク共有にリダイレクトするフォルダを右クリックします。
2. * プロパティ * をクリックします。

   選択した共有のプロパティが表示されます。

3. [* ショートカット *] タブで、 [* ターゲット *] をクリックし、選択したフォルダーをリダイレクトするネットワーク上の場所へのパスを指定します。

   たとえば、にマッピングされているホームディレクトリ内のフォルダ `Q:\`にフォルダをリダイレクトする場合 `data`は、をターゲットとして指定します `Q:\data`。

4. [OK]*をクリックします。

   オフラインフォルダの設定の詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

SMB 2.xを使用して**Windows**クライアントから**ONTAP ~snapshot**ディレクトリにアクセスする方法について学習します。

SMB 2.xを使用するWindowsクライアントからのディレクトリへのアクセスに使用する方法 `~snapshot`は、SMB 1.0の場合とは異なります。SMB 2.x接続を使用してSnapshotに格納されたデータに正常にアクセスするために、ディレクトリにアクセスする方法について理解しておく必要があり `~snapshot`ます。

SVM管理者は、vserver cifs share propertiesファミリーのコマンドを使用して共有プロパティを有効または無効にすることで、Windowsクライアントのユーザが共有のディレクトリを表示してアクセスできるかどうかを制御します `~snapshot`。 `showsnapshot`

共有プロパティが無効になっている場合、 `showsnapshot`SMB 2.xを使用するWindowsクライアントのユーザは、ディレクトリへのパスまたはディレクトリ内の特定のSnapshotへのパスを手動で入力しても、ディレクトリを表示できず、ディレクトリ `~snapshot`内のSnapshotにアクセスできませ `~snapshot`ん `~snapshot`。

共有プロパティが有効になっている場合 `showsnapshot`でも、SMB 2.xを使用するWindowsクライアントのユーザは、共有のルートにあるディレクトリ、または共有のルートより下のジャンクションまたはディレクトリ内のディレクトリを表示できません `~snapshot`。ただし、共有に接続したユーザは、共有パスの末尾にを手動で追加することで、非表示のディレクトリに `\~snapshot`アクセスできます `~snapshot`。非表示の `~snapshot`ディレクトリには、次の2つのエントリポイントからアクセスできます。

- 共有のルート
- 共有スペースのすべてのジャンクションポイント

非表示の `~snapshot`ディレクトリには、共有内のジャンクション以外のサブディレクトリからはアクセスできません。

例

次の例に示す設定では、「eng'」共有へのSMB 2.x接続を使用するWindowsクライアントのユーザが、共有パス（共有のルートおよびパス内のすべてのジャンクションポイント）に手動でを追加することで、ディレクトリにアクセスできます `~snapshot`。 `\~snapshot`非表示の `~snapshot`ディレクトリには、次の3つのパスからアクセスできます。

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

以前のバージョン機能を使用したファイルとフォルダのリカバリ

以前のバージョンを使用して **ONTAP SMB** ファイルとフォルダをリカバリする方法について説明します。

Microsoftの以前のバージョンを使用する機能は'何らかの形でスナップショットをサポートし'スナップショットが有効になっているファイル・システムに適用されますSnapshot テクノロジは ONTAP に不可欠なテクノロジの 1 つです。ユーザーは、Microsoftの以前のバージョン機能を使用して、Windowsクライアントからスナップショットからファイルやフォルダをリカバリできます。

以前のバージョン機能を使用すると、ストレージ管理者の介入なしに、ユーザがスナップショットを参照したり、スナップショットからデータをリストアしたりすることができます。以前のバージョン機能は設定できません。常に有効になります。ストレージ管理者が共有でSnapshotを使用できるようにしている場合、ユーザは[以前のバージョン]機能を使用して次のタスクを実行できます。

- 誤って削除したファイルをリカバリする。
- 誤って上書きしたファイルをリカバリする。
- 作業中にファイルのバージョンを比較します。

Snapshotに格納されるデータは読み取り専用です。ファイルに変更を加えるには、ファイルのコピーを別の場所に保存する必要があります。スナップショットは定期的に削除されるため、ユーザーが以前のバージョンのファイルを無期限に保持するには、以前のバージョンに含まれていたファイルのコピーを作成する必要があります。

Microsoft の以前のバージョンを使用するための ONTAP SMB の要件

CIFSサーバで[以前のバージョン]機能を使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。また、Snapshot設定の要件についても理解しておく必要があります。

ONTAPのバージョンの要件

以前のバージョンをサポートします。

SMBプロトコルのバージョン

Storage Virtual Machine（SVM）についてはONTAP、すべてのバージョンのSMBで[以前のバージョン]機能がサポートされます。

Windowsクライアントの要件

[以前のバージョン]機能を使用してスナップショットのデータにアクセスするには、Windowsクライアントでこの機能がサポートされている必要があります。

[以前のバージョン]機能をサポートするWindowsクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

スナップショット設定の要件

[以前のバージョン]機能を使用してSnapshotのデータにアクセスするには、有効なSnapshotポリシーがデータを含むボリュームに関連付けられ、クライアントがSnapshotデータにアクセスできること、およびSnapshotが存在していることが必要です。

Windows の以前のバージョンタブを使用して ONTAP SMB スナップショット データを表示および管理します

Windowsクライアントマシンでは、Windowsの[プロパティ]ウィンドウの[以前のバージョン]タブを使用して、Storage Virtual Machine（SVM）管理者の手を借りなくても、Snapshotに格納されたデータをユーザがリストアできます。

タスクの内容

SVMに格納されたデータのSnapshotのデータを[以前のバージョン]タブで表示および管理できるのは、管理者が共有を含むボリュームでSnapshotを有効にし、Snapshotを表示するように共有を設定している場合のみです。

手順

1. エクスプローラで、CIFSサーバに格納されているデータのマッピングされたドライブの内容を表示します。
2. スナップショットを表示または管理するマッピングされたネットワークドライブ内のファイルまたはフォルダを右クリックします。
3. * プロパティ * をクリックします。

   選択したファイルまたはフォルダのプロパティが表示されます。

4. [以前のバージョン *] タブをクリックします。

   選択したファイルまたはフォルダの使用可能なスナップショットのリストが[フォルダバージョン：（Folder Versions：）]ボックスに表示されます。表示されたSnapshotは、Snapshot名のプレフィックスと作成時のタイムスタンプで識別されます。

5. [* フォルダーバージョン： *] ボックスで、管理するファイルまたはフォルダーのコピーを右クリックします。
6. 適切な操作を実行します。

状況	操作
スナップショットのデータを表示する	• 開く * をクリックします。
そのSnapshotからデータのコピーを作成する	[* コピー（ Copy ）] をクリックします

   Snapshotのデータは読み取り専用です。[以前のバージョン]タブに表示されているファイルやフォルダに変更を加える場合は、変更するファイルやフォルダのコピーを書き込み可能な場所に保存し、コピーに変更を加える必要があります。

7. スナップショットデータの管理が終了したら、* OK *をクリックして*プロパティ*ダイアログボックスを閉じます。

   [以前のバージョン]タブを使用したSnapshotデータの表示と管理の詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

ONTAP SMBスナップショットが以前のバージョンで使用可能かどうかを確認します

[以前のバージョン]タブからSnapshotを表示できるのは、有効なSnapshotポリシーが共有を含むボリュームに適用され、ボリューム構成でSnapshotへのアクセスが許可されている場合のみです。Snapshotの可用性を確認すると、[以前のバージョン]機能へのアクセスをユーザに提供する際に役立ちます。

手順

1. 共有データが存在するボリュームで自動Snapshotが有効になっているかどうか、およびクライアントがSnapshotディレクトリにアクセスできるかどうかを確認します。 `volume show -vserver`

```
vserver-name -volume volume-name -fields vserver,volume,snapdir-
access,snapshot-policy,snapshot-count
```

出力には、ボリュームに関連付けられているSnapshotポリシー、クライアントSnapshotディレクトリアクセスが有効かどうか、および使用可能なSnapshotの数が表示されます。

2. 関連付けられているSnapshotポリシーが有効になっているかどうかを確認します。 `volume snapshot policy show -policy policy-name`
3. 使用可能なSnapshotを表示します。 `volume snapshot show -volume volume_name`

SnapshotポリシーとSnapshotスケジュールの設定と管理の詳細については、を参照してください"データ保護"。

例

次の例は、「data1」上の共有データと使用可能なSnapshotを含む「data1」という名前のボリュームに関連付けられているSnapshotポリシーに関する情報を表示します。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                     3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

関連情報

- 以前のバージョンへのアクセスを有効にするためにスナップショット構成を作成する
- "データ保護"

以前のバージョンへのアクセスを有効にするために **ONTAP SMB** スナップショット構成を作成する

スナップショットへのクライアントアクセスが有効で、スナップショットが存在する場合は、以前のバージョン機能を常に使用できます。スナップショット構成がこれらの要件を満たしていない場合は、その要件を満たすスナップショット構成を作成できます。

手順

1. 以前のバージョン機能からのアクセスを許可する共有が含まれているボリュームにSnapshotポリシーが関連付けられていない場合は、コマンドを使用してSnapshotポリシーをボリュームに関連付け、有効にします `volume modify`。

   の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用してオプションをに `true`設定し `-snap-dir`、Snapshotへのアクセスを有効にします `volume modify`。

   の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドと `volume snapshot policy show`コマンドを使用して、Snapshotポリシーが有効になっていること、およびSnapshotディレクトリへのアクセスが有効になっていることを確認します `volume show`。

   および `volume snapshot policy show`の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

   SnapshotポリシーとSnapshotスケジュールの設定と管理の詳細については、を参照してください"データ保護"。

関連情報

"データ保護"

ONTAP SMBジャンクションを含む以前のバージョンのディレクトリを復元する方法について説明します。

以前のバージョン機能を使用してジャンクションポイントを含むフォルダをリストアする場合は、一定のガイドラインに注意する必要があります。

以前のバージョンを使用して、ジャンクションポイントである子フォルダを含むフォルダをリストアすると、リストアがエラーで失敗することがあります `Access Denied`。

リストアしようとしているフォルダにジャンクションが含まれているかどうかを確認するには、 `vol show`コマンドでオプションを指定し `-parent`ます。コマンドを使用して、ファイルやフォルダのアクセスに関する問題に関する詳細なログを作成することもできます `vserver security trace`。

関連情報

NASネームスペースでのデータボリュームの作成と管理

SMBサーバベースのサービスの導入

ホームディレクトリを管理します。

ONTAP SMBサーバーで動的ホームディレクトリを有効にする方法について学習します

ONTAP ホームディレクトリを使用すると、 SMB 共有を設定し、ユーザと一連の変数に基づいてさまざまなディレクトリにマッピングすることができます。ユーザごとに別個の共有を作成するのではなく、 1 つの共有を設定し、いくつかのホームディレクトリパ

ラメータを指定して、エントリポイント（共有）とホームディレクトリ（ SVM 上のディレクトリ）間の関係をユーザ単位で定義します。

ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。ユーザとディレクトリのマッピング方法を決定する 4 つの変数があります。

- * 共有名 *

  ユーザの接続先として作成する共有の名前です。この共有にはホームディレクトリのプロパティを設定する必要があります。

  共有名には、次の動的な名前を使用できます。

  - `%w`（ユーザのWindowsユーザ名）
  - `%d`（ユーザのWindowsドメイン名）
  - `%u`（ユーザのマッピングされたUNIXユーザ名）すべてのホームディレクトリ間で共有名を一意にするには、共有名にまたは `%u`変数を使用する必要があります/%w`。共有名には変数と/`%w`変数の両方を使用することも（など `%d/%w`）、静的な部分と変数の部分を使用することも（home_など/`%w`）できます `%d`。

- * 共有パス *

  共有によって定義される、つまり、共有名の 1 つに関連付けられる相対パスです。各検索パスに付加されて、 SVM のルートからのユーザのホームディレクトリの完全パスを生成します。静的（例：）、動的（例：）、または2つの組み合わせ（例： `%w`）を `eng/%w`指定できます `home`。

- * 検索パス *

  SVM のルートからの絶対パスのセットで、 ONTAP ではこのパスに基づいてホームディレクトリが検索されます。コマンドを使用すると、1つ以上の検索パスを指定できます `vserver cifs home-directory search-path add`。複数の検索パスを指定すると、ONTAPは有効なパスが見つかるまで、指定された順序で検索パスを試行します。の詳細については `vserver cifs home-directory search-path add`、を"ONTAPコマンド リファレンス"参照してください。

- * ディレクトリ *

  ユーザに対して作成する、そのユーザのホームディレクトリです。通常、ディレクトリ名はユーザの名前です。ホームディレクトリは、検索パスで定義されるいずれかのディレクトリに作成する必要があります。

たとえば、次のように設定します。

- ユーザ： John Smith
- ユーザのドメイン： acme
- ユーザ名： jsmith
- SVM 名： vs1
- ホームディレクトリ共有名#1：home_ `%w`-共有パス： `%w`

- ホームディレクトリ共有名#2： `%w-共有パス： %d/%w`
- 検索パス#1： `/vol0home/home`
- 検索パス#2： `/vol1home/home`
- 検索パス#3： `/vol2home/home`
- ホームディレクトリ： `/vol1home/home/jsmith`

シナリオ1：ユーザーがに接続し `\\vs1\home_jsmith`ます。これは最初のホームディレクトリ共有名に一致し、相対パスが生成され `jsmith`ます。ONTAPでは、各検索パスが順にチェックされ、という名前のディレクトリが検索されるようになりまし `jsmith`た。

- `/vol0home/home/jsmith`は存在しません。検索パス#2に進みます。
- `/vol1home/home/jsmith`は存在します。したがって、検索パス#3はチェックされません。これで、ユーザは自分のホームディレクトリに接続されました。

シナリオ2：ユーザーがに接続します `\\vs1\jsmith`。これは2番目のホームディレクトリ共有名に一致し、相対パスが生成され `acme/jsmith`ます。ONTAPでは、各検索パスが順にチェックされ、という名前のディレクトリが検索されるようになりまし `acme/jsmith`た。

- `/vol0home/home/acme/jsmith`は存在しません。検索パス#2に進みます。
- `/vol1home/home/acme/jsmith`は存在しません。検索パス#3に進みます。
- `/vol2home/home/acme/jsmith`は存在しません。ホームディレクトリが存在しないため、接続は失敗します。

ホームディレクトリ共有

ONTAP SMBホームディレクトリ共有を追加する

SMBホームディレクトリ機能を使用する場合は、ホームディレクトリプロパティが設定された共有を少なくとも1つ追加する必要があります。

タスクの内容

ホームディレクトリ共有は、共有の作成時にコマンドを使用して作成できます `vserver cifs share create`。既存の共有をホームディレクトリ共有に変更するには、コマンドを使用します `vserver cifs share modify`。

ホームディレクトリ共有を作成するには、共有を作成または変更するときにオプションに値 `-share -properties`を指定する必要があります `homedirectory`。共有名と共有パスは変数を使用して指定できます。変数はユーザがホームディレクトリに接続するときに動的に拡張されます。パスに使用できる変数は、 `%w`、 `%d`、および `%u`です。それぞれ、Windowsユーザ名、ドメイン、およびマッピングされたUNIXユーザ名に対応します。

手順

1. ホームディレクトリ共有を追加します。+
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver` `vserver`検索パスを追加するCIFS対応のStorage Virtual Machine（SVM）を指定します。

`-share-name *share-name*`ホームディレクトリ共有名を指定します。

必要な変数の1つに加えて、リテラル文字列 `%u`、、またはの `%d`いずれかが共有名に含まれている場合は `%w`、リテラル文字列の前に%（パーセント）文字を付けて、ONTAPがリテラル文字列を変数として処理しないようにする必要があります（例： `%%w`）。

- 共有名には変数またはの `%u`いずれかを使用する必要があります `%w`。
- 共有名には、さらに変数（など `%d`/`%w`）を含めることも、静的な部分（例：home1_/`%w`）を含めることもできます `%d`。
- 管理者が、他のユーザのホームディレクトリに接続するために、またはユーザが他のユーザのホームディレクトリに接続するのを許可するために共有を使用する場合は、動的な共有名のパターンの先頭にチルダ（ ~ ）を付ける必要があります。

> `vserver cifs home-directory modify`このアクセスを有効にするには、オプションを `true`に設定する `-is-home-dirs-access-for-admin-enabled`か、アドバンストオプションをに `true`設定します `-is-home-dirs-access-for-public-enabled`。

`-path` `path`ホームディレクトリの相対パスを指定します。

`-share-properties homedirectory[,…]`その共有の共有プロパティを指定します。値を指定する必要があり `homedirectory`ます。追加の共有プロパティをカンマで区切って指定できます。

1. コマンドを使用して、ホームディレクトリ共有が追加されたことを確認します `vserver cifs share show`。

例

次のコマンドは、という名前のホームディレクトリ共有を作成し `%w`ます。 `oplocks` `browsable`、、および `changenotify`共有プロパティは、共有プロパティに加えて設定され `homedirectory`ます。

> この例で表示されているのは、SVM上のすべての共有の出力ではありません。出力は省略されています。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

関連情報

- ホームディレクトリの検索パスを追加する
- サーバー上で自動ノード紹介を使用するための要件とガイドライン
- ユーザーのホームディレクトリへのアクセスを管理する

ホームディレクトリ共有の固有の **ONTAP SMB** ユーザー名要件について学習します。

（Windowsユーザ名）変数または（UNIXユーザ名） `%u`変数を使用してホームディレクトリ共有を動的に生成する場合は、一意のユーザ名を割り当てるように注意してください `%w`。共有名はユーザ名にマッピングされます。

静的共有の名前とユーザの名前が同じ場合、次の 2 つの問題が発生する可能性があります。

- ユーザがコマンドを使用してクラスタ上の共有の一覧を表示する `net view`と、同じユーザ名の2つの共有が表示されます。
- ユーザがその共有名に接続すると、常に静的共有に接続され、同じ名前のホームディレクトリ共有にはアクセスできません。

たとえば、「 administrator 」という名前の共有があり、「 administrator 」という名前の Windows ユーザ名が割り当てられているとします。ホーム・ディレクトリ共有を作成し、その共有に接続すると、「管理者」のホーム・ディレクトリ共有ではなく、「管理者」の静的共有に接続されます。

共有名が重複している問題を解決するには、次のいずれかの手順を実行します。

- 静的共有の名前を変更し、ユーザのホームディレクトリ共有と競合しないようにします。
- ユーザに新しいユーザ名を割り当てて、静的共有名と競合しないようにします。
- パラメータを使用する代わりに、「home」などの静的な名前を使用してCIFSホームディレクトリ共有を作成し、`%w`共有名との競合を回避します。

アップグレード後に静的 **ONTAP SMB** ホームディレクトリ共有名がどうなるかについて説明します。

ホームディレクトリ共有名には、または `%u`動的変数のいずれかが含まれている必要があります `%w`。新しい要件がある ONTAP のバージョンにアップグレードしたあとに、既存の静的ホームディレクトリ共有名が受ける影響について理解しておく必要があります。

ホームディレクトリの設定に静的共有名が含まれている場合に ONTAP にアップグレードしても、静的ホームディレクトリ共有名は変更されず、共有も有効なままです。ただし、変数または `%u`を含まない新しいホームディレクトリ共有は作成できません `%w`。

ユーザのホームディレクトリ共有名にどちらかの変数を含めるという必須条件によって、すべての共有名がホームディレクトリ設定全体で一意であることが保証されます。必要に応じて、静的ホームディレクトリ共有名を変数または `%u`を含む名前に変更できます `%w`。

ONTAP SMBホームディレクトリの検索パスを追加する

ONTAP SMBホームディレクトリを使用する場合は、ホームディレクトリ検索パスを少なくとも1つ追加する必要があります。

タスクの内容

ホームディレクトリ検索パスを追加するには、コマンドを使用し `vserver cifs home-directory search-path add`ます。

コマンドは `vserver cifs home-directory search-path add`、コマンドの実行中にオプションで指定されたパスをチェックし `-path`ます。指定したパスが存在しない場合は、続行するかどうかを確認するメッセージが表示されます。または `n`を選択し `y`ます。続行する場合は `y`、ONTAPによって検索パスが作成されます。ただし、ホームディレクトリ設定で検索パスを使用するには、事前にディレクトリ構造を作成しておく必要があります。続行しない場合、コマンドは失敗し、検索パスは作成されません。その後、パスディレクトリ構造を作成してコマンドを再実行できます `vserver cifs home-directory search-path add`。

手順

1. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`
2. コマンドを使用して、検索パスが追加されたことを確認します `vserver cifs home-directory search-path show`。

例

次の例は、SVM vs1のホームディレクトリ設定にパスを追加します `/home1`。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

次の例は、SVM vs1のホームディレクトリ設定にパスを追加することを試みます `/home2`。パスが存在しません。続行しないことが選択されます。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

関連情報

ホームディレクトリの共有を追加する

%w および **%d** 変数を使用して **ONTAP SMB** ホーム ディレクトリ構成を作成します。

変数と `%d`変数を使用して、ホームディレクトリ設定を作成できます `%w`。ユーザは、動的に作成された共有を使用してホーム共有に接続できます。

手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 目的のセキュリティ形式がqtreeで使用されていない場合は、コマンドを使用してセキュリティ形式を変更し `volume qtree security`ます。
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver` `vserver`検索パスを追加するCIFS対応のStorage Virtual Machine（SVM）を指定します。

   `-share-name` `%w`ホームディレクトリ共有名を指定します。ONTAPでは、ユーザがホームディレクトリに接続するたびに、共有名が動的に作成されます。共有名の形式は _windows_user_name です。

   `-path` `%d/%w`ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _domain/windows_user_name の形式で相対パスが動的に作成されます。

   `-share-properties homedirectory[,…]+`その共有の共有プロパティを指定します。値を指定する必要があり `homedirectory`ます。追加の共有プロパティをカンマで区切って指定できます。

5. コマンドを使用して、共有が目的の設定になっていることを確認します `vserver cifs share show`。
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *vserver-name*`検索パスを追加するCIFS対応のSVMを指定します。

   `-path` *path*`検索パスの絶対ディレクトリパスを指定します。

7. コマンドを使用して、検索パスが追加されたことを確認します `vserver cifs home-directory search-path show`。
8. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定したqtreeまたはボリューム内に、対応するディレクトリを作成します。

   たとえば、というパスのqtreeを作成し、ディレクトリを作成するユーザ名がmydomain\user1である場合は `/vol/vol1/users`、というパスでディレクトリを作成します `/vol/vol1/users/mydomain/user1`。

   にマウントされる「home1」という名前のボリュームを作成した場合は、というパスでディレクトリを作成し `/home1`ます `/home1/mydomain/user1`。

9. ドライブをマッピングするか、UNCパスを使用して接続し、ユーザがホーム共有に正常に接続できることを確認します。

   たとえば、ユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順8で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1`。

例

次の例のコマンドは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は%wです。
- 相対ホームディレクトリパスは%d/%wです。
- ホームディレクトリを含むように指定した検索パス `/home1`は、NTFSセキュリティ形式が設定されたボリュームです。
- 設定はSVM vs1に作成されます。

ユーザがWindowsホストからホームディレクトリにアクセスする場合は、このようなホームディレクトリ設定を使用できます。また、ユーザがWindowsホストおよびUNIXホストからホームディレクトリにアクセスし、ファイルシステム管理者がWindowsベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合にも、このような設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

関連情報

- %u 変数を使用してホームディレクトリを構成する

- 追加のホームディレクトリ構成について学ぶ
- ユーザーのホームディレクトリパスに関する情報を表示する

%u変数を使用して**ONTAP SMB**ホームディレクトリを構成する

ホームディレクトリ設定を作成し、変数を使用して共有名を指定し、変数を使用して `%u` ホームディレクトリ共有の相対パスを指定することができます `%w`。これにより、ユーザは、ホームディレクトリの実際の名前やパスを意識することなく、Windowsユーザ名を使用して動的に作成された共有を使用してホーム共有に接続できます。

手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 目的のセキュリティ形式がqtreeで使用されていない場合は、コマンドを使用してセキュリティ形式を変更し `volume qtree security`ます。
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver` `vserver`検索パスを追加するCIFS対応のStorage Virtual Machine（SVM）を指定します。

   `-share-name` `%w`ホームディレクトリ共有名を指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _windows_user_name の形式で共有名が動的に作成されます。

   > オプションに変数 `-share-name`を使用することもでき `%u`ます。これにより、マッピングされたUNIXユーザ名を使用する相対共有パスが作成されます。

   `-path` `%u`ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _mapped_UNIX_user_name の形式で共有名が動的に作成されます。

   > このオプションの値には、静的要素も含めることができます。たとえば、 `eng/%u`です。

   `-share-properties` `homedirectory\[,...\]`その共有の共有プロパティを指定します。値を指定する必要があり `homedirectory`ます。追加の共有プロパティをカンマで区切って指定できます。

5. コマンドを使用して、共有が目的の設定になっていることを確認します `vserver cifs share show`。
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` `vserver`検索パスを追加するCIFS対応のSVMを指定します。

   `-path` `path`検索パスの絶対ディレクトリパスを指定します。

7. コマンドを使用して、検索パスが追加されたことを確認します `vserver cifs home-directory search-path show`。
8. UNIXユーザが存在しない場合は、コマンドを使用してUNIXユーザを作成し `vserver services unix-user create`ます。

ユーザをマッピングする前に、Windowsユーザ名のマッピング先となるUNIXユーザ名が存在している必要があります。

9. 次のコマンドを使用して、UNIXユーザへのWindowsユーザのネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   WindowsユーザをUNIXユーザにマッピングするネームマッピングがすでに存在する場合は、マッピング手順を実行する必要はありません。

   Windowsユーザ名は対応するUNIXユーザ名にマッピングされます。Windowsユーザは、ホームディレクトリ共有に接続すると、Windowsユーザ名に対応する共有名を使用して動的に作成されたホームディレクトリに接続します。ディレクトリ名がUNIXユーザ名に対応していることは認識されません。

10. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定したqtreeまたはボリューム内に、対応するディレクトリを作成します。

    たとえば、というパスのqtreeを作成し、ディレクトリの作成対象となるユーザのマッピングされたUNIXユーザ名が「unixuser1」の場合、 `/vol/vol1/users`というパスでディレクトリを作成します `/vol/vol1/users/unixuser1`。

    にマウントされる「home1」という名前のボリュームを作成した場合は、というパスでディレクトリを作成し `/home1`ます `/home1/unixuser1`。

11. ドライブをマッピングするか、UNCパスを使用して接続し、ユーザがホーム共有に正常に接続できることを確認します。

    たとえば、UNIXユーザunixuser1にマッピングされるユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順10で作成）に接続する場合は、UNCパスを使用して接続し `\\vs1\user1`ます。

例

次の例のコマンドは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は%wです。
- 相対ホームディレクトリパスは%uです。
- ホームディレクトリを含むように指定した検索パス `/home1`は、UNIXセキュリティ形式が設定されたボリュームです。
- 設定はSVM vs1に作成されます。

ユーザがWindowsホスト、またはWindowsホストとUNIXホストの両方からホームディレクトリにアクセスし、ファイルシステム管理者がUNIXベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合は、このようなホームディレクトリ設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

関連情報

- %w および %d 変数を使用してホームディレクトリ構成を作成します
- 追加のホームディレクトリ構成について学ぶ
- ユーザーのホームディレクトリパスに関する情報を表示する

、 %d`の `%u`各変数を使用して追加のホームディレクトリの設定を作成し、ニーズに合わせてホームディレクトリの設定をカスタマイズできます `%w。

共有名と検索パスで変数と静的文字列の組み合わせを使用して、多数のホームディレクトリの設定を作成できます。次の表に、さまざまなホームディレクトリ設定を作成する例を示します。

がホームディレクトリを含む場合に作成されるパス /vol1/user	**share** コマンド
ユーザをに転送する /vol1/user/win_username` 共有パスを作成するには `\\vs1\~win_username	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
ユーザをに転送する /vol1/user/domain/win_username`共有パスを作成するには `\\vs1\win_username	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
ユーザをに転送する /vol1/user/unix_username`共有パスを作成するには `\\vs1\win_username	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
ユーザをに転送する /vol1/user/unix_username`共有パスを作成するには `\\vs1\unix_username	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

SMB検索パスを管理するための**ONTAP**コマンド

ONTAPには、SMBホームディレクトリ設定の検索パスを管理するためのコマンドが用意されています。たとえば、検索パスを追加、削除、および情報を表示するためのコマンドが用意されています。また、検索パスの順序を変更するためのコマンドもあります。

状況	使用するコマンド
検索パスを追加する	`vserver cifs home-directory search-path add`
検索パスを表示します。	`vserver cifs home-directory search-path show`
検索パスの順序を変更する	`vserver cifs home-directory search-path reorder`

状況	使用するコマンド
検索パスを削除する	`vserver cifs home-directory search-path remove`

の詳細については `vserver cifs home-directory search-path`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMBユーザのホームディレクトリパスに関する情報を表示する

Storage Virtual Machine（SVM）上のSMBユーザのホームディレクトリパスを表示できます。このパスは、複数のCIFSホームディレクトリパスが設定されていて、ユーザのホームディレクトリがあるパスを確認する場合に使用できます。

ステップ

1. コマンドを使用して、ホームディレクトリパスを表示します `vserver cifs home-directory show-user`。

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  ----------------------
   vs1          user1                /home/user1
   ```

関連情報

ユーザーのホームディレクトリへのアクセスを管理する

ONTAP SMBユーザのホームディレクトリへのアクセスを管理する

デフォルトでは、ユーザのホームディレクトリにアクセスできるのはそのユーザだけです。動的な共有名の前にチルダ（ ｛チルダ｝ ）が付いている共有の場合、 Windows 管理者や他のユーザ（パブリックアクセス）によるユーザのホームディレクトリへのアクセスを有効または無効にできます。

開始する前に

Storage Virtual Machine （ SVM ）のホームディレクトリ共有に、動的な共有名の前にチルダ（ ｛チルダ｝ ）を追加した共有名を設定する必要があります。共有の命名要件を次に示します。

ホームディレクトリ共有名	共有に接続するコマンドの例
｛チルダ｝ %d ｛チルダ｝ %w	`net use * \\IPaddress\~domain~user/u:credentials`
｛チルダ｝ %w	`net use * \\IPaddress\~user/u:credentials`

ホームディレクトリ共有名	共有に接続するコマンドの例
｛チルダ｝ abc ｛チルダ｝ %w	`net use * \\IPaddress\abc~user/u:credentials`

ステップ

1. 適切な操作を実行します。

ユーザのホームディレクトリへのアクセスを有効または無効にする対象	入力するコマンド
Windows管理者	`vserver cifs home-directory modify -vserver` *vserver_name* `-is-home-dirs -access-for-admin-enabled {true|false}`デフォルトはです `true。
任意のユーザ（パブリックアクセス）	a. 権限レベルをadvancedに設定します。+ `set -privilege advanced` b. アクセスを有効または無効にします。 `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public -enabled {true

次の例は、ユーザのホームディレクトリへのパブリックアクセスを有効にします。

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true++
set -privilege admin
```

関連情報

ユーザーのホームディレクトリパスに関する情報を表示する

UNIXシンボリックリンクへのSMBクライアントアクセスの設定

ONTAP SMBクライアントにUNIXシンボリックリンクへのアクセスを提供する方法について学習します。

シンボリックリンクは UNIX 環境で作成されるファイルで、別のファイルまたはディレクトリへの参照が含まれます。シンボリックリンクにアクセスしたクライアントは、シンボリックリンクが参照するターゲットファイルまたはディレクトリにリダイレクトされます。ONTAPは、ワイドリンク（ローカルファイルシステムの外部にあるターゲットとの絶対リンク）を含む相対シンボリックリンクと絶対シンボリックリンクをサポートします。

ONTAP には、 SMB クライアントが SVM で設定されている UNIX のシンボリックリンクをたどるための機能が用意されています。この機能はオプションであり、次のいずれかの設定を指定してコマンドのオプションを `vserver cifs share create`使用すると、共有ごとに設定でき `-symlink-properties`ます。

- 読み取り / 書き込みアクセスで有効化

- 読み取り専用アクセスで有効化
- SMB クライアントに対してシンボリックリンクを非表示にして無効にしました
- SMB クライアントからシンボリックリンクへのアクセス権なしで無効になりました

共有でシンボリックリンクを有効にした場合、相対シンボリックリンクは追加の設定なしで機能します。

共有でシンボリックリンクを有効にしただけでは、絶対シンボリックリンクは機能しません。最初に、シンボリックリンクの UNIX パスからデスティネーション SMB パスへのマッピングを作成する必要があります。絶対シンボリックリンクのマッピングを作成する場合、ローカルリンクか a_widelink ；ワイドリンクを他のストレージデバイス上のファイルシステムにリンクするか、同じ ONTAP システム上の別々の SVM でホストされているファイルシステムにリンクするかを指定できます。ワイドリンクを作成するときは、クライアントがたどる情報を含める必要があります。つまり、クライアントがディレクトリジャンクションポイントを検出するためのリパースポイントを作成します。ローカル共有外のファイルまたはディレクトリへの絶対シンボリックリンクを作成しても、局所性をローカルに設定すると、 ONTAP はターゲットへのアクセスを許可しません。

> クライアントがローカルシンボリックリンク（絶対または相対）を削除しようとすると、シンボリックリンクのみが削除され、ターゲットファイルやターゲットディレクトリは削除されません。ただし、クライアントがワイドリンクを削除しようとすると、ワイドリンクが参照する実際のターゲットファイルやターゲットディレクトリが削除される可能性があります。クライアントは SVM 外のターゲットファイルまたはディレクトリを明示的に開いて削除できるため、 ONTAP ではこの操作を制御できません。

- * リパースポイントと ONTAP ファイルシステムサービス *

  a_reparse point_ は、オプションでファイルとともにボリュームに格納できる NTFS ファイルシステムオブジェクトです。リパースポイントを使用すると、SMBクライアントは、NTFS形式のボリュームを使用する際に拡張ファイルシステムサービスを利用できます。リパースポイントは、リパースポイントのタイプを識別する標準のタグと、SMBクライアントが取得して以降の処理を実行できるリパースポイントの内容で構成されます。ファイルシステムの拡張機能で使用できるオブジェクトタイプのうち、ONTAPでは、リパースポイントタグを使用したNTFSシンボリックリンクとディレクトリジャンクションポイントのサポートが実装されています。リパースポイントの内容を理解できないSMBクライアントは、リパースポイントを無視し、リパースポイントで有効になる可能性のある拡張ファイルシステムサービスを提供しません。

- * ディレクトリジャンクションポイントおよびシンボリックリンクの ONTAP サポート *

  ディレクトリジャンクションポイントはファイルシステムディレクトリ構造内の場所で、別のパス（シンボリックリンク）または別のストレージデバイス（ワイドリンク）上のファイルが格納されている別の場所を参照できます。ONTAP SMBサーバはディレクトリジャンクションポイントをリパースポイントとしてWindowsクライアントに公開するため、対応するクライアントは、ディレクトリジャンクションポイントがトラバースされたときにONTAPからリパースポイントのコンテンツを取得できます。これにより、同じファイルシステムの一部であるかのように、異なるパスやストレージデバイスに移動して接続できます。

- * リパースポイントオプションを使用したワイドリンクサポートの有効化 *

  ONTAP 9では、この `-is-use-junctions-as-reparse-points-enabled`オプションはデフォルトで有効になっています。すべてのSMBクライアントがワイドリンクをサポートしているわけではないため、この情報を有効にするオプションはプロトコルバージョンごとに設定可能です。これにより、管理者はサポートされているSMBクライアントとサポートされていないSMBクライアントの両方に対応できます。このオプションを有効にする必要があります。 `-widelink-as-reparse-point-versions`ワイドリンクを使用して共有にア

クセスする各クライアント プロトコル。デフォルトは SMB1 です。

関連情報

- "WindowsバックアップアプリケーションとUNIX形式のシンボリックリンク"
- "Microsoft のドキュメント：「 Reparse Points"

ONTAP SMBアクセス用の**UNIX**シンボリックリンクを設定する際の制限

SMBアクセス用にUNIXシンボリックリンクを設定する場合は、一定の制限事項に注意する必要があります。

制限	説明
45	CIFSサーバ名のFQDNを使用して指定できるCIFSサーバ名の最大長。 代わりに、CIFSサーバ名を15文字以内のNetBIOS名として指定することもできます。
80	共有名の最大文字数。
256	シンボリックリンクを作成するとき、または既存のシンボリックリンクのUNIXパスを変更するときに指定できるUNIXパスの最大長。UNIXパスは「/」で始まる必要があります。/`" (slash) and end with a "`先頭と末尾のスラッシュは、256文字の制限の一部としてカウントされます。
256	シンボリックリンクの作成時、または既存のシンボリックリンクのCIFSパスの変更時に指定できるCIFSパスの最大長。CIFSパスはで始まる必要があります。/`" (slash) and end with a "`先頭と末尾のスラッシュは、256文字の制限の一部としてカウントされます。

関連情報

共有のシンボリックリンクマッピングを作成する

ONTAP SMBサーバ上の自動**DFS**アドバタイズメントを制御する

共有に接続する SMB クライアントに DFS 対応を通知する方法は、 CIFS サーバオプションで制御されます。ONTAP では、クライアントが SMB 経由でシンボリックリンクにアクセスするときに DFS リファーラルを使用するため、このオプションを無効または有効にしたときの影響を理解しておく必要があります。

DFS に対応していることを CIFS サーバが SMB クライアントに自動的に通知するかどうかは、 CIFS サーバオプションで指定します。デフォルトでは、このオプションは有効になっており、 CIFS サーバは DFS に対

応していることを常に SMB クライアントに（たとえシンボリックリンクへのアクセスが無効になっている共有に接続する場合でも）通知します。シンボリックリンクへのアクセスが有効になっている共有にクライアントが接続する場合にのみ、 DFS に対応していることを CIFS サーバがクライアントに通知するようにするには、このオプションを無効にします。

このオプションを無効にすると次のような影響があることに注意してください。

- シンボリックリンクの共有設定は変更されません。
- シンボリックリンクアクセス（読み取り / 書き込みアクセスまたは読み取り専用アクセス）を許可するように共有パラメータが設定されている場合、 CIFS サーバは、その共有に接続するクライアントに DFS 対応を通知します。

  シンボリックリンクへのクライアントの接続とアクセスは中断されることなく続行されます。

- シンボリックリンクアクセスを許可しないように共有パラメータが設定されている場合（アクセスを無効にしているか共有パラメータの値が null の場合）、 CIFS サーバは、その共有に接続するクライアントに DFS 対応を通知しません。

  クライアントは、 CIFS サーバが DFS に対応しているというキャッシュされた情報を保持しており、 CIFS サーバはそのことを通知しなくなるので、シンボリックリンクアクセスが無効になっている共有に接続されたクライアントは、 CIFS サーバオプションが無効になったあとでそれらの共有にアクセスできなくなることがあります。オプションが無効になったあとで、それらの共有に接続されたクライアントをリブートし、キャッシュされた情報を消去する必要があります。

これらの変更は SMB 1.0 の接続には適用されません。

ONTAP SMB共有でUNIXシンボリックリンクのサポートを構成する

SMB共有の作成時に、または既存のSMB共有の変更によっていつでも、シンボリックリンクの共有プロパティ設定を指定することで、SMB共有でUNIXシンボリックリンクのサポートを設定できます。UNIXシンボリックリンクのサポートはデフォルトで有効になっています。共有でUNIXシンボリックリンクのサポートを無効にすることもできます。

タスクの内容

SMB共有に対してUNIXシンボリックリンクのサポートを設定する場合は、次のいずれかの設定を選択できます。

設定	説明
`enable`（廃止予定*）	読み取り/書き込みアクセスに対してシンボリックリンクを有効にします。
`read_only`（廃止予定*）	読み取り専用アクセスに対してシンボリックリンクを有効にします。この設定はワイドリンクには適用されません。Widelinkアクセスは常に読み取り/書き込みです。
`hide`（廃止予定*）	SMBクライアントにシンボリックリンクが表示されないように指定します。

設定	説明
`no-strict-security`	クライアントが共有の範囲外でシンボリックリンクを参照するように指定します。
`symlinks`	読み取り/書き込みアクセスに対してローカルシンボリックリンクを有効にします。CIFSオプションがに設定されて `true`いても、DFS通知は生成されません `is-advertise-dfs-enabled。これがデフォルト設定です。
`symlinks-and-widelinks`	読み取り/書き込みアクセスに対してローカルシンボリックリンクとワイドリンクの両方を指定します。CIFSオプションがに設定されて `false`いる場合でも、DFS通知はローカルシンボリックリンクとワイドリンクの両方に対して生成され `is-advertise-dfs-enabled`ます。
`disable`	シンボリックリンクとワイドリンクを無効にします。CIFSオプションがに設定されて `true`いても、DFS通知は生成されません `is-advertise-dfs-enabled。
""（null、未設定）	シンボリックリンクを共有で無効にします。
-（未設定）	シンボリックリンクを共有で無効にします。

- ONTAP の今後のリリースでは、 *enable*,*hide*,_read-only パラメータは廃止されており、削除される可能性があります。

手順

1. シンボリックリンクのサポートを設定または無効にします。

条件	入力するコマンド
新しいSMB共有	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	既存のSMB共有

条件	入力するコマンド
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. SMB共有の設定が正しいことを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

例

次のコマンドでは、UNIXシンボリックリンク設定をに設定して、「data1」という名前のSMB共有を作成し`enable`ます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

関連情報

共有のシンボリックリンクマッピングを作成する

SMB共有に対するUNIXシンボリックリンクのマッピングを作成できます。親フォルダを基準としたファイルまたはフォルダを参照する相対シンボリックリンクを作成することも、絶対パスを使用してファイルまたはフォルダを参照する絶対シンボリックリンクを作成することもできます。

タスクの内容

SMB 2.xを使用している場合、Mac OS Xクライアントからワイドリンクにアクセスすることはできません。ユーザがMac OS Xクライアントからワイドリンクを使用して共有に接続しようとすると、接続は失敗します。ただし、SMB 1を使用している場合は、Mac OS Xクライアントでワイドリンクを使用できます。

手順

1. SMB共有のシンボリックリンクマッピングを作成するには： `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver` `virtual_server_name`Storage Virtual Machine（SVM）名を示します。

   `-unix-path` `path`UNIXパスを指定します。UNIXパスはスラッシュ(/で始まる必要があります）、およびスラッシュで終わる必要があり(/ます。

   `-share-name` `share_name`マッピングするSMB共有の名前を指定します。

   `-cifs-path` `path`CIFSパスを指定します。CIFSパスはスラッシュ(/で始まる必要があります）、およびスラッシュで終わる必要が(/あります。

   `-cifs-server` `server_name`CIFSサーバ名を指定します。CIFSサーバ名は、DNS名（mynetwork.cifs.server.comなど）、IPアドレス、またはNetBIOS名で指定できます。NetBIOS名は、コマンドを使用して確認できます `vserver cifs show`。（オプション）このパラメータを指定しない場合、デフォルト値はローカルCIFSサーバのNetBIOS名です。

   `-locality` `local|free|widelink}`は、ローカルリンク、フリーリンク、ワイドシンボリックリンクのいずれを作成するかを指定します。ローカルシンボリックリンクはローカルSMB共有にマッピングされます。フリーシンボリックリンクは、ローカルSMBサーバ上の任意の場所にマッピングできます。ワイドシンボリックリンクは、ネットワーク上の任意のSMB共有にマッピングされます。このオプションパラメータを指定しない場合、デフォルト値はです `local`。

   `-home-directory` `true` `false}` ターゲットの共有がホームディレクトリかどうかを指定します。このパラメータはオプションですが、ターゲットの共有をホームディレクトリとして設定する場合は、このパラメータをに設定する必要があります `true`。デフォルトはです `false`。

例

次のコマンドは、vs1という名前のSVM上にシンボリックリンクマッピングを作成します。このマッピングは、UNIXパス `/src/`、SMB共有名「ソース」、CIFSパス、CIFS `/mycompany/source/`サーバのIPアドレスが123.123.123.123で、ワイドリンクです。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

関連情報

共有上のUNIXシンボリックリンクのサポートを構成する

SMBシンボリックリンクマッピングを管理するための**ONTAP**コマンド

ONTAP には、シンボリックリンクのマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
シンボリックリンクのマッピングを作成します	`vserver cifs symlink create`
シンボリックリンクのマッピングに関する情報を表示する	`vserver cifs symlink show`
シンボリックリンクのマッピングを変更する	`vserver cifs symlink modify`
シンボリックリンクのマッピングを削除する	`vserver cifs symlink delete`

の詳細については `vserver cifs symlink`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SMB サーバー上の **Windows** バックアップ アプリケーションと **Unix** スタイルのシンボリック リンク

Windowsで実行されているバックアップアプリケーションでUNIX形式のシンボリックリンク（symlink）が検出されると、リンクに従ってデータがバックアップされます。ONTAP 9.15.1以降では、データの代わりにシンボリックリンクをバックアップするオプションが用意されています。この機能は、ONTAP FlexGroupボリュームとFlexVolで完全にサポートされています。

概要

Windowsバックアップ処理中のシンボリックリンクの処理方法を変更する前に、ONTAP利点、主要な概念、および設定オプションについて理解しておく必要があります。

メリット

この機能を無効にするか使用できない場合、各シンボリックリンクがトラバースされ、リンク先のデータがバックアップされます。このため、不要なデータがバックアップされることがあり、特定の状況ではアプリケーションがループに陥る可能性があります。代わりに、シンボリックリンクをバックアップすることでこれらの問題を回避できます。また、ほとんどの場合、シンボリックリンクファイルはデータに比べて非常に小さいため、バックアップにかかる時間が短縮されます。IO処理が減少するため、クラスタの全体的なパフォーマンスも向上します。

Windowsサーバ環境

この機能は、Windowsで実行されているバックアップアプリケーションでサポートされています。環境を使用する前に、環境の関連する技術的側面を理解しておく必要があります。

拡張属性

Windowsでは、拡張属性（EA）がサポートされています。この拡張属性は、オプションでファイルに関連付けられた追加のメタデータをまとめて形成します。これらの属性は、Windows Subsystem for Linuxなどのさまざまなアプリケーションで使用されます（を参照） "WSLのファイル権限"。アプリケーションは、ONTAPからデータを読み取るときに、各ファイルの拡張属性を要求できます。

シンボリックリンクは、この機能が有効になっている場合に拡張属性で返されます。したがって、バックアップアプリケーションは、メタデータの格納に使用される標準のEAサポートを提供する必要があります。一部のWindowsユーティリティでは、拡張属性がサポートされ、保持されます。ただし、バックアップソフトウェアで拡張属性のバックアップとリストアがサポートされていない場合は、各ファイルに関連付けられているメタデータが保持されず、シンボリックリンクの適切な処理が失敗します。

Windowsコウセイ

Microsoft Windowsサーバ上で実行されているバックアップアプリケーションには、通常のファイルセキュリティをバイパスできる特別な権限を付与できます。これは通常、アプリケーションをBackup Operatorsグループに追加することによって行われます。アプリケーションは、必要に応じてファイルをバックアップおよび復元したり、その他の関連システム操作を実行したりできます。バックアップアプリケーションで使用されるSMBプロトコルにはわずかな変更が加えられていますが、データの読み取りと書き込みの際にONTAPで検出される可能性があります。

要件

シンボリックリンクバックアップ機能には、次のようないくつかの要件があります。

- クラスタでONTAP 9.15.1以降が実行されている。
- 特別なバックアップ権限が付与されたWindowsバックアップアプリケーション。
- バックアップアプリケーションでは、拡張属性もサポートし、バックアップ処理中に要求する必要があります。
- 該当するデータSVMに対してONTAPシンボリックリンクバックアップ機能が有効になっている。

設定オプション

ONTAP CLIに加えて、REST APIを使用してこの機能を管理することもできます。詳細については、を参照してください "ONTAP REST APIと自動化の新機能" 。ONTAPでのUNIX形式のシンボリックリンクの処理方法を決定する設定は、SVMごとに個別に実行する必要があります。

ONTAPでシンボリックリンクバックアップ機能を有効にする

ONTAP 9.15.1では、既存のCLIコマンドに設定オプションが導入されています。このオプションを使用すると、UNIX形式のシンボリックリンク処理を有効または無効にできます。

開始する前に

基本を確認します [要件]。その他：

- CLI権限をadvancedレベルに昇格できるようにします。

- 変更するデータSVMを決定します。このコマンド例ではSVMを `vs1` 使用しています。

手順

1. advanced権限レベルを設定します。

```
set privilege advanced
```

2. シンボリックリンクファイルのバックアップを有効にします。

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

BranchCacheを使用してブランチオフィスで**SMB**共有のコンテンツをキャッシュする

BranchCache を使用してブランチ オフィスで **ONTAP SMB** 共有コンテンツをキャッシュする方法について説明します。

BranchCacheは、要求元のクライアントのローカルコンピュータにコンテンツをキャッシュできるようにするためにMicrosoftが開発したものです。ONTAPにBranchCacheを実装すると、Storage Virtual Machine（SVM）に格納されたコンテンツにSMBを使用してブランチオフィスのユーザがアクセスする際に、広域ネットワーク（WAN）の使用量を抑え、アクセス応答時間を短縮できます。

BranchCacheを設定すると、Windows BranchCacheクライアントはまずSVMのコンテンツを取得し、次にそのコンテンツをブランチオフィスのコンピュータにキャッシュします。ブランチオフィスの別のBranchCache対応クライアントが同じコンテンツを要求すると、SVMは最初に要求元ユーザの認証と許可を行います。次にSVMは、キャッシュされたコンテンツが最新のものであるかどうかを確認し、最新のものである場合はそのコンテンツに関するメタデータをクライアントに送信します。クライアントは、そのメタデータを使用して、ローカルのキャッシュから直接コンテンツを取得します。

関連情報

オフラインファイルを使用して、オフラインで使用するためにファイルをキャッシュできるようにする方法について学習します。

要件とガイドライン

ONTAP SMB BranchCache バージョンのサポートについて

ONTAPでサポートされるBranchCacheのバージョンを確認しておく必要があります。

ONTAPでは、BranchCache 1と強化されたBranchCache 2がサポートされています。

- Storage Virtual Machine（SVM）のSMBサーバでBranchCacheを設定するときに、BranchCache 1、BranchCache 2、またはすべてのバージョンを有効にすることができます。

  デフォルトでは、すべてのバージョンが有効になっています。

- BranchCache 2のみを有効にする場合は、リモートオフィスのWindowsクライアントマシンでBranchCache 2がサポートされている必要があります。

BranchCache 2をサポートするのはSMB 3.0以降のクライアントだけです。

BranchCacheのバージョンの詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

ONTAP SMBネットワークプロトコルのサポート要件について学ぶ

ONTAP BranchCache を実装するときは、ネットワークプロトコルの要件を考慮する必要があります。

ONTAP BranchCache 機能は、 SMB 2.1 以降を使用して、 IPv4 および IPv6 のネットワークに実装できます。

BranchCache の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、 SMB 2.1 以降のプロトコルを有効にする必要があります。SMB 2.1 では、プロトコルの機能拡張により、クライアントを BranchCache 環境に含めることができます。SMB プロトコルとして BranchCache をサポートするために必要な最小バージョンを指定してください。SMB 2.1 は、 BranchCache バージョン 1 をサポートします。

BranchCache バージョン 2 を使用する場合は、サポートする SMB の最小バージョンは SMB 3.0 になります。BranchCache 2 の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、 SMB 3.0 以降を有効にする必要があります。

リモートオフィスでSMB 2.1のみをサポートするクライアントとSMB 3.0をサポートするクライアントがある場合は、BranchCache 1とBranchCache 2の両方でキャッシュをサポートするCIFSサーバにBranchCache設定を実装できます。

Microsoft BranchCache 機能ではファイルアクセスプロトコルとして HTTP / HTTPS と SMB プロトコルの両方がサポートされますが、 ONTAP BranchCache でサポートされるのは SMB のみです。

ONTAP SMBおよび**Windows**ホストのバージョン要件について学ぶ

BranchCacheを設定するには、ONTAPやブランチオフィスのWindowsホストが特定のバージョン要件を満たしている必要があります。

BranchCacheを設定するには、クラスタのONTAPのバージョンや対象となるブランチオフィスのクライアントで、SMB 2.1以降とBranchCacheの機能をサポートしている必要があります。ホスト型キャッシュモードを設定する場合は、サポートされているホストをキャッシュサーバに使用する必要もあります。

BranchCache 1は、次のONTAPバージョンおよびWindowsホストでサポートされています。

- コンテンツサーバ：ONTAPを備えたStorage Virtual Machine（SVM）
- キャッシュサーバ： Windows Server 2008 R2 または Windows Server 2012 以降
- ピアまたはクライアント： Windows 7 Enterprise 、 Windows 7 Ultimate 、 Windows 8 、 Windows Server 2008 R2 、または Windows Server 2012 以降

BranchCache 2は、次のONTAPバージョンおよびWindowsホストでサポートされています。

- コンテンツサーバ： ONTAP を備えた SVM
- キャッシュサーバ： Windows Server 2012 以降
- ピアまたはクライアント： Windows 8 または Windows Server 2012 以降

ONTAP SMBが**BranchCache**ハッシュを無効にする理由について学ぶ

ONTAP でどのような場合にハッシュが無効になるかを理解すると、 BranchCache の設定を計画するときに役立ちます。この情報に基づいて、設定する必要がある動作モードの決定と、 BranchCache を有効にする共有を選択するかどうかの検討の助けになります。

ONTAP は、 BranchCache ハッシュが有効なものであるかを管理しています。ハッシュが無効な場合、 ONTAP は次にコンテンツが要求されたときにハッシュを無効にして新しいハッシュを計算します。これは、 BranchCache が有効なままであることを前提としています。

ONTAP は、以下の場合にハッシュを無効にします。

- サーバキーが変更された場合。

  サーバキーが変更された場合は、 ONTAP によってハッシュストア内のすべてのハッシュが無効になります。

- BranchCache のハッシュストアの最大サイズに達したために、ハッシュがキャッシュからフラッシュされた場合。

  このパラメータは調整可能で、ビジネス要件に合わせて変更することができます。

- SMB または NFS 経由のアクセスでファイルが変更された場合。
- 有効なハッシュが含まれているファイルがコマンドを使用してリストアされた `snap restore`場合。
- BranchCache対応のSMB共有を含むボリュームがコマンドを使用してリストアされた場合 `snap restore`。

ONTAP SMBハッシュストアの場所の選択について学ぶ

BranchCacheを設定する場合は、ハッシュを格納する場所とハッシュストアのサイズを選択します。ハッシュストアの場所とサイズの選択に関するガイドラインについて理解しておくと、CIFS対応のSVMでBranchCacheの設定を計画するのに役立ちます。

- ハッシュストアは、atime更新が許可されているボリュームに配置する必要があります。

  ハッシュファイルへのアクセス時間は、アクセス頻度の高いファイルをハッシュストア内に保持するために使用されます。atime更新が無効になっている場合は、作成時間がこの目的に使用されます。頻繁に使用するファイルを追跡するには、atimeを使用することを推奨します。

- SnapMirrorデスティネーションやSnapLockボリュームなどの読み取り専用のファイルシステムにはハッシュを保存できません。
- ハッシュストアの最大サイズに達すると、古いハッシュがフラッシュされて新しいハッシュ用のスペースが確保されます。

ハッシュストアの最大サイズを拡張して、キャッシュからフラッシュされるハッシュの量を減らすことができます。

- ハッシュを格納するボリュームが使用できないかいっぱいである場合、またはクラスタ内通信に問題があり、BranchCacheサービスがハッシュ情報を取得できない場合は、BranchCacheサービスを使用できません。

  ボリュームがオフラインであるか、ストレージ管理者がハッシュストアの新しい場所を指定したために、ボリュームを使用できない可能性があります。

  これにより、ファイルアクセスで問題が発生することはありません。ハッシュストアに正常にアクセスできない場合、ONTAPはMicrosoft定義のエラーをクライアントに返します。これにより、クライアントは通常のSMB読み取り要求を使用してファイルを要求します。

関連情報

- サーバー上でBranchCacheを構成する
- 共有上の BranchCache 構成を変更する

ONTAP SMB BranchCacheの推奨事項について学ぶ

BranchCache を設定する前に、 BranchCache キャッシュを有効にする SMB 共有の決定時に考慮する必要がある推奨事項がいくつかあります。

使用する動作モードと BranchCache を有効にする SMB 共有の決定時には、次の推奨事項を考慮してください。

- リモートからキャッシュするデータが頻繁に変更されると、 BranchCache の利点が十分には生かされません。
- BranchCacheサービスは、複数のリモートオフィスクライアントで再利用されるファイルコンテンツや、1人のリモートユーザが繰り返しアクセスするファイルコンテンツを含む共有の場合に便利です。
- SnapshotやSnapMirrorデスティネーションのデータなど、読み取り専用コンテンツのキャッシュを有効にすることを検討してください。

BranchCacheの設定

ONTAP SMB BranchCache の構成について学ぶ

SMBサーバでBranchCacheを設定するには、ONTAPコマンドを使用します。BranchCache を実装するには、クライアント、および必要に応じてコンテンツをキャッシュするブランチオフィスにホストされるキャッシュサーバも設定する必要があります。

共有ごとにキャッシュを有効にするように BranchCache を設定する場合は、 BranchCache キャッシュサービスの対象となる SMB 共有で BranchCache を有効にする必要があります。

ONTAP SMB BranchCache を構成するための要件

BranchCacheをセットアップするには、いくつかの前提条件を満たしている必要があります。

SVMのCIFSサーバでBranchCacheを設定するには、次の要件を満たしている必要があります。

- クラスタ内のすべてのノードにONTAPがインストールされている必要があります。
- CIFSのライセンスが有効になっていて、SMBサーバが設定されている必要があります。SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- IPv4またはIPv6のネットワーク接続が設定されている必要があります。
- BranchCache 1の場合、SMB 2.1以降が有効になっている必要があります。
- BranchCache 2の場合、SMB 3.0が有効になっていて、リモートのWindowsクライアントでBranchCache 2がサポートされている必要があります。

ONTAP SMBサーバーで**BranchCache**を構成する

BranchCacheサービスを共有ごとに提供するようにBranchCacheを設定できます。また、すべてのSMB共有でキャッシュを自動的に有効にするようにBranchCacheを設定することもできます。

タスクの内容

BranchCacheはSVMで設定できます。

- CIFSサーバ上のすべてのSMB共有に格納されたすべてのコンテンツに対してキャッシュサービスを提供する場合は、すべての共有のBranchCache設定を作成できます。
- CIFSサーバ上の選択したSMB共有に格納されたコンテンツに対してキャッシュサービスを提供する場合は、共有ごとのBranchCache設定を作成できます。

BranchCacheの設定時には、次のパラメータを指定する必要があります。

必須パラメータ	説明
SVM 名 _	BranchCacheはSVM単位で設定します。BranchCacheサービスを設定するCIFS対応SVMを指定する必要があります。

必須パラメータ	説明
ハッシュストアへのパス _	BranchCacheハッシュは、SVMボリューム上の通常のファイルに格納されます。ONTAPにハッシュデータを格納する既存のディレクトリのパスを指定する必要があります。BranchCacheハッシュパスは読み取り/書き込み可能である必要があります。Snapshotディレクトリなどの読み取り専用パスは指定できません。他のデータを含むボリュームにハッシュデータを格納することも、ハッシュデータを格納するための別のボリュームを作成することもできます。 SVMがSVMディザスタリカバリソースの場合、ハッシュパスをルートボリュームに配置することはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。 ハッシュパスには、空白とファイル名の有効な文字を含めることができます。

必要に応じて、次のパラメータを指定できます。

オプションのパラメータ	説明
サポートされているバージョン _	ONTAPでは、BranchCache 1および2がサポートされます。バージョン1、バージョン2、またはその両方を有効にできます。デフォルトでは、両方のバージョンが有効になります。
_ ハッシュストアの最大サイズ _	ハッシュデータストアに使用するサイズを指定できます。ハッシュデータがこの値を超えると、ONTAPは古いハッシュを削除して新しいハッシュ用のスペースを確保します。ハッシュストアのデフォルトサイズは1GBです。ハッシュが過度に破棄されない場合、BranchCacheのパフォーマンスは向上します。ハッシュストアがいっぱいになったためにハッシュが頻繁に破棄されると判断した場合は、BranchCacheの設定を変更してハッシュストアのサイズを大きくすることができます。

オプションのパラメータ	説明
_ サーバキー _	クライアントがBranchCacheサーバを偽装できないようにするためにBranchCacheサービスで使用されるサーバキーを指定できます。指定しない場合、BranchCacheの設定の作成時にサーバキーがランダムに生成されます。サーバキーを特定の値に設定すると、複数のサーバが同じファイルのBranchCacheデータを提供している場合に、クライアントが同じサーバキーを使用して任意のサーバのハッシュを使用できるようになります。サーバキーにスペースを含める場合は、サーバキーを引用符で囲む必要があります。
オペレーティングモード _	デフォルトでは、BranchCacheは共有ごとに有効になります。 • BranchCacheを共有ごとに有効にするBranchCacheの設定を作成するには、このオプションパラメータを指定しないか、を指定します `per-share`。 • すべての共有でBranchCacheを自動的に有効にするには、動作モードをに設定する必要があります `all-shares`。

手順

1. 必要に応じてSMB 2.1および3.0を有効にします。
   a. 権限レベルをadvancedに設定します。 `set -privilege advanced`
   b. SVMのSMB設定を確認して、必要なすべてのバージョンのSMBが有効になっているかどうかを確認します。 `vserver cifs options show -vserver vserver_name`
   c. 必要に応じて、SMB 2.1を有効にします。 `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      コマンドは、SMB 2.0とSMB 2.1の両方を有効にします。
   d. 必要に応じて、SMB 3.0を有効にします。 `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
   e. admin権限レベルに戻ります。 `set -privilege admin`
2. BranchCacheを設定します。 `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   指定したハッシュストレージのパスが存在し、SVMによって管理されているボリューム上にある必要があります。また、パスは読み取り / 書き込み可能なボリュームにある必要があります。パスが読み取り専用であるか、または存在しない場合、コマンドは失敗します。

   SVM BranchCacheの追加設定で同じサーバキーを使用する場合は、サーバキーとして入力した値を記録

しておきます。BranchCacheの設定に関する情報を表示しても、サーバキーは表示されません。

3. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver` *`vserver_name`*

例

次のコマンドは、SMB 2.1と3.0の両方が有効になっていることを確認し、SVM vs1のすべてのSMB共有でキャッシュを自動的に有効にするようにBranchCacheを設定します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

次のコマンドは、SMB 2.1と3.0の両方が有効になっていることを確認し、SVM vs1の共有ごとにキャッシュを有効にするようにBranchCacheを設定し、BranchCacheの設定を確認します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

関連情報

- BranchCacheのバージョンサポートについて
- リモートオフィスでのBranchCacheの構成について学ぶ
- BranchCacheが有効なSMB共有を作成する
- 既存の共有でBranchCacheを有効にする
- 共有上の BranchCache 構成を変更する
- 共有上のBranchCacheを無効にする方法について
- 共有上のBranchCache構成を削除する

ONTAP SMBでリモートオフィスに**BranchCache**を構成する方法について学習します

SMBサーバでBranchCacheを設定したら、リモートオフィスのクライアントコンピュータおよびキャッシュサーバ（オプション）にBranchCacheをインストールして設定する必要があります。リモートオフィスでBranchCacheを設定する手順については、Microsoftから説明されています。

BranchCacheを使用するようにブランチオフィスのクライアントおよびキャッシュサーバ（オプション）を設

定する手順については、MicrosoftのBranchCacheのWebサイトを参照してください。

"Microsoft BranchCache のドキュメント：「 What's New"

BranchCacheが有効な**SMB**共有の設定

BranchCache 対応 **ONTAP SMB** 共有の構成について学習します

SMBサーバとブランチオフィスでBranchCacheを設定したら、ブランチオフィスのクライアントによるコンテンツのキャッシュを許可するSMB共有でBranchCacheを有効にすることができます。

BranchCacheキャッシュは、SMBサーバ上のすべてのSMB共有で有効にすることも、共有ごとに有効にすることもできます。

- BranchCache を共有ごとに有効にする場合、 BranchCache は共有の作成時に有効にするか、既存の共有を変更して有効にすることができます。

  既存の SMB 共有でキャッシュを有効にすると、その共有で BranchCache を有効にした時点で、 ONTAP によるハッシュの計算と要求元クライアントへのメタデータの送信が開始されます。

- 共有への SMB 接続をすでに確立しているクライアントは、それ以降にその共有で BranchCache が有効になった場合、 BranchCache のサポートを得ることができません。

  ONTAP は、 SMB セッションがセットアップされたときに共有の BranchCache のサポートを通知します。BranchCacheを有効にしたときにすでにセッションを確立していたクライアントは、キャッシュされたコンテンツをこの共有で使用するために、いったん切断してから再接続する必要があります。

> その後 SMB 共有に対する BranchCache を無効にすると、 ONTAP による要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ（SMBサーバ）から直接データを取得します。

BranchCache対応の**ONTAP SMB**共有を作成する

SMB共有の作成時に共有プロパティを設定して、共有でBranchCacheを有効にすることができます `branchcache`。

タスクの内容

- SMB共有でBranchCacheが有効になっている場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

  これは、共有を作成するときのデフォルト設定です。

- BranchCacheが有効な共有を作成するときに、オプションの共有パラメータを追加で指定することもできます。
- Storage Virtual Machine（SVM）でBranchCacheが設定されておらず、有効になっていない場合でも、共有のプロパティを設定でき `branchcache`ます。

  ただし、共有でキャッシュされたコンテンツを提供するには、SVMでBranchCacheを設定して有効にする必要があります。

- パラメータを使用する場合、共有に適用されるデフォルトの共有プロパティはないため、 `-share -properties`共有プロパティに加えて、共有に適用する他のすべての共有プロパティをカンマで区切って指定する必要があります `branchcache`。
- の詳細については `vserver cifs share create`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. BranchCacheが有効なSMB共有を作成します。+
`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,…]`
2. コマンドを使用して、SMB共有に対してBranchCache共有プロパティが設定されていることを確認します `vserver cifs share show`。

例

次のコマンドは、SVM vs1上でパスを使用して、「data」という名前のBranchCacheが有効なSMB共有を作成します `/data`。デフォルトでは、オフラインファイルの設定は次のように設定されてい `manual`ます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

関連情報

単一の共有で BranchCache を無効にする

既存の **ONTAP SMB** 共有で **BranchCache** を有効にする

既存のSMB共有でBranchCacheを有効にするには、共有プロパティの既存のリストに共

有プロパティを追加し `branchcache`ます。

タスクの内容

- SMB共有でBranchCacheが有効になっている場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

  既存の共有のオフラインファイル設定が手動キャッシュに設定されていない場合は、共有を変更して設定する必要があります。

- Storage Virtual Machine（SVM）でBranchCacheが設定されておらず、有効になっていない場合でも、共有のプロパティを設定でき `branchcache`ます。

  ただし、共有でキャッシュされたコンテンツを提供するには、SVMでBranchCacheを設定して有効にする必要があります。

- 共有に共有プロパティを追加しても `branchcache`、既存の共有設定と共有プロパティは維持されます。

  branchcache共有プロパティは既存の共有プロパティリストに追加されます。の詳細については `vserver cifs share properties add`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. 必要に応じて、オフラインファイルの共有設定を手動キャッシュ用に設定します。
   a. コマンドを使用して、オフラインファイルの共有設定を確認します `vserver cifs share show`。
   b. オフラインファイルの共有設定がmanualに設定されていない場合は、必要な値に変更します。 `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. 既存のSMB共有でBranchCacheを有効にします。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. SMB共有でBranchCache共有プロパティが設定されていることを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドは、SVM vs1上のパスにある「data2」という名前の既存のSMB共有でBranchCacheを有効にします `/data2`。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

関連情報

- 既存の共有の共有プロパティを追加または削除する
- 単一の共有で BranchCache を無効にする

BranchCache設定を管理および監視する

ONTAP SMB共有の**BranchCache**構成を変更する

SVM上のBranchCacheサービスの設定では、ハッシュストアディレクトリのパス、最大サイズ、動作モード、サポートするBranchCacheのバージョンなどの設定を変更できます。ハッシュストアを含むボリュームのサイズを拡張することもできます。

手順

1. 適切な操作を実行します。

状況	入力するコマンド
ハッシュストアディレクトリのサイズ変更	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
ハッシュストアを含むボリュームのサイズを拡張する	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]`ハッシュストアを含むボリュームがいっぱいになった場合は、ボリュームのサイズを拡張できることがあります。新しいボリュームサイズは、数字と単位で指定できます。 詳細はこちら"FlexVol ボリュームの管理"	ハッシュストアディレクトリのパス変更

状況	入力するコマンド
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}`SVMがSVMディザスタリカバリソースの場合、ハッシュパスをルートボリュームに配置することはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。  BranchCacheハッシュパスには、空白とファイル名の有効な文字を含めることができます。  ハッシュパスを変更する場合、 `-flush-hashes`ONTAPで元のハッシュストアの場所からハッシュをフラッシュするかどうかを指定するには、が必須パラメータです。パラメータには次の値を設定でき `-flush-hashes`ます。  を指定する **`true`**と、**ONTAP**は元の場所にあるハッシュを削除し、**BranchCache**対応クライアントが新しい要求を行うたびに新しい場所に新しいハッシュを作成します。 を指定した場合 `false`、ハッシュはフラッシュされません。 + この場合、ハッシュストアパスを元の場所に戻すことで、既存のハッシュをあとから再利用できます。
動作モードの変更	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share	all-shares	disable}` 動作モードを変更する場合は、次の点に注意してください。 **ONTAP**では、**SMB**セッションのセットアップ時に、**BranchCache**による共有のサポートが通知されます。 BranchCacheを有効にしたときにすでにセッションを確立していたクライアントは、キャッシュされたコンテンツをこの共有で使用するために、いったん切断してから再接続する必要があります。
サポートするBranchCacheバージョンの変更	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable	v2-enable	enable-all}`

2. コマンドを使用して、設定の変更を確認します `vserver cifs branchcache show`。

ONTAP SMB共有上の**BranchCache**構成に関する情報を表示する

Storage Virtual Machine （ SVM ）の BranchCache 設定に関する情報を表示できます。

この情報は、設定を検証する場合や、設定を変更する前に現在の設定を確認する場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する項目	入力するコマンド
すべての SVM の BranchCache 設定に関する概要情報	`vserver cifs branchcache show`
特定の SVM の設定に関する詳細情報	`vserver cifs branchcache show -vserver` *`vserver_name`*

例

次の例では、SVM vs1のBranchCache設定に関する情報を表示します。

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

ONTAP SMB BranchCacheサーバキーを変更する

BranchCacheサーバキーを変更するには、Storage Virtual Machine（SVM）でBranchCacheの設定を変更し、別のサーバキーを指定します。

タスクの内容

サーバキーを特定の値に設定すると、複数のサーバが同じファイルのBranchCacheデータを提供している場合に、クライアントが同じサーバキーを使用して任意のサーバのハッシュを使用できるようになります。

サーバキーを変更する場合は、ハッシュキャッシュもフラッシュする必要があります。ハッシュのフラッシュ後、BranchCache対応クライアントによって新しい要求が行われると、ONTAPによって新しいハッシュが作成されます。

手順

1. 次のコマンドを使用して、サーバキーを変更します。 `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   新しいサーバキーを設定する場合は、も指定して値をに設定する `true`必要があります `-flush-hashes`。

2. コマンドを使用して、BranchCacheの設定が正しいことを確認し `vserver cifs branchcache show`ます。

例

次の例では、SVM vs1でスペースを含む新しいサーバキーを設定し、ハッシュキャッシュをフラッシュします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

関連情報

ONTAPがBranchCacheハッシュを無効にする理由について学ぶ

指定された **ONTAP SMB** パスの **BranchCache** ハッシュを事前計算します。

単一のファイル、ディレクトリ、またはディレクトリ構造内のすべてのファイルについて、ハッシュを事前に計算するようにBranchCacheサービスを設定できます。これは、BranchCacheが有効な共有内のデータのハッシュをピーク以外の時間帯に計算する場合に役立ちます。

タスクの内容

ハッシュの統計を表示する前にデータサンプルを収集する場合は、コマンドとオプションの `statistics stop`コマンドを使用する必要があり `statistics start`ます。

- ハッシュを事前に計算するStorage Virtual Machine（SVM）とパスを指定する必要があります。
- また、ハッシュを再帰的に計算するかどうかも指定する必要があります。
- ハッシュを再帰的に計算する場合、BranchCacheサービスは指定されたパスの下のディレクトリツリー全体をトラバースし、対象となるオブジェクトごとにハッシュを計算します。

  詳細はこちら `statistics start`そして `statistics stop`の中で"ONTAPコマンド リファレンス" 。

手順

1. 必要に応じてハッシュを事前に計算します。

ハッシュを事前に計算する対象	入力するコマンド
単一のファイルまたはディレクトリ	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
ディレクトリ構造内のすべてのファイルに対して再帰的に実行	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. コマンドを使用して、ハッシュが計算されていることを確認し `statistics`ます。

   a. 目的のSVMインスタンス上のオブジェクトの統計を表示します `hashd。 statistics show -object hashd -instance vserver_name`

   b. コマンドを繰り返し実行して、作成済みのハッシュの数が増加していることを確認します。

   の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

例

次の例では、パスおよびSVM vs1に格納されているすべてのファイルとサブディレクトリを対象にハッシュを作成します `/data`。

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

関連情報

- "パフォーマンス監視のセットアップ"

ONTAP SMB SVM BranchCacheハッシュストアからハッシュをフラッシュする

Storage Virtual Machine （ SVM ）上の BranchCache ハッシュストアから、キャッシュされたハッシュをすべてフラッシュできます。これは、ブランチオフィスの BranchCache の設定を変更した場合に役立ちます。たとえば、最近キャッシュモードを分散キャッシュからホスト型キャッシュモードに再設定した場合は、ハッシュストアをフラッシュする必要があります。

タスクの内容

ハッシュのフラッシュ後、BranchCache対応クライアントによって新しい要求が行われると、ONTAPによって新しいハッシュが作成されます。

ステップ

1. BranchCacheハッシュストアからハッシュをフラッシュします。 `vserver cifs branchcache hash-flush -vserver vserver_name`

```
vserver cifs branchcache hash-flush -vserver vs1
```

ONTAP SMB BranchCache統計を表示する

BranchCache統計を表示すると、キャッシュが適切に実行されているかどうか、キャッシュされたコンテンツをクライアントに提供しているかどうか、新しいハッシュデータ用のスペースを確保するためにハッシュファイルが削除されたかどうかなどの情報を確認できます。

タスクの内容

`hashd`statisticオブジェクトには、BranchCacheハッシュに関する統計情報を提供するカウンタが含まれます。 `cifs`statisticオブジェクトには、BranchCache関連のアクティビティに関する統計情報を提供するカウンタが含まれます。これらのオブジェクトに関する情報は、advanced権限レベルで収集および表示できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. コマンドを使用して、BranchCache関連のカウンタを表示します `statistics catalog counter show`。

```
cluster1::*> statistics catalog counter show -object hashd
```

```
Object: hashd
    Counter                       Description
    ---------------------------
-------------------------------------------
    branchcache_hash_created      Number of times a request to generate
                                  BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                  Number of times a BranchCache hash file
was
                                  deleted to make room for more recent
hash
                                  data. This happens if the hash store
size is
                                  exceeded.
    branchcache_hash_rejected     Number of times a request to generate
                                  BranchCache hash data failed.
    branchcache_hash_store_bytes
                                  Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                  data for the Vserver.
    instance_name                 Instance Name
    instance_uuid                 Instance UUID
    node_name                     System node name
    node_uuid                     System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                       Description
    ---------------------------
-------------------------------------------
    active_searches               Number of active searches over SMB and
SMB2
    auth_reject_too_many          Authentication refused after too many
                                  requests were made in rapid succession
    avg_directory_depth           Average number of directories crossed by
SMB
                                  and SMB2 path-based commands
    avg_junction_depth            Average number of junctions crossed by
SMB
                                  and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
```

```
hash
                                   data failed. These are failures when
                                   attempting to read existing hash data.
It
                                   does not include attempts to fetch hash
data
                                   that has not yet been generated.
    branchcache_hash_fetch_ok      Total number of times a request to fetch
hash
                                   data succeeded.
    branchcache_hash_sent_bytes    Total number of bytes sent to clients
                                   requesting hashes.
    branchcache_missing_hash_bytes
                                   Total number of bytes of data that had
to be
                                   read by the client because the hash for
that
                                   content was not available on the server.
   ....Output truncated....
```

の詳細については `statistics catalog counter show`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドと `statistics stop`コマンドを使用して、BranchCache関連の統計を収集し `statistics start`ます。

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

詳細はこちら `statistics start`そして `statistics stop`の中で"ONTAPコマンド リファレンス" 。

4. コマンドを使用して、収集したBranchCache統計を表示します `statistics show`。

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

5. admin権限レベルに戻ります。 `set -privilege admin`

```
cluster1::*> set -privilege admin
```

関連情報

- 統計情報を表示
- "パフォーマンス監視のセットアップ"
- "statistics start"
- "statistics stop"

ONTAP SMBのBranchCacheグループポリシーオブジェクトサポートについて学ぶ

ONTAP BranchCacheでは、BranchCacheのグループポリシーオブジェクト（GPO）をサポートしており、特定のBranchCacheの設定パラメータを一元管理できます。BranchCacheには、BranchCacheのハッシュの発行GPOとBranchCacheのハッシュバージョンサポートGPOの2つのGPOが使用されます。

- * BranchCache のハッシュの発行 GPO *

  BranchCacheのハッシュの発行GPOは、パラメータに対応し `-operating-mode`ます。GPOが更新されると、グループポリシーが適用される組織単位（OU）に含まれるStorage Virtual Machine（SVM）オブジェクトにこの値が適用されます。

- * BranchCache のハッシュバージョンサポート *

  BranchCacheのハッシュバージョンサポートGPOは、パラメータに対応し `-versions`ます。GPOが更新されると、グループポリシーが適用される組織単位に含まれるSVMオブジェクトにこの値が適用されます。

関連情報

SMBサーバーにグループポリシーオブジェクトを適用する方法について学習します

ONTAP SMB BranchCacheグループポリシーオブジェクトに関する情報を表示する

CIFSサーバのグループポリシーオブジェクト（GPO）の設定に関する情報を表示して、CIFSサーバが属しているドメインに対してBranchCache GPOが定義されているかどうか、定義されている場合は許可されている設定を確認できます。また、BranchCache GPO設定がCIFSサーバに適用されているかどうかを確認することもできます。

タスクの内容

CIFSサーバが属しているドメイン内でGPO設定が定義されていても、CIFS対応のStorage Virtual Machine（SVM）が含まれるOrganizational Unit（OU；組織単位）に適用されているとは限りません。適用されるGPO設定は、CIFS対応のSVMに適用されているすべての定義済みGPOの一部です。GPOを使用して適用されたBranchCache設定は、CLIを使用した設定よりも優先されます。

手順

1. コマンドを使用して、Active Directoryドメインに対して定義されているBranchCache GPO設定を表示します `vserver cifs group-policy show-defined`。

   この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. コマンドを使用して、CIFSサーバに適用されているBranchCache GPO設定を表示します `vserver cifs group-policy show-applied`。``

> この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

関連情報

- サーバー上の GPO サポートを有効または無効にする
- "vserver cifs group-policy show-defined"
- "vserver cifs group-policy show-applied"

SMB共有でのBranchCacheの無効化

ONTAP SMB共有でBranchCacheを無効にする方法について

特定のSMB共有でBranchCacheキャッシュサービスを提供せずに、あとからそれらの共有でキャッシュサービスを提供する場合は、BranchCacheを共有ごとに無効にすることができます。すべての共有でキャッシュを提供するようにBranchCacheを設定していて、一時的にすべてのキャッシュサービスを無効にする場合は、BranchCache設定を変更してすべての共有で自動キャッシュを停止できます。

SMB共有で有効になっていたBranchCacheをあとから無効にすると、ONTAPによる要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ（ Storage Virtual Machine （ SVM ）上の CIFS サーバ）から直接データを取得します。

関連情報

BranchCache 対応共有の構成について学習します

単一の **ONTAP SMB** 共有で **BranchCache** を無効にする

キャッシュコンテンツを使用できるようにしていた特定の共有でキャッシュサービスを提供する必要がなくなった場合は、既存の SMB 共有で BranchCache を無効にすることができます。

ステップ

1. 次のコマンドを入力します。 `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   BranchCache 共有プロパティが削除されます。適用されているその他の共有プロパティは有効なままです。

例

次のコマンドは、「 `d ata2` 」という名前の既存の SMB 共有で BranchCache を無効にします。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

すべての **ONTAP SMB** 共有の自動キャッシュを停止します

Storage Virtual Machine（SVM）のすべてのSMB共有に対してBranchCacheキャッシュを自動的に有効にするように設定している場合、BranchCacheの設定を変更して、すべてのSMB共有に対するコンテンツの自動キャッシュを停止することができます。

タスクの内容

すべての SMB 共有に対する自動キャッシュを停止するには、 BranchCache の動作モードを共有ごとのキャッシュに変更します。

手順

1. すべてのSMB共有で自動キャッシュを停止するようにBranchCacheを設定します。 `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドを実行すると、Storage Virtual Machine（SVM、旧Vserver）vs1のBranchCache設定が変更され、すべてのSMB共有に対する自動キャッシュが停止します。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

SVMで**BranchCache**を無効または有効にする

ONTAP SMBサーバーで**BranchCache**を無効または再度有効にすると何が起こるかを学びます

BranchCache を設定したあとに、ブランチオフィスのクライアントがキャッシュされたコンテンツを使用できないようにするには、 CIFS サーバでキャッシュを無効にします。BranchCache を無効にするときは、それを実行した場合の動作について理解しておく必要があります

BranchCache を無効にすると、 ONTAP によるハッシュの計算や要求元クライアントへのメタデータの送信が行われなくなります。ただし、ファイルアクセスは中断されません。以降に、 BranchCache 対応クライアント ONTAP からアクセスするコンテンツのメタデータ情報を要求すると、 Microsoft のエラーが返されます。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、CIFSサーバからStorage Virtual Machine（SVM）に格納されている実際のコンテンツが送信されます。

CIFS サーバで BranchCache を無効にしたあとは、 SMB 共有で BranchCache の機能がアドバタイズされなくなります。新しい SMB 接続でデータにアクセスするには、通常の SMB 読み取り要求を行います。

BranchCache は、 CIFS サーバでいつでも再度有効にすることができます。

- BranchCache ONTAP を無効にしてもハッシュストアは削除されないため、要求されたハッシュがまだ有効であれば、 BranchCache を再度有効にしたあとに、格納されたハッシュを使用してハッシュの要求に応答することができます。
- BranchCache 対応の共有に対する SMB 接続を確立したクライアントで接続を確立したときに BranchCache が無効になっていたクライアントの場合には、以降に BranchCache を再度有効にしても、BranchCache のサポートは有効になりません。

  これは、 SMB セッションのセットアップ時に共有に対する BranchCache のサポートが通知されるから ONTAP です。BranchCache を無効にしたときに BranchCache 対応の共有に対するセッションを確立していた場合、その共有のキャッシュされたコンテンツを使用するには、いったん切断してから再接続する必要があります。

CIFS サーバで BranchCache を無効にしたあとにハッシュストアを保存しておく必要がない場合は、手動で削除することができます。BranchCache を再度有効にするときは、ハッシュストアのディレクトリが存在することを確認する必要があります。BranchCache を再度有効にすると、 BranchCache 対応の共有で BranchCache の機能がアドバタイズされるようになります。BranchCache 対応クライアントから新しい要求が行われると、 ONTAP によって新しいハッシュが作成されます。

ONTAP SMB共有で**BranchCache**を無効または有効にする

Storage Virtual Machine（SVM）でBranchCacheを無効にするには、BranchCacheの動作モードをに変更します。`disabled`BranchCache サービスを共有単位で提供するか、すべての共有で自動的に提供するように動作モードを変更すると、いつでも BranchCache を有効にすることができます。

手順

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCacheを無効にする	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
共有ごとに BranchCache を有効にします	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
すべての共有で BranchCache を有効にします	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. BranchCacheの動作モードが目的の設定になっていることを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次の例では、SVM vs1でBranchCacheを無効にします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

SVMのBranchCache設定を削除する

ONTAP SMB共有上のBranchCache構成を削除すると何が起こるかを学びます

BranchCache を設定したあとに、 Storage Virtual Machine （ SVM ）からのキャッシュされたコンテンツの提供を中止する場合は、 CIFS サーバで BranchCache 設定を削除します。設定を削除するときは、それを実行した場合の動作について理解しておく必要があります。

設定を削除すると、 ONTAP によってその SVM の設定情報がクラスタから削除され、 BranchCache サービスが停止します。SVM のハッシュストアについては、 ONTAP で削除するかどうかを選択することができます。

BranchCache 設定を削除しても、 BranchCache 対応クライアントによるアクセスは中断されません。以降に、 BranchCache 対応クライアントから既存の SMB 接続でキャッシュ済みのコンテンツのメタデータ情報を要求すると、 ONTAP は Microsoft のエラーを返します。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、 CIFS サーバから SVM に格納されている実際のコンテンツが送信されます

BranchCache 設定を削除すると、 SMB 共有で BranchCache の機能がアドバタイズされなくなります。キャッシュされていないコンテンツに新しい SMB 接続でアクセスするには、通常の SMB 読み取り要求を行います。

ONTAP SMB共有上のBranchCache構成を削除します

Storage Virtual Machine（SVM）でBranchCacheサービスの削除に使用するコマンドは、既存のハッシュを削除するか保持するかによって異なります。

ステップ

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCache設定を削除して既存のハッシュを削除する	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
BranchCache設定を削除しますが、既存のハッシュは保持します	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

例

次の例は、SVM vs1でBranchCache設定を削除し、既存のハッシュをすべて削除します。

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

ONTAP SMB BranchCacheをリバートするとどうなるかを知る

ONTAPをBranchCacheがサポートされないリリースにリバートする場合の動作について理解しておくことが重要です。

- ONTAPをBranchCacheがサポートされないバージョンにリバートすると、BranchCache対応クライアントに対してSMB共有でBranchCacheの機能がアドバタイズされなくなります。そのため、クライアントからハッシュ情報が要求されることはありません。

  代わりに、通常のSMB読み取り要求を使用して実際のコンテンツを要求します。これに対する応答として、SMBサーバからStorage Virtual Machine（SVM）に格納されている実際のコンテンツが送信されます。

- ハッシュストアをホストするノードをBranchCacheがサポートされないリリースにリバートする場合、リバート時に出力されるコマンドを使用して、ストレージ管理者がBranchCacheの設定を手動でリバートする必要があります。

  このコマンドは、BranchCacheの設定とハッシュを削除します。

  リバートの完了後、必要に応じて、ハッシュストアが格納されていたディレクトリを手動で削除できます。

関連情報

共有上のBranchCache構成を削除する

Microsoftリモートコピーのパフォーマンスを向上

ONTAP SMB サーバーにおける **Microsoft** リモート コピーのパフォーマンス向上について学習します。

Microsoft Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _ コピーオフロード _ とも呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やスト

レージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。ソースとデスティネーションにはCIFSサーバまたはLUNのどちらかを指定できます。

ODX以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションに転送します。要約すると、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODXファイル転送では、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現されるパフォーマンス上のメリットには、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用率（CPU、メモリ）の削減、ネットワークI/O帯域幅の使用量の削減などがあります。

SMB環境では、この機能は、クライアントとストレージサーバの両方でSMB 3.0およびODX機能がサポートされている場合にのみ使用できます。SAN環境では、この機能は、クライアントとストレージサーバの両方でODX機能がサポートされている場合にのみ使用できます。ODXをサポートしていてODXが有効になっているクライアントコンピュータでは、ファイルの移動またはコピー時にオフロードされたファイル転送が自動的かつ透過的に使用されます。ODXは、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

関連情報

- 自動ロケーションによる自動ノード紹介の提供によりクライアント応答時間を改善する方法について学習します。
- "Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"

ONTAP SMBサーバー上の**ODX**について学ぶ

ODX コピーオフロードでは、トークンベースのメカニズムを使用して、 ODX 対応の CIFS サーバ内または CIFS サーバ間でデータの読み取りおよび書き込みを行います。CIFS サーバは、ホストを介してデータをルーティングするのではなく、データを表す小さなトークンをクライアントに送信します。ODX クライアントがそのトークンをデスティネーションサーバに提示すると、サーバはそのトークンで表されるデータをソースからデスティネーションに転送できます。

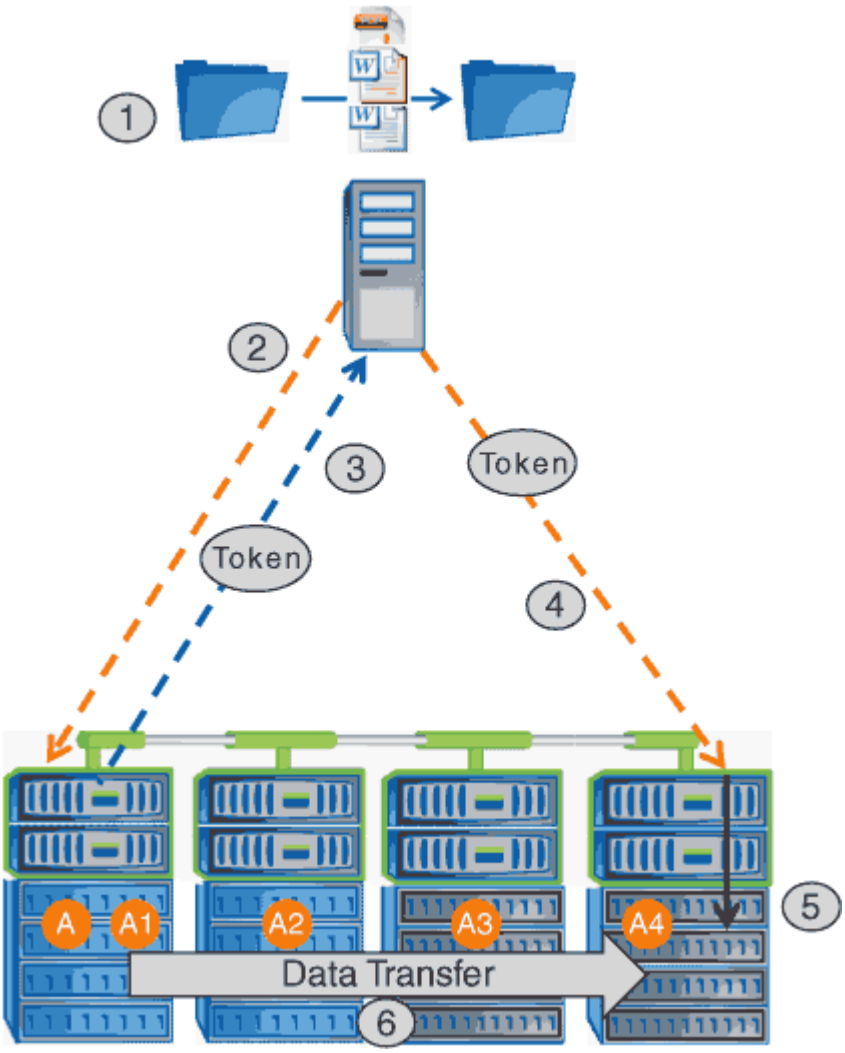
ODX クライアントは、 CIFS サーバが ODX 対応であると認識すると、ソースファイルを開いて CIFS サーバのトークンを要求します。デスティネーションファイルを開いたあと、クライアントはトークンを使用して、データをソースからデスティネーションに直接コピーするようにサーバに指示します。

ソースとデスティネーションは、コピー処理の範囲に応じて、同じ Storage Virtual Machine （ SVM ）上に存在する場合も異なる SVM 上に存在する場合もあります。

トークンは、データのポイントインタイム表現として機能します。たとえば、ストレージ間でデータをコピーする場合、データセグメントを表すトークンが要求元クライアントに返され、そのトークンをクライアントがデスティネーションにコピーするため、クライアントを介して基盤となるデータをコピーする必要がありません。

ONTAP では、 8MB のデータを表すトークンがサポートされます。8MB を超える ODX コピーは、 8MB のデータを表すトークンを複数使用して実行されます。

次の図で、 ODX コピー処理に関連する手順について説明します。



1. エクスプローラを使用するか、コマンドラインインターフェイスを使用するか、仮想マシンの移行の一環として、ユーザがファイルをコピーまたは移動します。または、アプリケーションによってファイルのコピーまたは移動が開始されます。
2. ODX 対応のクライアントが、この転送要求を ODX 要求に自動的に変換します。

   CIFS サーバに送信される ODX 要求には、トークン要求が含まれています。
3. CIFS サーバで ODX が有効になっていて、接続が SMB 3.0 経由の場合は、ソースのデータを論理的に表したものであるトークンが CIFS サーバによって生成されます。
4. クライアントは、データを表すトークンを受信し、書き込み要求を使用してそのトークンをデスティネーション CIFS サーバに送信します。

   ネットワーク経由でソースからクライアントにコピーされ、クライアントからデスティネーションにコピーされるのは、このデータだけです。
5. トークンがストレージサブシステムに送信されます。
6. コピーまたは移動が SVM によって内部的に実行されます。

   コピーまたは移動されるファイルが 8MB より大きい場合、コピーを実行するには複数のトークンが必要

になります。コピーが完了するまで、必要に応じて手順 2~6 を実行します。

ODX オフロードコピーで障害が発生した場合、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。同様に、デスティネーション CIFS サーバで ODX がサポートされていない場合、または ODX が無効になっている場合は、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。

ONTAP SMBサーバーで**ODX**を使用するための要件

Storage Virtual Machine（SVM）でODXによるコピーオフロードを使用する前に、一定の要件について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAPリリースでは、ODXによるコピーオフロードがサポートされます。

SMBのバージョンの要件

- ONTAPでは、SMB 3.0以降でODXがサポートされます。
- ODXを有効にする前に、CIFSサーバでSMB 3.0を有効にしておく必要があります。
  - ODX を有効にすると、 SMB 3.0 も有効になります（まだ有効になっていない場合）。
  - SMB 3.0を無効にするとODXも無効になります。

Windowsサーバとクライアントの要件

ODXによるコピーオフロードを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。

"NetAppのInteroperability Matrix"サポートされるWindowsクライアントの最新情報については、を参照してください。

ボリュームの要件

- ソースボリュームは1.25GB以上である必要があります。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは8Kのみです。

  二次圧縮形式はサポートされません。

ONTAP SMBサーバーで**ODX**を使用するためのガイドライン

コピーオフロードにODXを使用する前に、次のガイドラインを確認しておく必要があります。たとえば、ODXを使用できるボリュームのタイプや、クラスタ内およびクラスタ間のODXに関する考慮事項について理解しておく必要があります。

ボリュームに関するガイドライン

- 次のボリューム構成では、ODXをコピーオフロードに使用できません。
  - ソースボリュームサイズが 1.25GB 未満である必要があります

    ODXを使用するには、ボリュームサイズが1.25GB以上である必要があります。

  - 読み取り専用ボリューム

    負荷共有ミラー、SnapMirrorまたはSnapVaultデスティネーションボリュームにあるファイルやフォルダにはODXを使用できません。

  - ソースボリュームが重複排除されていない場合
- ODXコピーはクラスタ内のコピーでのみサポートされます。

  ODXを使用して、ファイルやフォルダを別のクラスタ内のボリュームにコピーすることはできません。

その他のガイドライン

- SMB環境でコピーオフロードにODXを使用するには、256KB以上のファイルである必要があります。

  サイズが小さいファイルは、従来のコピー処理を使用して転送されます。

- ODXコピーオフロードでは、コピープロセスの一部として重複排除が使用されます。

  データのコピーまたは移動時にSVMのボリュームで重複排除が発生しないようにするには、そのSVMでODXコピーオフロードを無効にする必要があります。

- データ転送を実行するアプリケーションは、ODXをサポートするように記述する必要があります。

  ODXをサポートするアプリケーションの処理は次のとおりです。

  - 仮想ハードディスク（VHD）の作成と変換、スナップショットの管理、仮想マシン間でのファイルのコピーなど、Hyper-Vの管理操作
  - エクスプローラでの操作
  - Windows PowerShell の copy コマンド
  - Windows コマンドプロンプトの copy コマンド

    WindowsコマンドプロンプトのRobocopyはODXをサポートしています。

    > ODXをサポートするWindowsサーバまたはクライアントでアプリケーションが実行されている必要があります。

  +
  Windowsサーバおよびクライアントでサポートされる ODXアプリケーションの詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

ONTAP SMBサーバー上の**ODX**のユースケース

SVMでODXを使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODXをサポートするWindowsサーバおよびクライアントでは、リモートサーバ間でデータをコピーするデフォルトの方法として、コピーオフロードが使用されます。Windowsサーバまたはクライアントで ODXがサポートされていない場合や、ODXコピーオフロードがいずれかの時点で失敗した場合、コピー処理または移動処理は、その処理の従来の読み取りと書き込みにフォールバックされます。

ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとSVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- クラスタ間

  ソースLUNとデスティネーションLUNは、クラスタの異なるノードにある異なるボリュームにあります。これはSANでのみサポートされ、CIFSでは機能しません。

その他にも、次のような特殊なユースケースがあります。

- ONTAP ODXの実装では、ODXを使用して、SMB共有とFCまたはiSCSIで接続された仮想ドライブの間でファイルをコピーできます。

  Windowsエクスプローラ、Windows CLI（PowerShell）、Hyper-V、またはODXをサポートするその他のアプリケーションでODXコピーオフロードを使用すると、SMB共有と接続されたLUNが同じクラスタにある場合に、それらの間でシームレスにファイルをコピーまたは移動できます。

- Hyper-Vでは、その他にもODXコピーオフロードのユースケースがいくつか用意されています。
  - Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク（VHD）ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

    これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。
  - 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。

> Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

ONTAP SMBサーバーで**ODX**を有効または無効にする

Storage Virtual Machine（SVM）でODXを有効または無効にすることができます。デフォルトでは、SMB 3.0が有効になっている場合、ODXコピーオフロードのサポートが有効になります。

開始する前に

SMB 3.0が有効になっている必要があります。

タスクの内容

SMB 3.0を無効にすると、ONTAPではSMB ODXも無効になります。SMB 3.0を再度有効にする場合は、SMB ODXを手動で再度有効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ODX コピーオフロードの設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例は、SVM vs1でODXコピーオフロードを有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

関連情報

利用可能なサーバーオプション

Auto Locationを使用したSMB自動ノードリファーラルによるクライアントの応答時間の短縮

Auto Location による **ONTAP SMB** 自動ノード リファーラルの提供によるクライアント応答時間の改善について学習します。

Auto Locationは、SMB自動ノードリファーラルを使用して、Storage Virtual Machine（SVM）でのSMBクライアントのパフォーマンスを向上させます。自動ノードリファーラルは、要求しているクライアントを、データが存在するボリュームをホストしているノードSVM上のLIFに自動的にリダイレクトします。これにより、クライアントの応答時間を短縮できます。

SMBクライアントがSVM上でホストされているSMB共有に接続するときに、要求されたデータを所有していないノード上のLIFを使用して接続することがあります。クライアントの接続先のノードは、クラスタネットワークを使用して別のノードが所有するデータにアクセスします。SMB接続で要求されたデータを含むノード上のLIFを使用している場合、クライアントへの応答時間が短縮されます。

- ONTAPでは、MicrosoftのDFSリファーラルを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることをSMBクライアントに通知することで、この機能を実現します。

  ノードがリファーラルを作成するのは、データを含むノード上にSVMのLIFがあることを特定した場合です。

- 自動ノードリファーラルは、IPv4とIPv6のLIFのIPアドレスでサポートされます。
- リファーラルは、クライアントの接続に使用する共有のルートの場所に基づいて作成されます。
- リファーラルはSMBネゴシエーション中に発生します。

  リファーラルは、接続が確立される前に作成されます。ONTAPがターゲット ノードに参照先のSMBクライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先LIFパスを介してデータにアクセスします。これにより、クライアントにはより高速なデータ アクセスが提供され、クラスタの余分な通信も回避されます。

共有が複数のジャンクションポイントにまたがっていて、ジャンクションの一部が他のノードに格納されているボリュームである場合、共有内のデータは複数のノードに分散されます。ONTAPは共有のルートに対してローカルなリファーラルを提供するため、ONTAPはクラスタネットワークを使用してこれらのローカルでないボリュームに格納されたデータを取得する必要があります。このタイプのネームスペースアーキテクチャでは、自動ノードリファーラルによってパフォーマンスが大幅に向上しない場合があります。

データをホストするノードに使用可能なLIFがない場合、ONTAPは、クライアントが選択したLIFを使用して接続を確立します。SMBクライアントによってファイルが開かれると、クライアントは参照された同じ接続を介してファイルに引き続きアクセスします。

何らかの理由でCIFSサーバがリファーラルを作成できない場合でも、SMBサービスは中断されません。自動ノードリファーラルが有効になっていない場合と同様に、SMB接続が確立されます。

関連情報

Microsoftリモートコピーのパフォーマンスの向上

ONTAP SMBサーバで自動ノードリファーラルを使用するための要件とガイドライン

SMB 自動ノードリファーラル（別名 _autolocation _ ）を使用する前に、この機能をサポートする ONTAP のバージョンなど、一定の要件について理解しておく必要があります。また、サポートされるSMBプロトコルのバージョンやその他の特別なガイドラインについても確認しておく必要があります。

ONTAPのバージョンとライセンスの要件

- クラスタ内のすべてのノードで、自動ノードリファーラルがサポートされているバージョンのONTAPが実行されている必要があります。
- オートロケーションを使用するには、SMB共有でワイドリンクが有効になっている必要があります。
- CIFSのライセンスが有効になっていて、SVMにSMBサーバが配置されている必要があります。SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMBプロトコルのバージョン

- SVMについては、すべてのバージョンのSMBで自動ノード リファーラルがサポートされます。

SMBクライアントの要件

SMB自動ノード リファーラルは、ONTAPでサポートされるすべてのMicrosoftクライアントでサポートされます。

ONTAPでサポートされるWindowsクライアントの最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

データ**LIF**の要件

データLIFをSMBクライアントのリファーラルとして使用する可能性がある場合は、NFSとCIFSの両方を有効にしたデータLIFを作成する必要があります。

自動ノードリファーラルは、ターゲットノードのデータLIFでNFSプロトコルまたはSMBプロトコルのみが有効になっている場合は機能しないことがあります。

この要件が満たされていない場合でも、データアクセスには影響しません。SMBクライアントは、SVMへの接続に使用した元のLIFを使用して共有をマッピングします。

参照された**SMB**接続を確立する際の**NTLM**認証の要件

CIFSサーバが含まれているドメイン、および自動ノードリファーラルを使用するクライアントが含まれているドメインで、NTLM認証が許可されている必要があります。

リファーラルを作成する際には、SMBサーバからWindowsクライアントに参照先のIPアドレスが渡されます。IPアドレスを使用した接続ではNTLM認証が使用されるため、参照された接続ではKerberos認証は実行されません。

これは、WindowsクライアントがKerberosで使用されるサービスプリンシパル名（および `service/FQDN` の形式）を作成できず、クライアントがサービスに`Kerberos`チケットを要求できないためです `service/NetBIOS name`。

自動ノードリファーラルでホームディレクトリ機能を使用する場合のガイドライン

ホームディレクトリ共有プロパティを有効にして共有を設定すると、ホームディレクトリ設定用に1つ以上のホームディレクトリ検索パスを設定できます。この検索パスで、SVMのボリュームを含む各ノードに格納されているボリュームを指定できます。クライアントはリファーラルを受け取り、使用可能なアクティブなローカルデータLIFがある場合は、ホームユーザのホームディレクトリに対してローカルな参照されたLIFを介して接続します。

SMB 1.0クライアントで自動ノードリファーラルを有効にして動的ホームディレクトリにアクセスする場合は注意が必要です。SMB 1.0クライアントでは、認証を行う前、つまりSMBサーバでユーザの名前が指定されていない前に自動ノードリファーラルが必要になるためです。ただし、次の条件に該当する場合、SMB 1.0クライアントでSMBホームディレクトリへのアクセスは正しく機能します。

- SMB ホームディレクトリは、「 %w 」（ Windows ユーザ名）または「 %u 」（マッピングされた UNIX ユーザ名）のような単純な名前を使用するように設定されており、「 %d\%w 」（ドメイン名 \ ユーザ名 ）のようなドメイン名形式の名前では使用されません。
- ホーム・ディレクトリ共有を作成するときに、 CIFS ホーム・ディレクトリ共有名は変数（「 %w 」または「 %u 」）で設定され、「 home 」などの静的な名前では設定されません。

SMB 2.xクライアントとSMB 3.0クライアントの場合、自動ノードリファーラルを使用してホームディレクトリにアクセスする際に特別なガイドラインはありません。

参照接続が確立されている**CIFS**サーバで自動ノードリファーラルを無効にする場合のガイドライン

オプションを有効にしたあとに自動ノードリファーラルを無効にした場合、参照LIFに現在接続されているクライアントでは参照接続が維持されます。ONTAPではSMB自動ノードリファーラルのメカニズムとしてDFSリファーラルを使用するため、オプションを無効にしたあとも、参照接続用にクライアントにキャッシュされているDFSリファーラルがタイムアウトするまでは参照LIFに再接続できます。これは、自動ノードリファー

ラルがサポートされないバージョンのONTAPにリバートした場合も同様です。クライアントは、DFSリファーラルがクライアントのキャッシュからタイムアウトするまで、リファーラルを使用し続けます。

オートロケーションでは、SMB自動ノードリファーラルを使用して、SVMのデータボリュームを所有するノード上のLIFをクライアントに参照させることで、SMBクライアントのパフォーマンスを向上させます。SMBクライアントがSVM上でホストされているSMB共有に接続するときに、要求されたデータを所有しておらず、クラスタインターコネクトネットワークを使用してデータを取得しているノード上のLIFを使用して接続することがあります。SMB接続で要求されたデータを含むノード上のLIFを使用している場合、クライアントへの応答時間が短縮されます。

ONTAPでは、Microsoftの分散ファイルシステム（DFS）リファーラルを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることをSMBクライアントに通知することで、この機能を実現します。ノードがリファーラルを作成するのは、データを含むノード上にSVMのLIFがあることを特定した場合です。リファーラルは、クライアントの接続に使用する共有のルートの場所に基づいて作成されます。

リファーラルはSMBネゴシエーション中に発生します。リファーラルは、接続が確立される前に作成されます。ONTAPがターゲット ノードに参照先のSMBクライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先LIFパスを介してデータにアクセスします。これにより、クライアントにはより高速なデータ アクセスが提供され、クラスタの余分な通信も回避されます。

Mac OSクライアントで自動ノード リファーラルを使用する際のガイドライン

Mac OSはMicrosoftのDistributed File System（DFS;分散ファイルシステム）をサポートしていますが、Mac OS Xクライアントは**SMB**自動ノード リファーラルをサポートしていません。Windowsクライアントは、SMB共有に接続する前にDFSリファーラル要求を行います。ONTAPは、要求されたデータをホストしているノード上で見つかったデータLIFへのリファーラルを提供します。これによって、クライアントの応答時間が短縮されます。Mac OSでもDFSはサポートされますが、Mac OSクライアントの動作はWindowsクライアントとまったく同じではありません。

関連情報

- サーバー上で動的ホームディレクトリを有効にする方法について学習します
- "ネットワーク管理"
- "NetApp Interoperability Matrix Tool"

ONTAP SMB自動ノード紹介のサポート

SMB 自動ノードリファーラルを有効にする際に、 ONTAP の一部の機能ではリファーラルがサポートされない点に注意してください。

- SMB 自動ノードリファーラルは、次の種類のボリュームではサポートされません。
  - 負荷共有ミラーの読み取り専用のメンバー
  - データ保護ミラーのデスティネーションボリューム
- LIF が移動してもノードリファーラルは移動しません。

  クライアントが SMB 2.x または SMB 3.0 接続を介した参照接続を使用している場合、データ LIF が無停止で移動してもクライアントは引き続き同じ参照接続を使用します。 LIF がデータに対してローカルでなくなった場合も同様です。

- ボリュームが移動してもノードリファーラルは移動しません。

クライアントがいずれかの SMB 接続による参照接続を使用している場合、ボリュームが移動してもクライアントは引き続き同じ参照接続を使用します。ボリュームがデータ LIF と異なるノードに移動した場合も同様です。

ONTAP SMB自動ノード紹介を有効または無効にする

SMB自動ノードリファーラルを有効にすると、SMBクライアントアクセスのパフォーマンスを向上させることができます。ONTAPでSMBクライアントを参照しないようにするには、自動ノードリファーラルを無効にします。

開始する前に

Storage Virtual Machine（SVM）でCIFSサーバが設定されて実行されている必要があります。

タスクの内容

SMB自動ノードリファーラル機能は、デフォルトでは無効になっています。必要に応じて、各SVMでこの機能を有効または無効にすることができます。

このオプションは、advanced権限レベルで使用できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. SMB自動ノードリファーラルを必要に応じて有効または無効にします。

SMB 自動ノードリファーラルの設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

このオプションの設定は、新しいSMBセッションに対して有効になります。既存の接続を使用するクライアントは、既存のキャッシュがタイムアウトした場合にのみノードリファーラルを使用できます。

3. admin権限レベルに切り替えます。 `set -privilege admin`

関連情報

利用可能なサーバーオプション

統計を使用して **ONTAP SMB** 自動ノード リファーラル アクティビティを監視する

参照されるSMB接続の数を確認するには、コマンドを使用して自動ノードリファーラルのアクティビティを監視し `statistics`ます。リファーラルを監視することで、自動リファーラルによって共有をホストするノード上の接続が割り当てられている範囲や、CIFSサーバ上の共有へのローカルアクセスを強化するためにデータLIFを再配置する必要があるかどうかを判断できます。

タスクの内容

オブジェクトには `cifs`、SMB自動ノードリファーラルの監視に役立つadvanced権限レベルのカウンタがいくつか用意されています。

- `node_referral_issued`

  共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントのうち、共有のルートのノードへのリファーラルが発行されたクライアントの数。

- `node_referral_local`

  共有のルートと同じノードでホストされるLIFを使用して接続したクライアントの数。一般に、ローカルアクセスは最適なパフォーマンスを提供します。

- `node_referral_not_possible`

  共有のルートとは別のノードでホストされるLIFを使用して接続したあとに、共有のルートをホストするノードへのリファーラルが発行されていないクライアントの数。共有のルートのノードのアクティブなデータLIFが見つからなかったためです。

- `node_referral_remote`

  共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントの数。リモートアクセスを実行すると、パフォーマンスが低下する可能性があります。

一定期間内のデータ（サンプル）を収集して表示することで、Storage Virtual Machine（SVM）の自動ノードリファーラル統計を監視できます。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

コマンドで収集した情報を評価して使用するには `statistics`、環境内でクライアントがどのように分散しているかを理解しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. コマンドを使用して、自動ノードリファーラルの統計を表示します `statistics`。

   次に、サンプリングされた期間のデータを収集して表示することで、自動ノードリファーラルの統計を表示する例を示します。

   a. 収集を開始します。 `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. 目的の収集時間が経過するまで待ちます。

   c. 収集を停止します。 `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

詳細はこちら `statistics start`そして `statistics stop`の中で"ONTAPコマンド リファレンス" 。

d. 自動ノードリファーラルの統計を表示します。 `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

出力には、SVM vs1に含まれるすべてのノードのカウンタが表示されます。この例では、わかりやすくするために、自動ノードリファーラルの統計に関連する出力フィールドのみを示しています。

の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

3. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

- 統計情報を表示
- "パフォーマンス監視のセットアップ"

Windowsクライアントを使用してクライアント側の**ONTAP SMB**自動ノードリファーラル情報を監視します

クライアント側から発行されているリファーラルを確認するには、Windowsのユーティリティを使用し `dfsutil.exe`ます。

このユーティリティは、Windows 7以降のクライアントで使用できるRemote Server Administration Tools（RSAT）キットに含まれてい `dfsutil.exe`ます。このユーティリティを使用すると、リファーラルキャッシュの内容に関する情報を表示したり、クライアントが現在使用している各リファーラルに関する情報を表示したりできます。ユーティリティを使用して、クライアントのリファーラルキャッシュをクリアすることもできます。詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

アクセスベースの列挙による共有のフォルダのセキュリティを提供する

アクセスベースの列挙により共有上の **ONTAP SMB** フォルダ セキュリティを提供します

Access-Based Enumeration（ABE；アクセスベースの列挙）がSMB共有で有効になっている場合、共有内のフォルダまたはファイルに（個人またはグループの権限制限により）アクセスする権限がないユーザの環境には、共有自体は引き続き表示されますが、その共有リソースは表示されます。

従来の共有プロパティでは、共有内のファイルやフォルダの表示や変更を許可するユーザ（個人またはグループ）を指定できます。ただし、権限のないユーザに対して共有内のフォルダやファイルを表示可能とするかどうかを制御することはできません。この状態だと、共有内のこれらのフォルダ名またはファイル名に、顧客名や開発中の製品などの重要な情報が記述されている場合に問題になることがあります。

ABEでは、共有プロパティが拡張され、共有内のファイルやフォルダの列挙も対象になりました。このため、ABEを使用すると、ユーザのアクセス権に基づいて共有内のファイルやフォルダの表示をフィルタリングできます。つまり、共有自体はすべてのユーザに表示されますが、共有内のファイルやフォルダは指定したユーザに対して表示または非表示にすることができます。ABEを使用すると、職場の機密情報を保護するだけでなく、大規模なディレクトリ構造の表示を簡素化して、すべてのコンテンツにアクセスする必要がないユーザにメリットを提供できます。たとえば、共有自体はすべてのユーザに表示されますが、共有内のファイルやフォルダは表示または非表示にできます。

詳細はこちらをご覧ください "SMB / CIFSアクセスベースの列挙を使用する際のパフォーマンスへの影響"。

ONTAP SMB共有のアクセスベースの列挙を有効または無効にする

SMB共有でAccess-Based Enumeration（ABE；アクセスベースの列挙）を有効または無効にすると、ユーザにアクセス権限のない共有リソースが表示されることを許可または禁止できます。

タスクの内容

デフォルトでは、ABEは無効になっています。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
新しい共有でABEを有効にする	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration`SMB共有の作成時に、追加のオプションの共有設定および追加の共有プロパティを指定できます。の詳細については `vserver cifs share create`、を"ONTAPコマンド リファレンス"参照してください。
既存の共有でABEを有効にする	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`既存の共有プロパティは維持されます。ABE共有プロパティは既存の共有プロパティリストに追加されます。
既存の共有でABEを無効にする	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`その他の共有プロパティは維持されます。ABE共有プロパティのみが共有プロパティのリストから削除されます。

2. コマンドを使用して、共有設定が正しいことを確認し `vserver cifs share show`ます。

例

次の例は、SVM vs1上のパスで「sales」という名前のABE SMB共有を作成します `/sales`。共有は、共有プロパティとしてを使用して作成され `access-based-enumeration`ます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例は、「data2」という名前のSMB共有に共有プロパティを追加します `access-based-enumeration`。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ---------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

関連情報

[既存の共有の共有プロパティを追加または削除する]

ONTAP SMB共有上の**Windows**クライアントからのアクセスベースの列挙を有効または無効にする

SMB共有に対するAccess-Based Enumeration（ABE；アクセスベースの列挙）をWindowsクライアントから有効または無効にすることができます。これにより、CIFSサーバに接続することなく、この共有設定を行うことができます。

この `abecmd`ユーティリティは、Windows ServerおよびWindowsクライアントの新しいバージョンでは使用できません。Windows Server 2008の一部としてリリースされた。Windows Server 2008のサポートは2020年1月14日をもって終了しました。

手順

1. ABEをサポートするWindowsクライアントで、次のコマンドを入力します。 `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   コマンドの詳細については `abecmd`、Windowsクライアントのマニュアルを参照してください。

NFSトSMBノファイルオヨヒテイレクトリノメイメイキソク

ONTAP NFSおよび**SMB**のファイルとディレクトリの命名依存関係について学習します

ファイルとディレクトリの命名規則は、 ONTAP クラスタおよびクライアントの言語設定に加え、ネットワーククライアントのオペレーティングシステムとファイル共有プロトコルによって異なります。

オペレーティングシステムとファイル共有プロトコルによって、次の項目が決まります。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAPでは、ONTAPのリリースに応じて、ファイル、ディレクトリ、およびqtreeの名前でマルチバイト文字がサポートされます。

ONTAP SMBファイル名またはディレクトリ名に有効な文字について学習します

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、 UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン（ : ）を使用しないでください。コロンは、 MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限はオペレーティングシステムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティングシステムのマニュアルを参照してください。

マルチプロトコル環境における **ONTAP SMB** ファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。マルチプロトコル環境におけるこれらの影響と、SMB共有の作成時にパスを指定する場合や、共有内のデータにアクセスする場合に実行する必要がある対処方法を理解しておく必要があります。

SMBクライアントでという名前のディレクトリを作成すると、 `testdir`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `testdir`。ただし、SMBユーザがあとでディレクトリ名を作成しようとすると、SMBクライアントではその名前がすでに存在しているとみなされるため作成 `TESTDIR`できません。NFSユーザがあとでという名前のディレクトリを作成すると、 `TESTDIR`このディレクトリ名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ディレクトリ名の大文字と小文字が区別されるため、両方のディレクトリ名が作成したとおりにと `TESTDIR`表示されます（例：） `testdir`。
- SMBクライアントでは、2つのディレクトリを区別するために8.3形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TESTDI~1`表示され `testdir`ます。
  - ONTAPは、2つのディレクトリを区別するためにディレクトリ名を作成します `TESTDI~1`。

    この場合、Storage Virtual Machine（SVM）で共有を作成または変更するときに共有パスを指定するときは、8.3形式の名前を使用する必要があります。

ファイルについても同様に、SMBクライアントでを作成すると、 `test.txt`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `text.txt`。ただし、SMBユーザがあとでを作成しようとすると、 `Test.txt`SMBクライアントではその名前がすでに存在しているとみなされるため作成できません。NFSユーザがという名前のファイルをあとで作成すると、 `Test.txt`このファイル名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ファイル名の大文字と小文字が区別されるため、両方のファイル名が作成したとおりに、およびと `Test.txt`表示されます `test.txt`。
- SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。1つのファイルにはベースファイル名が付いています。追加のファイルには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TEST~1.TXT`表示され `test.txt`ます。
  - ONTAPは、2つのファイルを区別するためにファイル名を作成します `TEST~1.TXT`。

> Vserver cifs character-mappingコマンドを使用して文字マッピングを有効または変更した場合、通常は大文字と小文字が区別されないWindowsでの検索で大文字と小文字が区別されるようになります。

ONTAP SMBのファイル名とディレクトリ名の作成について学習します

ONTAP は、 SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2 つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、 ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（ ~ ）と 1~5 の数字が追加されます。

  同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成する `specifications.html`と、ONTAPでは

という8.3形式のファイル名が作成されます `specif~1.htm`。この名前がすでに存在する場合、 ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという別のファイルを作成すると `specifications_new.html`、の8.3形式は `specifications_new.html`になり `specif~2.htm`ます。

ONTAP SMBのマルチバイトファイル名、ディレクトリ名、および**qtree**名について学ぶ

ONTAP 9 .5以降では、4バイトのUTF-8エンコード名がサポートされているため、基本多言語面（BMP）以外のUnicode補助文字を含むファイル名、ディレクトリ名、ツリー名を作成および表示できます。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8エンコード名のサポートを有効にするために、コマンドファミリーと `volume`コマンドファミリーで新しい_utf8mb4_言語コードを使用でき `vserver`ます。

次のいずれかの方法で新しいボリュームを作成する必要があります。

- ボリューム・オプションを明示的に設定し `-language`ます。 `volume create -language utf8mb4 {…}`
- ボリュームオプションを指定して作成または変更されたSVMからボリュームオプションを継承し `-language`ます。 `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- ONTAP 9 .6以前では、utf8mb4をサポートするために既存のボリュームを変更することはできません。新しいutf8mb4対応ボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

  SVM は utf8mb4 をサポートするように更新できますが、既存のボリュームの言語コードは元の設定のままです。

  ONTAP 9 .7P1以降を使用している場合は、utf8mb4の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください "ONTAPでの作成後にボリュームの言語を変更できますか。"。

- ONTAP 9 .8以降では、パラメータを使用して、ボリュームの言語を*。utf-8からutf8mb4に変更でき `[-language <Language code>]`ます。ボリュームの言語を変更するには、に連絡します"NetAppのサポート"。

> 4バイトのUTF-8文字を使用するLUN名は現在サポートされていません。

- 通常、Unicode文字データは、Windowsファイルシステムアプリケーションでは16-bit Unicode Transformation Format（UTF-16）を使用し、NFSファイルシステムでは8-bit Unicode Transformation Format（UTF-8）を使用して表されます。

  ONTAP 9 .5より前のリリースでは、Windowsクライアントで作成されたUTF-16の補助文字を含む名前は他のWindowsクライアントには正しく表示されましたが、NFSクライアントではUTF-8に正しく変換されませんでした。同様に、NFSクライアントで作成されたUTF-8の補助文字を含む名前は、Windowsクライアントでは正しく変換されませんでした。

- ONTAP 9 .4以前を実行しているシステムで、有効または無効な補助文字を含むファイル名を作成すると、ONTAPはファイル名を拒否し、無効なファイル名エラーを返します。

  この問題を回避するには、ファイル名にBMP文字のみを使用して補助文字を使用しないようにする

か、ONTAP 9 .5以降にアップグレードしてください。

ONTAP 9以降では、Unicode文字をqtree名に使用できます。

- qtree名を設定または変更するには、コマンドファミリーまたはSystem Managerを使用し `volume qtree` ます。
- qtree名には、日本語や中国語などのUnicode形式のマルチバイト文字を含めることができます。
- ONTAP 9 .5より前のリリースでは、BMP文字（つまり、3バイトで表現できる文字）のみがサポートされていました。

> ONTAP 9 .5より前のリリースでは、qtreeの親ボリュームのジャンクションパスに、Unicode文字を使用したqtree名とディレクトリ名を含めることができます。 `volume show`親ボリュームの言語設定がUTF-8の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定がUTF-8のいずれかでない場合は、ジャンクションパスの一部が数値のNFS名に置き換えられて表示されます。

- 9.5以降のリリースでは、utf8mb4が有効なボリュームにqtreeが含まれていれば、qtree名で4バイト文字がサポートされます。

ボリューム上の **ONTAP SMB** ファイル名変換の文字マッピングを構成する

NFSクライアントは、SMBクライアントおよび特定のWindowsアプリケーションで無効な文字を含むファイル名を作成できます。ボリュームでのファイル名の変換のための文字マッピングを設定すると、本来は無効なNFS名を持つファイルにSMBクライアントからアクセスできるようになります。

タスクの内容

SMBクライアントがNFSクライアントによって作成されたファイルにアクセスすると、ONTAPはファイル名を確認します。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、 ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、重要な情報を長いファイル名にエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステム上のクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMBクライアントで有効でない文字を含むファイル名をNFSクライアントが作成する場合は、無効なNFS文字をSMBと特定のWindowsアプリケーションの両方で使用できるUnicode文字に変換するマップを定義できます。たとえば、この機能は、CATIA MCADおよびMathematicaアプリケーションだけでなく、この要件を持つ他のアプリケーションもサポートしています。

文字マッピングはボリューム単位で設定できます。

ボリュームに文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイント全体には適用されません。

  文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字または不正な文字を表すUnicode文字は、通常はファイル名に使用されない文字であることを確認する必要があります。使用されていないと、不要なマッピングが発生します。

たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用されていれば 'Windows クライアントが "a-b`" という名前のファイルにアクセスしようとすると ' その要求は NFS 名 "a:b`" にマップされます (望ましい結果ではありません)

- 文字マッピングを適用したあともマッピングに無効なWindows文字が含まれている場合、ONTAPはWindows 8.3ファイル名にフォールバックします。
- FPolicy通知、NAS監査ログ、およびセキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- DPタイプのSnapMirror関係が作成された場合、ソースボリュームの文字マッピングはデスティネーションDPボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされたWindows名はNFS名に変わるため、名前の検索はNFSのセマンティクスに従って行われます。これには、NFS検索では大文字と小文字が区別されることも含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windowsの大文字と小文字を区別しない動作に依存してはなりません。ただし8.3形式の名前は使用可能で、大文字と小文字は区別されません。
- 部分マッピングまたは無効なマッピング：名前をマッピングしてディレクトリ列挙（「dir」）を実行するクライアントに戻ったあと、生成されたUnicode名がWindowsで有効かどうかがチェックされます。その名前に無効な文字が含まれている場合、またはWindowsで無効な文字が含まれている場合（例：「.」または空白で終わる場合）は、無効な名前の代わりに8.3形式の名前が返されます。

ステップ

1. 文字マッピング「 + 」を設定します

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, …+
```

マッピングは、「 : 」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16進数を使用して入力されたUnicode文字です。例： 3C ： E03C+

コロンで区切られた各ペアの最初の値 `mapping_text`は、変換するNFS文字の16進値です。2番目の値は、SMBで使用されるUnicode値です。マッピングペアは一意である必要があります（1対1のマッピングが存在する必要があります）。

- ソースマッピング +

次の表に、ソースマッピングで許可されるUnicode文字セットを示します。

+

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C		バックスラッシュ
0x3A	：	コロン
0x2A	*	アスタリスク

Unicode 文字	印刷された文字	説明
0x3F	?	疑問符
0x22	"	引用符
0x3C	<	より小さい
0x3E	>	次の値より大きい
0x7C		
縦線	0xB1	±

- ターゲットマッピング

  ターゲット文字には、 U+E0000…U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、 Storage Virtual Machine （ SVM ） vs1 上の「 data 」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

関連情報

名前空間でのデータボリュームの作成と管理について学習します

SMB ファイル名変換の文字マッピングを管理するための **ONTAP** コマンド

文字マッピングを管理するには、FlexVolでSMBファイル名の変換に使用する情報を作成、変更、表示、または削除します。

状況	使用するコマンド
新しいファイル文字マッピングを作成する	`vserver cifs character-mapping create`
ファイル文字マッピングに関する情報を表示する	`vserver cifs character-mapping show`

状況	使用するコマンド
既存のファイル文字マッピングを変更する	`vserver cifs character-mapping modify`
ファイル文字マッピングを削除します。	`vserver cifs character-mapping delete`

の詳細については `vserver cifs character-mapping`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

ボリューム上のファイル名変換の文字マッピングを構成する

NASデータへのS3クライアントアクセスの提供

ONTAP S3 マルチプロトコルサポートについて学ぶ

ONTAP 9 12.1以降では、S3プロトコルを実行するクライアントが、NFSプロトコルとSMBプロトコルを使用するクライアントに提供されるデータと同じデータに再フォーマットすることなくアクセスできるようになりました。この機能により、NASデータを引き続きNASクライアントに提供しながら、S3アプリケーション（データマイニングや人工知能など）を実行するS3クライアントにオブジェクトデータを提供できます。

S3マルチプロトコル機能は次の2つのユースケースに対応します。

1. S3クライアントを使用した既存のNASデータへのアクセス

   既存のデータが従来の NAS クライアント (NFS または SMB) を使用して作成され、NAS ボリューム (FlexVolまたはFlexGroupボリューム) に配置されている場合は、S3 クライアント上の分析ツールを使用してこのデータにアクセスできます。

2. NASプロトコルとS3プロトコルの両方を使用してI/Oを実行できる、最新のクライアント向けのバックエンドストレージ

   NAS プロトコルと S3 プロトコルの両方を使用して同じデータを読み書きできる Spark や Kafka などのアプリケーションに統合アクセスを提供できます。

S3マルチプロトコルのサポートの仕組み

ONTAPマルチプロトコル サポートを使用すると、同じデータセットをファイル階層またはバケット内のオブジェクトとして提供できます。そのために、 ONTAP は「S3 NAS バケット」を作成し、S3 クライアントが S3 オブジェクト要求を使用して NAS ストレージ内のファイルを作成、読み取り、削除、列挙できるようにします。このマッピングはNASのセキュリティ設定に準拠しており、ファイルおよびディレクトリのアクセス権を監視し、必要に応じてセキュリティ監査証跡に書き込みます。

このマッピングは、指定されたNASディレクトリ階層をS3バケットとして提供することで実現されます。ディレクトリ階層内の各ファイルはS3オブジェクトとして表されます。S3オブジェクトの名前は、マッピングされたディレクトリから下への相対パスで、ディレクトリ境界はスラッシュ（/）で表されます。

ONTAPで定義されたS3ユーザは、NASディレクトリにマッピングされるバケット用に定義されたバケットポリシーに従って、このストレージにアクセスできます。これを実現するには、S3ユーザとSMB / NFSユーザの間にマッピングを定義する必要があります。SMB / NFSユーザのクレデンシャルはNAS権限のチェックに使用され、これらのアクセスから発生する監査レコードに含まれます。

SMBクライアントまたはNFSクライアントによって作成されたファイルは即座にディレクトリに配置されるため、クライアントからはデータが書き込まれる前に参照できます。S3クライアントは異なるセマンティクスを想定しており、すべてのデータが書き込まれるまで新しいオブジェクトはネームスペースに表示されません。S3からNASストレージへのこのマッピングでは、S3のセマンティクスを使用してファイルが作成され、S3の作成コマンドが完了するまでファイルが外部に表示されません。

S3 NASバケットのデータ保護

S3 NAS「バケット」は、単に S3 クライアントの NAS データのマッピングであり、標準の S3 バケットではありません。したがって、NetApp SnapMirror S3機能を使用してS3 NASバケットを保護する必要はありません。代わりに、SnapMirror非同期ボリューム レプリケーションを使用して、S3 NASバケットが含まれるボリュームを保護できます。SnapMirror同期とSVMディザスタ リカバリはサポートされていません。

ONTAP 9 .14.1以降では、MetroCluster IPおよびFC構成のミラーされたアグリゲートとミラーされていないアグリゲートでS3 NASバケットがサポートされます。

詳細はこちらをご覧ください "SnapMirror非同期"。

S3 NASバケットの監査

S3 NASバケットは従来のS3バケットではないため、バケットに対するアクセスを監査するようにS3監査を設定することはできません。詳細については、をご覧ください "S3の監査"。

ただし、S3 NASバケットにマッピングされたNASファイルとディレクトリのアクセスイベントは、従来のONTAP監査手順を使用して監査できます。そのため、S3処理でNASの監査イベントがトリガーされることがありますが、次の例外があります。

- S3クライアントアクセスがS3ポリシー設定（グループポリシーまたはバケットポリシー）で拒否された場合、イベントのNAS監査は開始されません。これは、SVMの監査チェックの前にS3権限がチェックされるためです。
- S3 GET要求のターゲットファイルのサイズが0の場合、GET要求には0のコンテンツが返され、読み取りアクセスはログに記録されません。
- S3 GET要求のターゲットファイルがユーザにトラバース権限がないフォルダにある場合は、アクセスの試行が失敗し、イベントはログに記録されません。

詳細はこちらをご覧ください "SVMでNASイベントを監査する"。

オブジェクトのマルチパートアップロード

ONTAP 9.16.1以降では、基盤となるFlexGroupボリュームでが有効になっている場合、S3 NASバケットでオブジェクトマルチパートアップロードがサポートされ"高度な容量分散"ます。

NASファイルストレージでのオブジェクトマルチパートアップロードを使用すると、S3プロトコルクライアントで大きなオブジェクトを小さなパートとしてアップロードできます。オブジェクトマルチパートアップロードには次の利点があります。

- オブジェクトを並行してアップロードできます。

- アップロードに失敗した場合や一時停止した場合は、まだアップロードされていないパーツのみをアップロードする必要があります。オブジェクト全体のアップロードを再開する必要はありません。
- オブジェクトのサイズが事前にわかっていない場合（大きなオブジェクトがまだ書き込まれている場合など）、クライアントはオブジェクトの一部のアップロードをただちに開始し、オブジェクト全体が作成されたあとにアップロードを完了できます。

> S3 NASバケット内のマルチパートオブジェクトは、1MB単位でアライメントする必要があります。たとえば、パーツは4MBまたは4GBなどのサイズにすることができます。部品では、4.5MBや4000.5MBなどのサブMBサイズは使用できません。

マルチパートアップロードでは、次のS3処理がサポートされます。

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject（ ONTAP 9.17.1以降）
- CreateMultipartUpload

  ONTAP 9.17.1 以降、CreateMultipartUpload はタグ付けとユーザー メタデータのキー/値ペアをサポートします。

- ListMultipartUpload
- パーツのアップロード

> パーツ番号による取得（「PartNumber=xx」）は、S3 NASバケットではサポートされていません。代わりに、完全なオブジェクトが返されます。

S3と**NAS**の相互運用性

ONTAP S3 NASバケットは、ここに記載されているものを除き、標準のNASおよびS3機能をサポートします。

NAS機能は現在、**S3 NAS**バケットではサポートされていません。

FabricPoolの大容量階層

S3 NASバケットをFabricPoolの大容量階層として設定することはできません。

S3の操作と機能は、現時点では**S3 NAS**バケットでサポートされていません。

アクション

- ByPassGovernanceRetention
- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersioning
- GetObjectRetention
- ListBucketVersioning

- ListObjectVersions
- PutBucketLifecycleConfiguration
- PutBucketVersioning
- PutObjectLockConfiguration
- PutObjectRetention

具体的には、S3 NASバケットでS3を使用する場合、これらのS3処理はサポートされません。ネイティブのS3バケットを使用している場合、次の処理が行われます。"ノーマルとしてサポート"

AWSユーザメタデータ

- ONTAP 9.17.1 以降、マルチパート オブジェクトを含むメタデータがサポートされます。
- ONTAP 9.16.1 以降、シングルアート オブジェクトを含むメタデータがサポートされます。
- ONTAP 9.15.1以前では、S3ユーザメタデータの一部として受信されたキーと値のペアは、オブジェクトデータと一緒にディスクに格納されません。
- ONTAP 9.15.1以前では、プレフィックスが「x-amz-meta」の要求ヘッダーは無視されます。

AWSタグ

- ONTAP 9.17.1 以降では、マルチパート オブジェクトを含むタグがサポートされます。
- ONTAP 9.16.1 以降では、シングルアート オブジェクトを含むタグがサポートされます。
- ONTAP 9.15.1以前のPUT object要求とマルチパートの開始要求では、プレフィックスが「x-amz-tagging」のヘッダーは無視されます。
- ONTAP 9.15.1以前では、既存のファイルのタグの更新要求（PUT、GET、およびDelete要求に？tagging query-stringを指定）がエラーで拒否されます。

バージョン管理

バケットのマッピング設定でバージョン管理を指定することはできません。

- null以外のバージョン指定（versionId=xyz query-string）を含む要求は、エラー応答を受信します。
- バケットのバージョン管理状態を変更する要求が拒否され、エラーが発生します。

ONTAP S3クライアントアクセスのNASデータ要件について学ぶ

S3アクセス用にNASファイルとディレクトリをマッピングする場合は、互換性の問題がいくつかあることを理解しておくことが重要です。S3 NASバケットを使用してサービスを提供する前に、NASファイル階層の調整が必要になる場合があります。

S3 NASバケットは、S3バケット構文を使用してそのディレクトリをマッピングすることでNASディレクトリへのS3アクセスを提供し、ディレクトリツリー内のファイルはオブジェクトとして表示されます。オブジェクト名は、S3バケット設定で指定されたディレクトリに対するファイルのパス名をスラッシュで区切って指定します。

このマッピングでは、S3 NASバケットを使用してファイルとディレクトリが提供される場合、いくつかの要件が課せられます。

- S3名は1024バイトに制限されているため、パス名が長いファイルにS3を使用してアクセスすることはできません。
- ファイル名とディレクトリ名は255文字に制限されているため、オブジェクト名の連続するスラッシュ以外の文字は255文字以下にする必要があります。
- s3では、バックスラッシュ（「\」）で区切られたSMBパス名は、代わりにスラッシュ（「/」）文字を含むオブジェクト名として表示されます。
- 有効なS3オブジェクト名でも、組み合わせによってはマッピングされたNASディレクトリ ツリーに共存できないものがあります。たとえば、有効な S3 オブジェクト名「part1/part2」と「part1/part2/part3」は、NAS ディレクトリ ツリーに同時に存在できないファイルにマップされます。「part1/part2」は最初の名前ではファイルであり、もう 1 つの名前ではディレクトリであるためです。
  - 「part1/part2」が既存のファイルである場合、「part1/part2/part3」の S3 作成は失敗します。
  - 「part1/part2/part3」が既存のファイルである場合、「part1/part2」の S3 作成または削除は失敗します。
  - 既存のオブジェクト（バージョン管理されていないバケット内の）が既存のオブジェクトの名前に一致するS3オブジェクトの作成で置き換えられます。このオブジェクトはNASで保持されますが、完全に一致する必要があります。上記の例では、名前が衝突しても一致しないため、既存のオブジェクトが削除されることはありません。

オブジェクト ストアは非常に多くの任意の名前をサポートするように設計されていますが、NASのディレクトリ構造では、非常に多くの名前が1つのディレクトリに配置されているとパフォーマンスの問題が発生する可能性があります。特に、スラッシュ（/）が含まれていない名前は、すべてNASマッピングのルート ディレクトリに配置されます。「NAS 対応」ではない名前を多用するアプリケーションは、NAS マッピングではなく、実際のオブジェクト ストア バケットでホストする方が適切です。

ONTAP SVM上のNASデータへのS3プロトコルアクセスを有効にする

S3プロトコルアクセスを有効にするには、NAS対応のSVMがS3対応サーバと同じ要件（オブジェクトストアサーバの追加など）を満たしていることを確認し、ネットワークと認証の要件を確認します。

ONTAPを新規にインストールする場合は、クライアントにNASデータを提供するようにSVMを設定したあとに、そのSVMへのS3プロトコルアクセスを有効にすることを推奨します。NASプロトコルの設定については、以下を参照してください。

- "NFSの設定"
- "SMBの設定"

開始する前に

S3プロトコルを有効にする前に、次の項目を設定する必要があります。

- S3プロトコルおよび目的のNASプロトコル（NFS、SMB、またはその両方）のライセンスが設定されています。
- 必要なNASプロトコル用にSVMが設定されている。
- NFSサーバまたはSMBサーバが存在します。
- DNSおよびその他の必要なサービスが設定されている。
- NASデータがクライアントシステムにエクスポートまたは共有されています。

タスクの内容

S3クライアントからS3対応SVMへのHTTPSトラフィックを有効にするには、認証局（CA）証明書が必要です。次の3つのソースからのCA証明書を使用できます。

- SVM上の新しいONTAP自己署名証明書。
- SVM上の既存のONTAP自己署名証明書。
- サードパーティの証明書。

NASデータの提供に使用するデータLIFをS3 / NASバケットにも使用できます。特定のIPアドレスが必要な場合は、を参照してください"データLIFを作成する"。LIFでS3データトラフィックを有効にするには、S3サービスデータポリシーが必要です。SVMの既存のサービスポリシーにS3を含めるように変更できます。

S3オブジェクトサーバを作成するときは、クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。S3サーバのFQDNの1文字目をバケット名にすることはできません。

System Manager

1. NASプロトコルが設定されているStorage VMでS3を有効にします。
   a. [ストレージ]>[Storage VM]*をクリックし、NAS対応Storage VMを選択して[設定]をクリックし、[S3]の下をクリックし ます。
   b. 証明書のタイプを選択します。システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。
   c. ネットワークインターフェイスを入力します。
2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。
   ◦ 今後シークレットキーは表示されません。
   ◦ 証明書情報が再度必要な場合は、 [* ストレージ] 、 [Storage VMs] の順にクリックし、 Storage VM を選択して、 [* 設定] をクリックします。

CLI

1. SVMでS3プロトコルが許可されていることを確認します。+
   `vserver show -fields allowed-protocols`
2. このSVMの公開鍵証明書を記録します。+新しいONTAP自己署名証明書が必要な場合は、を参照してください"CA証明書を作成してSVMにインストールする"。
3. サービスデータポリシーを更新する
   a. SVMのサービスデータポリシーを表示します。+
      `network interface service-policy show -vserver svm_name`

      の詳細については `network interface service-policy show`、を"ONTAPコマンド リファレンス"参照してください。

   b. とがない場合は、を `data-s3-server services`追加し `data-core`ます。+
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. SVMのデータLIFが要件を満たしていることを確認します。+
   `network interface show -vserver svm_name`

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

5. S3サーバを作成します。+
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

追加のオプションは、S3サーバの作成時または作成後いつでも指定できます。

- HTTPSはポート443ではデフォルトで有効になっています。ポート番号は、-secure-listener-portオプションを使用して変更できます。+ HTTPSを有効にすると、SSL/TLSとの適切な統合にCA証明書が必要になります。ONTAP 9 .15.1以降では、S3オブジェクトストレージでTLS 1.3がサポートされます。

- HTTPはデフォルトでは無効になっています。有効にすると、サーバはポート80でリスンします。is-http-enabledオプションを指定して有効にするか、-listener-portオプションを使用してポート番号を変更できます。+ HTTPを有効にすると、すべての要求と応答がクリアテキストでネットワーク経由で送信されます。

1. S3が設定されていることを確認します。+
   `vserver object-store-server show`

例次のコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。
`cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

関連情報

- "ネットワークインターフェイスservice-policy add-service"

ONTAP S3 NASバケットを作成する

S3 NAS バケットは、S3 バケット名と NAS パス間のマッピングです。S3 NASバケットを使用すると、既存のボリュームとディレクトリ構造を持つSVMネームスペースのどこにでもS3アクセスを提供できます。

開始する前に

- NASデータを含むSVMにS3オブジェクトサーバが設定されている。
- NASデータはに準拠していて"S3クライアントアクセスの要件"ます。

タスクの内容

SVMのルートディレクトリ内の任意のセットのファイルとディレクトリを指定するようにS3 NASバケットを設定できます。

また、次のパラメータを任意に組み合わせてNASデータへのアクセスを許可または禁止するバケットポリシーを設定することもできます。

- ファイルおよびディレクトリ
- ユーザおよびグループの権限
- S3処理

たとえば、大規模なユーザグループに読み取り専用データアクセスを許可するバケットポリシーと、そのデータのサブセットに対して限定されたグループに処理の実行を許可するバケットポリシーが必要になる場合があります。

ONTAP 9.17.1以降では、ジャンクションパスではなくボリュームにS3 NASバケットを直接リンクできます。デフォルトでは、NASボリューム上のS3バケットはジャンクションパスに関連付けられていますが、これはONTAP管理者がいつでも変更できます。これらの変更は、S3バケットの操作に支障をきたす可能性があります。ONTAPONTAP以降では、 `-is-nas-path-mutable false`オプション `vserver object-store-server bucket create` ONTAP CLIでコマンドを実行して、S3 NASバケットをボリュームにリンクできるようにします。デフォルトでは、 `-is-nas-path-mutable`設定されている `true` 。

S3 NAS「バケット」はマッピングであり、S3 バケットではないため、標準の S3 バケットの次のプロパティは S3 NAS バケットには適用されません。

- * aggr-list\aggr-list-multiplier \storage-service-level \volume\size\exclude-aggr-list\qos-policy-group *+ S3 NASバケットの設定時にボリュームまたはqtreeが作成されません。
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud** + S3 NAS バケットは、SnapMirror S3 を使用して保護またはミラーリングされませんが、代わりにボリューム粒度で利用可能な通常のSnapMirror保護が使用されます。
- バージョン管理状態+ NASボリュームには'通常'さまざまなバージョンを保存するためのスナップショット・テクノロジーが用意されていますただし、S3 NASバケットでは現在バージョン管理を使用できません。
- * logical-used\object-count *+と同等の統計情報は、volumeコマンドを使用してNASボリュームに対して利用できます。
- マルチパートオブジェクト + ONTAP 9.16.1以降、S3 NASバケットでマルチパートオブジェクトがサポートされます。 "高度な容量分散"基盤となるFlexGroupボリュームで有効になっています。高度な容量バランス調整はFlexGroupボリュームでのみ有効にできます。FlexVolFlexVolでは有効にできません。

手順

System Manager またはONTAP CLI を使用して NAS バケットを作成できます。

System Manager

NAS対応Storage VMに新しいS3 NASバケットを追加します。

1. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。
2. S3 NASバケットの名前を入力してStorage VMを選択し、サイズを入力せずに* More Options *をクリックします。
3. 有効なパス名を入力するか、[参照]をクリックして有効なパス名のリストから選択します。+有効なパス名を入力すると、S3 NAS設定に関係のないオプションは表示されません。
4. S3ユーザをNASユーザとグループにすでにマッピングしている場合は、権限を設定し、* Save *をクリックします。+この手順で権限を設定する前に、S3ユーザをNASユーザにマッピングしておく必要があります。

それ以外の場合は、* Save *をクリックしてS3 NASバケットの設定を完了します。

CLI

1. NAS ファイルシステムを含む SVM に S3 NAS バケットを作成します。+
```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
true|false [-comment <text>]
```

例1: S3 NASバケットを作成する

```
cluster1::> vserver object-store-server bucket create -bucket testbucket
-type nas -path /vol1
```

例2: S3 NASバケットを作成し、バケットをボリュームにリンクする

```
vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
-type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
```

ONTAP S3クライアントユーザーを有効にする

S3 クライアント ユーザーが NAS データにアクセスできるようにするには、S3 ユーザー名を対応する NAS ユーザーにマッピングし、バケット サービス ポリシーを使用して NAS データにアクセスする権限を付与する必要があります。

開始する前に

クライアント アクセス用のユーザー名 (LINUX/UNIX、Windows、S3 クライアント ユーザー) がすでに存在している必要があります。

S3の一部の機能はであることに注意して"S3 NASバケットではサポートされない"ください。

タスクの内容

S3ユーザ名を対応するLinux/UNIXまたはWindowsユーザにマッピングすると、NASファイルがS3クライアントからアクセスされたときにNASファイルの認証チェックが有効になります。S3からNASへのマッピングは、単一の名前またはPOSIXの正規表現で指定できるS3ユーザ名_Pattern_、およびLinux/UNIXまたはWindowsのユーザ名_Replacement _を指定して指定します。

ネームマッピングが存在しない場合は、デフォルトのネームマッピングが使用され、S3ユーザ名自体がUNIXユーザ名およびWindowsユーザ名として使用されます。UNIXおよびWindowsのデフォルトのユーザ名マッピングは、コマンドを使用して変更できます `vserver object-store-server modify`。

ローカルのネームマッピング設定のみがサポートされます。LDAPはサポートされません。

S3ユーザをNASユーザにマッピングしたら、ユーザに権限を付与できます。ユーザがアクセスできるリソース（ディレクトリとファイル）と、そのユーザに対して実行を許可または許可しないアクションを指定できます。

System Manager

1. UNIXクライアントまたはWindowsクライアント（またはその両方）のローカルネームマッピングを作成します。
   a. Storage > Buckets *をクリックし、S3 / NAS対応のStorage VMを選択します。
   b. を選択し、[ネームマッピング]（[ホストユーザとグループ]*）をクリックします → 。
   c. S3からWindows または S3からUNIX へのタイル（またはその両方）で、 Add をクリックし、目的の Pattern （**S3**）および Replacement *（NAS）ユーザ名を入力します。
2. クライアントアクセスを許可するバケットポリシーを作成します。
   a. [Storage]>[Buckets]をクリックし、目的の**S3**バケットの横にあるをクリックし ⋮ て、[Edit]*をクリックします。
   b. [*追加（Add）]をクリックし、必要な値を入力する。
      - * Principal *- S3ユーザ名を指定するか、デフォルト（すべてのユーザ）を使用します。
      - エフェクト-「*許可」または「*拒否」を選択します。
      - アクション-これらのユーザーとリソースのアクションを入力します。オブジェクトストアサーバで現在S3 NASバケットに対してサポートされているリソース処理のセットは、GetObject、PutObject、DeleteObject、ListBucket、GetBucketAclです。 GetObjectAcl 、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning、ListBucketVersionsの各メソッドに対応しています。このパラメータではワイルドカードを使用できます。
      - * Resources *-アクションを許可または拒否するフォルダまたはファイルのパスを入力するか、デフォルト（バケットのルートディレクトリ）を使用します。

CLI

1. UNIXクライアントまたはWindowsクライアント（またはその両方）のローカルネームマッピングを作成します。+
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position`-マッピング評価のプライオリティ番号。1または2を入力します。
   - `-pattern`- S3ユーザ名または正規表現
   - `-replacement`- WindowsまたはUNIXのユーザ名

例+
```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. クライアントアクセスを許可するバケットポリシーを作成します。+
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}`-ユーザが操作を要求したときにアクセスを許可するか拒否するかを指定します。

- `-action <Action>, …`-許可または拒否されるリソース操作を指定しますオブジェクトストアサーバで現在S3 NASバケットに対してサポートされている一連のリソース処理は、GetObject、PutObject、DeleteObject、ListBucket、GetBucketAcl、GetObjectAcl、およびGetBucketLocationです。このパラメータではワイルドカードを使用できます。
- `-principal <Objectstore Principal>, …`-このパラメータで指定したオブジェクトストアサーバのユーザまたはグループに対して、アクセスを要求しているユーザを検証します。
  - オブジェクトストアサーバグループを指定するには、グループ名にプレフィックスグループ/を追加します。
  - `-principal-`（ハイフン文字）は、すべてのユーザにアクセス権を付与します。
- `-resource <text>, …`-権限の許可/拒否を設定するバケット、フォルダ、またはオブジェクトを指定します。このパラメータではワイルドカードを使用できます。
- `[-sid <SID>]`-オブジェクトストアサーバのバケットポリシーのステートメントのテキストコメント（オプション）を指定します。

例+

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ

Microsoft Hyper-VおよびSQL Server向けのSMBの設定の概要

ONTAP の機能を使用すると、 SMB プロトコルを介した Microsoft アプリケーション、 Microsoft Hyper-V および Microsoft SQL Server の 2 つのノンストップオペレーションを有効にできます。

これらの手順は、SMBのノンストップオペレーションを実装する場合に使用します。想定している状況は次のとおりです。

- SMBプロトコルの基本的なファイルアクセスが設定されている。
- SVM にある SMB 3.0 以降のファイル共有を有効にして次のオブジェクトを格納する。
  - Hyper-Vカソウマシンファイル
  - SQL Serverシステムデータベース

関連情報

ONTAPテクノロジおよび外部サービスとのやり取りの詳細については、次のテクニカルレポート（TR）を参照してください。** "NetAppテクニカルレポート4172：『Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices』" "ネットアップテクニカルレポート 4369 ：『 Best Practices for Microsoft SQL Server and

SnapManager 7.2 for SQL Server with Clustered Data ONTAP 』"

Microsoft Hyper-VおよびSQL Server over SMBソリューション用のONTAPの設定

SMB 3.0以降のファイル共有では、継続的可用性を備えたファイル共有を使用して、Hyper-V仮想マシンファイルまたはは SQL ServerのシステムデータベースとユーザデータベースをSVM上のボリュームに格納し、同時に計画的イベントと計画外イベントのノンストップオペレーション（NDO）を実現できます。

Microsoft Hyper-V over SMB

Hyper-V over SMBソリューションを作成するには、まずMicrosoft Hyper-Vサーバにストレージサービスを提供するようにONTAPを設定する必要があります。また、Microsoftクラスタ（クラスタ構成を使用する場合）、Hyper-Vサーバ、CIFSサーバによってホストされている共有へのSMB 3.0の継続的可用性を備えた接続、および必要に応じて、SVMボリュームに格納されている仮想マシンファイルを保護するためのバックアップサービスも設定する必要があります。

Hyper-Vサーバは、Windows Server 2012以降で設定する必要があります。Hyper-Vサーバの構成は、スタンドアロン構成とクラスタ構成の両方がサポートされます。

- MicrosoftクラスタおよびHyper-Vサーバの作成については、MicrosoftのWebサイトを参照してください。
- SnapManager for Hyper-Vは、Snapshotベースの高速バックアップサービスを容易に実行できるホストベースのアプリケーションで、Hyper-V over SMB構成と統合できるように設計されています。

  Hyper-V over SMB 構成での SnapManager の使用については、 SnapManager for Hyper-V インストレーションアドミニストレーションガイドを参照してください。

Microsoft SQL Server over SMB

SQL Server over SMBソリューションを作成するには、まずMicrosoft SQL Serverアプリケーションにストレージサービスを提供するようにONTAPを設定する必要があります。また、Microsoftクラスタも設定する必要があります（クラスタ構成を使用している場合）。その後、WindowsサーバにSQL Serverをインストールして設定し、CIFSサーバによってホストされている共有への継続的可用性を備えたSMB 3.0接続を作成します。必要に応じて、SVMボリュームに格納されているデータベースファイルを保護するようにバックアップサービスを設定できます。

Windows Server 2012以降にSQL Serverをインストールして設定する必要があります。スタンドアロン構成とクラスタ構成の両方がサポートされます。

- Microsoftクラスタの作成およびSQL Serverのインストールと設定の詳細については、MicrosoftのWebサイトを参照してください。
- SnapCenter Plug-in for Microsoft SQL Serverは、Snapshotベースの高速バックアップサービスを容易に実現するホストベースのアプリケーションで、SQL Server over SMB構成と統合できるように設計されています。

  SnapCenter Plug-in for Microsoft SQL Serverの使用方法については、のドキュメントを参照してください "SnapCenter Plug-in for Microsoft SQL Server"。

Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨン

Hyper-V および SQL Server over SMB のノンストップオペレーションとは何ですか

Hyper-VおよびSQL Server over SMBのノンストップオペレーションとは、さまざまな管理タスクの間も、アプリケーションサーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持し、継続的可用性を実現できる機能のことです。これには、ストレージインフラの計画的停止と計画外停止の両方が含まれます。

SMBを介したアプリケーションサーバのノンストップオペレーションは、次のとおりです。

- 計画的なテイクオーバーとギブバック
- 計画外のテイクオーバー
- アップグレード
- 計画的なアグリゲートの再配置（ARL）
- LIF の移行とフェイルオーバー
- 計画的なボリュームの移動

SMB経由のノンストップオペレーションを実現するプロトコル

SMB 3.0のリリースに伴い、Microsoftから、Hyper-V over SMBおよびSQL Server over SMBのノンストップオペレーションのサポートに必要な機能を提供する新しいプロトコルがリリースされました。

ONTAP では、 SMB を介したアプリケーションサーバのノンストップオペレーションを実現するために、それらのプロトコルを使用しています。

- SMB 3.0
- 監視

Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨンニカンスルキナ概念

Hyper-V over SMB または SQL Server over SMB 解決策を設定する前に理解しておくべきノンストップオペレーション（ NDO ）の概念があります。

- * 共有の継続的な可用性 *

  継続的可用性プロパティが設定されている SMB 3.0 共有。継続的可用性を備えた共有を介して接続しているクライアントは、テイクオーバー、ギブバック、およびアグリゲート移転などのシステム停止を伴うイベントが発生しても、

- * ノード *

  クラスタのメンバーである単一のコントローラ。SFO ペアの 2 つのノードを区別するために、 1 つのノードを _local node_name と呼び、もう 1 つのノードを _partner node_or_remote node_name と呼ぶことがあります。ストレージのプライマリ所有者はローカルノードです。セカンダリ所有者は、プライマリ所有者に障害が発生したストレージを制御するパートナーノードです。各ノードは、そのストレージのプラ

イマリ所有者と、そのパートナーストレージのセカンダリ所有者です。

- * 無停止でのアグリゲートの再配置 *

  クライアントアプリケーションを中断することなく、クラスタの SFO ペア内のパートナーノード間でアグリゲートを移動できること。

- * 無停止フェイルオーバー *

  テイクオーバーを参照してください。

- * 無停止での LIF の移行 *

  LIF を介してクラスタに接続されたクライアントアプリケーションを中断することなく、 LIF を移行できること。SMB 接続の場合は、 SMB 2.0 以降を使用して接続するクライアントでのみ可能です。

- * ノンストップオペレーション * 。

  クライアントアプリケーションを中断することなく、 ONTAP の主な管理およびアップグレード操作を実行でき、ノード障害に耐えられること。全体として、この用語は、無停止テイクオーバー、無停止アップグレード、および無停止移行の各機能を指します。

- * 無停止アップグレード *

  アプリケーションを中断することなくノードのハードウェアまたはソフトウェアをアップグレードできること。

- * 無停止ボリューム移動 *

  ボリュームを使用しているすべてのアプリケーションを中断することなく、クラスタ内で自由にボリュームを移動できること。SMB 接続の場合、 SMB のすべてのバージョンで無停止でのボリューム移動がサポートされます。

- * 永続的ハンドル *

  接続が切断した場合に、継続的可用性を備えた接続が透過的に CIFS サーバに再接続できるように設定する SMB 3.0 のプロパティ。永続性ハンドルと同様に、接続中のクライアントとの通信が失われたあとの一定期間、 CIFS サーバによって永続的ハンドルが維持されます。ただし、永続的ハンドルは、永続性ハンドルよりも弾力性があります。CIFS サーバは、再接続後のクライアントにハンドルを 60 秒間使用する猶予を与え、その 60 秒間は、ファイルへのアクセスを要求する他のクライアントからのアクセスを拒否します。

  永続的ハンドルに関する情報は SFO パートナーの永続的ストレージにミラー化されます。これにより、永続的ハンドルを切断したクライアントが、 SFO パートナーによってノードのストレージの所有権が引き継がれた後に、永続性ハンドルを再利用することができるようになります。永続的ハンドルは、 LIF の移動（永続性ハンドルによってサポートされる）だけでなく、テイクオーバー、ギブバック、およびアグリゲートの再配置についても無停止での処理を提供します。

- * SFO ギブバック *

  テイクオーバーイベントから戻るときにホーム位置にアグリゲートを戻します。

- * SFO ペア *

2 つのノードのどちらかが機能を停止した場合に相互にデータを処理するようにコントローラが設定されたノードのペア。システムモデルに応じて、両方のコントローラを 1 つのシャーシに配置することも、別々のシャーシに配置することもできます。2 ノードクラスタでの HA ペアを指します。

- * テイクオーバー *

  ストレージのプライマリ所有者が失敗したときに、パートナーがストレージの制御を引き継ぐプロセス。SFO の文脈では、フェイルオーバーとテイクオーバーは同義です。

SMB 3.0の機能が**SMB**共有を介したノンストップオペレーションをサポートする仕組み

SMB 3.0 には、 Hyper-V over SMB および SQL Server over SMB 共有のノンストップオペレーションをサポートするためのきわめて重要な機能があります。これには、共有プロパティおよび_persistent handle_と呼ばれるファイルハンドルの一種が含まれます `continuously-available`。このハンドルを使用すると、SMBクライアントはファイルオープン状態を再要求し、SMB接続を透過的に再確立できます。

永続的ハンドルは、継続的な可用性が設定された共有に接続する SMB 3.0 対応のクライアントに付与できます。SMB セッションが切断された場合、 CIFS サーバは永続的ハンドルの状態に関する情報を保持します。CIFS サーバは、クライアントが再接続できる 60 秒間は他のクライアント要求をブロックするため、永続的ハンドルを持つクライアントは、ネットワークの切断後にハンドルを再要求できます。永続的ハンドルを持つクライアントは、Storage Virtual Machine（SVM）のいずれかのデータLIFを使用して、同じLIFまたは別のLIFを介して再接続できます。

アグリゲートの再配置、テイクオーバー、およびギブバックはすべて、 SFO ペア間で行われます。永続的ハンドルを持つファイルを使用したセッションの切断と再接続をシームレスに管理するために、パートナーノードでは、すべての永続的ハンドルのロック情報のコピーが保持されます。イベントが計画的か計画外かに関係なく、 SFO パートナーは、永続的ハンドルの再接続を無停止で管理できます。この新機能を使用すると、従来では業務が停止する状況となるイベントでも、 CIFS サーバへの SMB 3.0 接続を、 SVM に割り当てられた別のデータ LIF に透過的に無停止でフェイルオーバーできます。

永続的ハンドルを使用すると、CIFSサーバはSMB 3.0接続を透過的にフェイルオーバーできますが、障害によってHyper-VアプリケーションがWindows Serverクラスタ内の別のノードにフェイルオーバーされた場合、クライアントは切断されたハンドルのファイルハンドルを再要求できません。このシナリオでは、切断状態のファイルハンドルによって、Hyper-Vアプリケーションを別のノードで再起動した場合に、そのアプリケーションへのアクセスがブロックされる可能性があります。「フェイルオーバークラスタリング」は、 SMB 3.0 の一部で、古い競合するハンドルを無効にするメカニズムを提供して、このシナリオに対処します。このメカニズムを使用すると、 Hyper-V クラスタノードに障害が発生した場合に、 Hyper-V クラスタを迅速にリカバリできます。

透過的なフェイルオーバーを強化するための監視プロトコルの機能

監視プロトコルにより、 SMB 3.0 の継続的な可用性が確保された共有（ CA 共有）に対するクライアントフェイルオーバー機能が強化されます。監視を使用すると、 LIF のフェイルオーバーのリカバリがバイパスされるため、フェイルオーバーにかかる時間が短縮されます。ノードを使用できなくなると、 SMB 3.0 接続のタイムアウトを待たずにアプリケーションサーバに通知されます。

フェイルオーバーはシームレスです。クライアント上で実行されているアプリケーションは、フェイルオーバーが発生したことを認識しません。監視プロトコルを使用できなくてもフェイルオーバー処理に影響はありませんが、監視プロトコルを使用しないフェイルオーバーは効率が落ちます。

監視プロトコルを使用する高度なフェイルオーバーは、次の要件が満たされた場合に実行できます。

- SMB 3.0 が有効になっている SMB 3.0 対応の CIFS サーバでのみ使用できる。
- 共有で、共有の継続的な可用性プロパティが設定されている SMB 3.0 を使用している必要があります。
- アプリケーションサーバの接続先ノードのSFOパートナーに、少なくとも1つ以上、アプリケーションサーバのデータをホストするStorage Virtual Machine（SVM）に割り当てられた稼働中のデータLIFがある。

> 監視プロトコルは、 SFO ペアの間で実行されます。LIF はクラスタ内の任意のノードに移行できるため、すべてのノードがその SFO パートナーの監視プロトコルであることが必要になる場合があります。アプリケーションサーバのデータをホスティングしている SVM がパートナーノード上にアクティブなデータ LIF を持っていない場合、監視プロトコルは、指定されたノード上で SMB 接続の迅速なフェイルオーバーを提供することはできません。したがって、そのような構成の 1 つをホスティングしている SVM には、クラスタ内のすべてのノードに少なくとも 1 つ以上のデータ LIF が必要です。

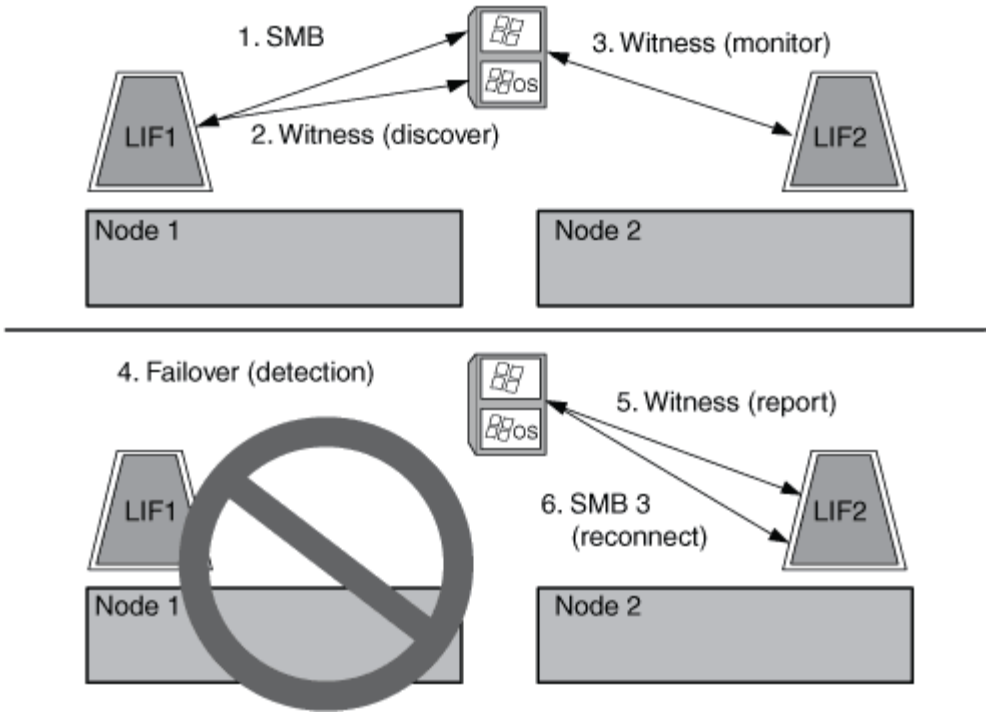
- アプリケーションサーバは、個々の LIF IP アドレスではなく、 DNS に格納されている CIFS サーバ名を使用して CIFS サーバに接続する必要があります。

監視プロトコルの仕組み

ONTAPは、ノードのSFOパートナーを監視として使用して、監視プロトコルを実装します。障害が発生した場合、パートナーは障害を迅速に検出し、SMBクライアントに通知します。

監視プロトコルでは、次のプロセスを使用してフェイルオーバーが強化されます。

1. アプリケーションサーバがノード1への継続的可用性を備えたSMB接続を確立すると、CIFSサーバからアプリケーションサーバに監視が利用可能であることが通知されます。
2. アプリケーションサーバは、ノード 1 に監視サーバの IP アドレスを要求し、 Storage Virtual Machine （ SVM ）に割り当てられたノード 2 （ SFO パートナー）のデータ LIF の IP アドレスリストを受け取ります。
3. アプリケーションサーバは、いずれかのIPアドレスを選択し、ノード2への監視接続を作成して、ノード1の継続的可用性を備えた接続を移行する必要がある場合に通知されるように登録します。
4. ノード 1 でフェイルオーバーが発生した場合、監視によってフェイルオーバーが容易になりますが、ギブバックには影響しません。
5. 監視によってフェイルオーバーイベントが検出され、監視接続を介してアプリケーションサーバに、SMB接続をノード2に移行する必要があることが通知されます。
6. アプリケーションサーバは、 SMB セッションをノード 2 に移行し、クライアントアクセスを中断することなく接続をリカバリします。



リモート**VSS**による共有ベースのバックアップ

リモート**VSS**を使用した共有ベースのバックアップの概要

リモートVSSを使用して、CIFSサーバに格納されているHyper-V仮想マシンファイルの共有ベースのバックアップを実行できます。

MicrosoftのリモートVSS（ボリュームシャドウコピーサービス）は、既存のMicrosoft VSSインフラを拡張したものです。リモートVSSでは、SMB共有のシャドウコピーをサポートするようにVSSインフラが拡張されました。また、Hyper-Vなどのサーバアプリケーションでは、SMBファイル共有にVHDファイルを格納できます。これらの拡張機能を使用すると、データと構成ファイルを共有に格納する仮想マシンに対して、アプリケーションと整合性のあるシャドウコピーを作成できます。

リモート**VSS**の概念

ここでは、リモートVSS（ボリュームシャドウコピーサービス）がHyper-V over SMB構成でバックアップサービスでどのように使用されるかを理解するために必要な概念について説明します。

- * VSS （ボリューム・シャドウ・コピー・サービス） *

  特定のボリューム上の特定の時点のデータのバックアップコピーまたはSnapshotを作成するMicrosoftのテクノロジ。VSSは、データサーバ、バックアップアプリケーション、ストレージ管理ソフトウェアを調整して、整合性のあるバックアップの作成と管理をサポートします。

- * リモート VSS （リモートボリュームシャドウコピーサービス） *

  SMB 3.0共有を介してデータにアクセスした特定の時点で整合性のあるデータの共有ベースのバックアップコピーを作成するMicrosoftのテクノロジです。Volume Shadow Copy Service と呼ばれることもあります。

- * シャドウコピー *

  共有に含まれるデータセットの明確に定義された特定の時点における複製です。シャドウコピーは、整合性のあるポイントインタイムバックアップを作成するために使用されます。これにより、システムまたはアプリケーションは元のボリューム上のデータを継続的に更新できます。

- * シャドウ・コピー・セット *

  1つ以上のシャドウコピーの集まりで、各シャドウコピーが1つの共有に対応します。シャドウコピーセット内のシャドウコピーは、同じ処理でバックアップする必要があるすべての共有を表します。セットに含めるシャドウコピーは、VSS対応アプリケーションのVSSクライアントによって識別されます。

- * シャドウ・コピー・セットの自動リカバリ *

  リモートVSSに対応したバックアップアプリケーションのバックアッププロセスの一部。シャドウコピーが格納されているレプリカディレクトリでポイントインタイムの整合性が確保されます。バックアップの開始時に、アプリケーション上のVSSクライアントは、バックアップ用にスケジュールされたデータ（Hyper-Vの場合は仮想マシンファイル）のソフトウェアチェックポイントの取得をアプリケーションにトリガーします。VSSクライアントは、アプリケーションの続行を許可します。シャドウコピーセットが作成されると、リモートVSSによってシャドウコピーセットが書き込み可能になり、書き込み可能なコピーがアプリケーションに公開されます。アプリケーションは、前の手順で作成したソフトウェアチェックポイントを使用して自動リカバリを実行し、シャドウコピーセットをバックアップ用に準備します。自動リカバリでは、チェックポイントの作成後にファイルとディレクトリに加えられた変更を展開することで、シャドウコピーを整合性のある状態にします。自動リカバリは、VSS対応バックアップのオプションの手順です。

- * シャドウ・コピー ID *

  シャドウコピーを一意に識別するGUIDです。

- * シャドウ・コピー・セット ID *

  同じサーバに対する一連のシャドウコピーIDを一意に識別するGUID。

- * SnapManager for Hyper-V *

  Microsoft Windows Server 2012 Hyper-Vのバックアップ / リストア処理を自動化して簡易化するソフトウェアです。リモートVSSと自動リカバリを使用して、SMB共有経由でHyper-Vファイルをバックアップします。

関連情報

Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨンニカンスルキナ概念

リモートVSSによる共有ベースのバックアップ

リモート**VSS**で使用されるディレクトリ構造の例

リモートVSSは、シャドウコピーの作成時に、Hyper-V仮想マシンファイルが格納されているディレクトリ構造をトラバースします。仮想マシンファイルのバックアップを正常に作成できるように、適切なディレクトリ構造について理解しておくことが重要です。

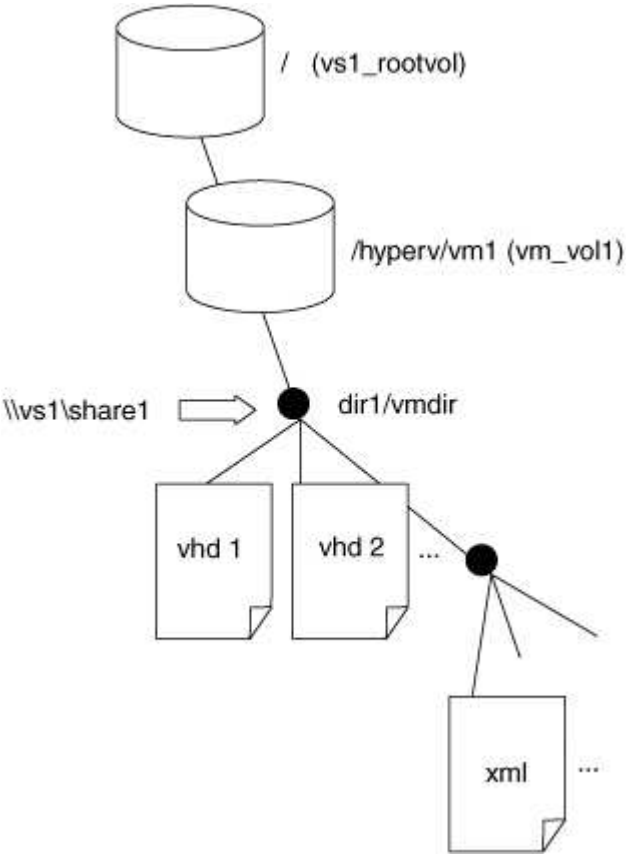
シャドウコピーを正常に作成するためにサポートされるディレクトリ構造は、次の要件を満たしています。

- 仮想マシンファイルの格納に使用されるディレクトリ構造内に存在するのは、ディレクトリと通常のファイルだけです。

  ディレクトリ構造には、ジャンクション、リンク、または通常以外のファイルは含まれません。

- 仮想マシンのファイルはすべて単一の共有内に存在します。
- 仮想マシンファイルの格納に使用されるディレクトリ構造が、設定されているシャドウコピーのディレクトリ階層を超えることはありません。
- 共有のルートディレクトリには、仮想マシンファイルまたはディレクトリのみが含まれています。

次の図では、Storage Virtual Machine（SVM）vs1上でジャンクションポイントをにしてvm_vol1という名前のボリュームが作成されています `/hyperv/vm1`。ジャンクションポイントの下に、仮想マシンファイルを格納するサブディレクトリが作成されます。Hyper-Vサーバの仮想マシンファイルには、パスのshare1を介してアクセスします `/hyperv/vm1/dir1/vmdir`。シャドウコピーサービスによって、share1の下のディレクトリ構造（設定されたシャドウコピーのディレクトリ階層まで）に格納されているすべての仮想マシンファイルのシャドウコピーが作成されます。



SnapManager for Hyper-Vによる**Hyper-V over SMB**のリモート**VSS**ベースのバックアップの管理方法

SnapManager for Hyper-V を使用して、リモート VSS ベースのバックアップサービスを管理できます。スペース効率に優れたバックアップセットを作成するには、SnapManager for Hyper-V で管理されているバックアップサービスを使用すると効果的です。

Hyper-V で管理されているバックアップ向けに SnapManager を最適化するには、次のようなものがあります。

- SnapDrive と ONTAP の統合により、 SMB 共有の場所を検出する際のパフォーマンスが最適化されます。

  ONTAP は、共有が存在するボリュームの名前を SnapDrive に提供します。

- SnapManager for Hyper-V は、シャドウコピーサービスでコピーする必要がある SMB 共有内の仮想マシンファイルのリストを指定します。

  仮想マシンファイルの対象リストを指定することで、シャドウコピーサービスで、共有内のすべてのファイルのシャドウコピーを作成する必要がなくなります。

- Storage Virtual Machine（SVM）には、SnapManager for Hyper-Vがリストアに使用するためのSnapshotが保持されます。

  バックアップフェーズはありません。バックアップは、スペース効率に優れたSnapshotです。

SnapManager for Hyper-V は、次のプロセスを使用して、 Hyper-V over SMB のバックアップとリストアの機能を提供します。

1. シャドウコピー処理を準備しています

   SnapManager for Hyper-V アプリケーションの VSS クライアントが、シャドウコピーセットを設定します。VSS クライアントは、どの共有をシャドウコピーセットに含めるかに関する情報を収集し、この情報を ONTAP に提供します。セットには 1 つ以上のシャドウコピーが含まれる場合があり、 1 つのシャドウコピーが 1 つの共有に対応します。

2. シャドウコピーセットの作成（自動リカバリが使用される場合）

   シャドウコピーセットに含まれている共有ごとに、 ONTAP がシャドウコピーを作成し、シャドウコピーを書き込み可能にします。

3. シャドウコピーセットの公開

   ONTAP によって作成されたシャドウコピーが Hyper-V 用の SnapManager に公開され、アプリケーションの VSS ライターが自動リカバリを実行できるようになります。

4. シャドウコピーセットを自動的にリカバリします

   シャドウコピーセットの作成中に、バックアップセットに含まれているファイルにアクティブな変更が発生する時間帯があります。アプリケーションの VSS ライターは、シャドウコピーを更新して、バックアップ前に完全な整合性が確保された状態にする必要があります。

   自動リカバリの実行方法はアプリケーションに固有です。リモート VSS はこのフェーズには関連しません。

5. シャドウコピーセットの完了とクリーンアップを行います

   自動リカバリの完了後に、 VSS クライアントが ONTAP に通知します。シャドウコピーセットが読み取り専用になり、バックアップできる状態になります。SnapManager for Hyper-Vをバックアップに使用する場合は、Snapshot内のファイルがバックアップになるため、バックアップフェーズでは、バックアップ

セット内の共有を含むボリュームごとにSnapshotが作成されます。バックアップが完了すると、シャドウコピーセットが CIFS サーバから削除されます。

Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピーオフロードの使用方法

Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _copy offloaded _ とも呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。ONTAP ODXコピーオフロードを使用すると、アプリケーションサーバでSMBインストール経由のコピー処理を実行する際のパフォーマンスが向上します。

ODX以外のファイル転送では、ソースCIFSサーバからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションCIFSサーバに転送します。要約すると、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODXファイル転送では、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現されるパフォーマンス上のメリットには、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用率（CPU、メモリ）の削減、ネットワークI/O帯域幅の使用量の削減などがあります。

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
```
ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとStorage Virtual Machine（SVM）は同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。

データは複数のSVMに所有されます。

Hyper-VソリューションでのODXコピーオフロードの具体的なユースケースには、次のようなものがあります。

- Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク（VHD）ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

  これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。

> Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

SQL Serverソリューションでの ODXコピーオフロードの具体的なユースケースには、次のようなものがあります。

- ODXコピーオフロードを使用すると、マッピングされたSMB共有間、または同じクラスタ内のSMB共有と接続されたiSCSI LUNの間でSQL Serverデータベースのエクスポートとインポートを行うことができます。
- ソースとデスティネーションのストレージが同じクラスタにある場合は、ODXコピーオフロードを使用してデータベースのエクスポートとインポートを行います。

設定に関する要件と考慮事項

ONTAPとライセンスの要件

SVMでノンストップオペレーションを実現するSQL Server over SMBまたはHyper-V over SMBソリューションを作成するときは、ONTAPとライセンスの特定の要件について理解しておく必要があります。

ONTAPのバージョンの要件

- Hyper-V over SMB

  ONTAPでは、Windows Server 2012以降で実行されるHyper-VでのSMB共有を介したノンストップ オペレーションがサポートされます。

- SQL Server over SMB

  ONTAPでは、Windows Server 2012以降で実行されるSQL Server 2012以降でのSMB共有を介したノンストップ オペレーションがサポートされます。

SMB共有を介したノンストップ オペレーションがサポートされるONTAP、Windows Server、およびSQL Serverのバージョンの最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ライセンス要件

次のライセンスが必要です。

- CIFS
- FlexClone（Hyper-V over SMBのみ）

  このライセンスは、バックアップにリモートVSSを使用する場合に必要になります。シャドウ コピー サービスでは、バックアップの作成時に使用されるファイルのポイントインタイム コピーを作成するためにFlexCloneが使用されます。

  リモートVSSを使用しないバックアップ方式を使用する場合、FlexCloneライセンスはオプションです。

FlexCloneライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneがない場合は、必要に"必要なライセンスがインストールされていることを確認する"応じて、必要に応じて"インストールする"を実行する必要があります。

ネットワークとデータ**LIF**の要件

ノンストップオペレーション用にSQL Server over SMBまたはHyper-V over SMB構成を作成する場合は、一定のネットワークとデータLIFの要件について理解しておく必要があります。

ネットワークプロトコルの要件

- IPv4およびIPv6ネットワークがサポートされています。
- SMB 3.0以降が必要です。

  SMB 3.0には、ノンストップオペレーションを実現するために必要な、継続的可用性を備えたSMB接続の確立に必要な機能が用意されています。

- DNSサーバには、CIFSサーバ名をStorage Virtual Machine（SVM）上のデータLIFに割り当てられたIPアドレスにマッピングするエントリが格納されている必要があります。

  通常、Hyper-VまたはSQL Serverアプリケーションサーバは、仮想マシンまたはデータベースファイルへのアクセス時に複数のデータLIFを介して複数の接続を確立します。正常に機能するためには、アプリケーションサーバは、複数の一意のIPアドレスへの複数の接続を確立するのではなく、CIFSサーバ名を使用してこれらの複数のSMB接続を確立する必要があります。

  監視でも、個 々 のLIF IPアドレスではなく、CIFSサーバのDNS名を使用する必要があります。

  ONTAP 9 .4以降では、SMBマルチチャネルを有効にすることで、Hyper-V over SMBおよびSQL Server over SMB構成のスループットとフォールトトレランスを向上させることができます。そのためには、クラスタとクライアントに1G、10G、またはそれ以上のNICを複数導入する必要があります。

データ**LIF**の要件

- SMB経由のアプリケーションサーバソリューションをホストするSVMには、クラスタ内のすべてのノードに稼働しているデータLIFが少なくとも1つ必要です。

  SVMデータLIFは、アプリケーションサーバがアクセスするデータを現在ホストしていないノードを含む、クラスタ内の他のデータポートにフェイルオーバーできます。さらに、監視ノードは常にアプリケーションサーバが接続されているノードのSFOパートナーであるため、クラスタ内のすべてのノードが監視ノードになる可能性があります。

- データLIFは、自動的にリバートされるように設定しないでください。

  テイクオーバーまたはギブバックの発生後、データLIFをホームポートに手動でリバートする必要があります。

- すべてのデータLIFのIPアドレスがDNSにエントリを持ち、すべてのエントリがCIFSサーバ名に解決される必要があります。

  アプリケーションサーバは、CIFSサーバ名を使用してSMB共有に接続する必要があります。LIFのIPアドレスを使用して接続を確立するようにアプリケーションサーバを設定しないでください。

- CIFSサーバ名がSVM名と異なる場合は、DNSエントリがCIFSサーバ名に解決される必要があります。

Hyper-V over SMB用の**SMB**サーバとボリュームの要件

ノンストップオペレーション用にHyper-V over SMB構成を作成する場合、一定のSMBサーバとボリュームの要件について理解しておく必要があります。

SMBサーバの要件

- SMB 3.0が有効になっている必要があります。

  これはデフォルトで有効になっています。

- デフォルトのUNIXユーザのCIFSサーバオプションが、有効なUNIXユーザアカウントを使用して設定されている必要があります。

  アプリケーションサーバは、SMB接続の作成時にマシンアカウントを使用します。すべてのSMBアクセスで、Windowsユーザが1つのUNIXユーザアカウントまたはデフォルトのUNIXユーザアカウントに正常にマッピングされている必要があるため、ONTAPは、アプリケーションサーバのマシンアカウントをデフォルトのUNIXユーザアカウントにマッピングできる必要があります。

- 自動ノードリファーラルを無効にする必要があります（この機能はデフォルトで無効になっています）。

  Hyper-Vマシンファイル以外のデータへのアクセスに自動ノードリファーラルを使用する場合は、そのデータ用のSVMを別途作成する必要があります。

- SMB サーバが属しているドメインで、 Kerberos と NTLM の両方の認証が許可されている必要があります。

  ONTAPはリモートVSSに対してKerberosサービスをアドバタイズしないため、ドメインはNTLMを許可するように設定する必要があります。

- シャドウコピー機能が有効になっている必要があります。

  この機能はデフォルトで有効になっています。

- シャドウコピーサービスでシャドウコピーの作成時に使用されるWindowsドメインアカウントが、SMBサーバのローカルのBUILTIN\AdministratorsグループまたはBUILTIN\Backup Operatorsグループに属している必要があります。

ボリュームの要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

  継続的可用性を備えたSMB接続を使用してアプリケーションサーバのNDOを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したNDOに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、SMB共有を介したNDOに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です。

  使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

SQLServeroverSMBノ**SMB**サアハトホリユウムノヨウケン

ノンストップオペレーション用にSQL Server over SMB構成を作成する場合は、SMBサーバとボリュームの一定の要件について理解しておく必要があります。

SMBサーバの要件

- SMB 3.0が有効になっている必要があります。

  これはデフォルトで有効になっています。

- デフォルトのUNIXユーザのCIFSサーバオプションが、有効なUNIXユーザアカウントを使用して設定されている必要があります。

  アプリケーションサーバは、SMB接続の作成時にマシンアカウントを使用します。すべてのSMBアクセスで、Windowsユーザが1つのUNIXユーザアカウントまたはデフォルトのUNIXユーザアカウントに正常にマッピングされている必要があるため、ONTAPは、アプリケーションサーバのマシンアカウントをデフォルトのUNIXユーザアカウントにマッピングできる必要があります。

また、SQL ServerはドメインユーザをSQL Serverサービスアカウントとして使用します。サービスアカウントは、デフォルトのUNIXユーザにもマッピングする必要があります。

- 自動ノードリファーラルを無効にする必要があります（この機能はデフォルトで無効になっています）。

  SQL Serverデータベースファイル以外のデータへのアクセスに自動ノードリファーラルを使用する場合は、そのデータ用のSVMを別途作成する必要があります。

- ONTAPへのSQL Serverのインストールに使用するWindowsユーザアカウントには、SeSecurityPrivilege権限を割り当てる必要があります。

  この権限は、SMBサーバのローカルのBUILTIN\Administratorsグループに割り当てられます。

ボリュームの要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

  継続的可用性を備えたSMB接続を使用してアプリケーションサーバのNDOを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したNDOに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、SMB共有を介したNDOに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- データベースファイルを含むボリュームにジャンクションを含めることはできますが、SQL Serverではデータベースディレクトリ構造の作成時にジャンクションをまたぐことはありません。
- SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理を成功させるには、ボリュームに十分な利用可能スペースが必要です。

  SQL Serverデータベースファイルが配置されているボリュームには、データベースディレクトリ構造と、共有内に格納されているすべてのファイルを格納できる十分なサイズが必要です。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

Hyper-V over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートするHyper-V over SMB構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項について理解しておく必要があります。

共有の要件

- アプリケーションサーバで使用される共有には、continuously-availableプロパティが設定されている必要があります。

継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイルロックを再要求できます。

- リモートVSSに対応したバックアップサービスを使用する場合は、ジャンクションを含む共有にHyper-Vファイルを配置することはできません。

  自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、シャドウコピーの作成は失敗します。自動リカバリ以外の場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

- リモートVSSに対応したバックアップサービスと自動リカバリを使用する場合は、次の内容を含む共有にHyper-Vファイルを配置できません。
  - シンボリックリンク、ハードリンク、またはワイドリンク
  - 通常以外のファイル

    シャドウコピーを実行する共有にリンクまたは通常以外のファイルがある場合、シャドウコピーの作成は失敗します。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

  - シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です（ Hyper-V over SMB の場合のみ）。

    使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

- アプリケーションサーバで使用される継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 属性のキャッシュ
  - BranchCache

考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- Hyper-V over SMB構成では、次の機能はサポートされません。
  - 監査
  - FPolicy
- パラメータがに設定され `Yes`ているSMB共有ではウィルススキャンは実行されません `continuously-availability`。

SQL Server over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートするSQL Server over SMB構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項について理解しておく必要があります。

共有の要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

  継続的可用性を備えたSMB接続を使用してアプリケーションサーバのノンストップオペレーションを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップオペレーションに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップオペレーションに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- アプリケーションサーバで使用される共有には、continuously-availableプロパティが設定されている必要があります。

  継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイルロックを再要求できます。

- データベースファイルを含むボリュームにジャンクションを含めることはできますが、SQL Serverではデータベースディレクトリ構造の作成時にジャンクションをまたぐことはありません。
- SnapCenter Plug-in for Microsoft SQL Serverの処理を成功させるには、ボリュームに十分な利用可能スペースが必要です。

  SQL Serverデータベースファイルが配置されているボリュームには、データベースディレクトリ構造と、共有内に格納されているすべてのファイルを格納できる十分なサイズが必要です。

- アプリケーションサーバで使用される継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 属性のキャッシュ
  - BranchCache

共有に関する考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- SQL Server over SMB構成では、次の機能はサポートされません。
  - 監査
  - FPolicy
- 共有プロパティが設定されているSMB共有ではウィルススキャンは実行されません `continuously-availability`。

Hyper-VoverSMBコウセイニカンスルリモオト**VSS**ニカンスルコウリヨシコウ

Hyper-V over SMB 構成用のリモート VSS に対応したバックアップソリューションを使用する場合は、一定の考慮事項について理解しておく必要があります。

一般的なリモート **VSS** の考慮事項

- Microsoft のアプリケーションサーバ 1 つにつき、最大 64 の共有を設定できます。

  1 つのシャドウコピーセットに 64 個を超える共有がある場合、シャドウコピー処理は失敗します。これはMicrosoftの要件です。

- アクティブなシャドウコピーセットは、 1 台の CIFS サーバで 1 つしか許可されません。

  同じCIFSサーバでシャドウコピー処理を実行中の場合、シャドウコピー処理は失敗します。これはMicrosoftの要件です。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、ジャンクションは許可されません。
  - 自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、シャドウコピーの作成は失敗します。
  - 自動リカバリではない場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

自動リカバリを行うシャドウコピーのみに適用されるリモート **VSS** の考慮事項

一部の制限は、自動リカバリを行うシャドウコピーにのみ適用されます。

- シャドウコピーの作成で許可される最大サブディレクトリ階層は 5 層です。

  これは、シャドウコピーサービスによってシャドウコピーバックアップセットが作成されるディレクトリ階層です。仮想マシンファイルを含むディレクトリのネストレベルが 5 よりも深い場合、シャドウコピーの作成は失敗します。この目的は、共有のクローニング時におけるディレクトリのトラバーサルを制限することです。最大ディレクトリ階層は CIFS サーバオプションを使用して変更できます。

- ボリューム上に利用可能なスペースが十分ある必要があります。

  使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、リンクまたは通常以外のファイルは許可されません。

  シャドウコピーの作成は、そのシャドウコピーに対応する共有内にリンクまたは通常以外のファイルがある場合には失敗します。これらのファイルはクローニングプロセスでサポートされていません。

- ディレクトリに対する NFSv4 ACL は許可されません。

  シャドウコピーの作成では、ファイルの NFSv4 ACL は維持されますが、ディレクトリの NFSv4 ACL は失われます。

- シャドウコピーセットの作成に許可される時間は最大 60 秒です。

Microsoft の仕様により、シャドウコピーセットの作成に許可される時間は最大 60 秒です。この時間内に VSS クライアントでシャドウコピーセットを作成できない場合、シャドウコピー処理は失敗します。したがって、シャドウコピーセット内のファイル数には制限があります。バックアップセットに含めることができる実際のファイル数または仮想マシン数は、一定ではなく、多くの要因に依存するため、お客様の環境ごとに判断する必要があります。

SQL ServerおよびHyper-V over SMBでのODXコピーオフロードの要件

アプリケーションサーバ経由でデータを送信せずに、仮想マシンファイルを移行する場合や、データベースファイルをソースストレージからデスティネーションストレージに直接エクスポートおよびインポートする場合は、 ODX コピーオフロードが有効になっている必要があります。ODX コピーオフロードと SQL Server および Hyper-V over SMB ソリューションを使用する場合は、理解しておくべきいくつかの要件があります。

ODX コピーオフロードを使用すると、パフォーマンスが大幅に向上します。この CIFS サーバオプションは、デフォルトで有効に設定されています。

- ODX コピーオフロードを使用するには、 SMB 3.0 が有効になっている必要があります。
- ソースボリュームは1.25GB以上である必要があります。
- コピーオフロードに使用するボリュームで重複排除を有効にする必要があります。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは8Kのみです。

  二次圧縮形式はサポートされません

- ODX コピーオフロードを使用して Hyper-V ゲストをディスク内やディスク間で移行するには、 Hyper-V サーバが SCSI ディスクを使用するように設定されている必要があります。

  デフォルトでは IDE ディスクが設定されますが、ディスクが IDE ディスクを使用して作成されている場合は、ゲストの移行時に ODX コピーオフロードは機能しません。

SQL ServerおよびHyper-V over SMB構成に関する推奨事項

SQL Server over SMB および Hyper-V over SMB 構成が安定して機能するようにするには、ソリューションの設定に関する推奨されるベストプラクティスについて理解しておく必要があります。

一般的な推奨事項

- アプリケーションサーバのファイルは一般的なユーザデータとは別に格納します。

  可能な場合は、 Storage Virtual Machine （ SVM ）とそのストレージ全体をアプリケーションサーバのデータ専用にします。

- パフォーマンスを最大限に高めるには、アプリケーションサーバのデータを格納する SVM で SMB 署名を無効にします。
- パフォーマンスの最適化とフォールトトレランスの向上を図るためには、 SMB マルチチャネルを有効にして、 1 つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立できるようにします。

- Hyper-VまたはSQL Server over SMB構成で使用する共有以外では、継続的可用性を備えた共有を作成しないでください。
- 継続的な可用性を確保するために使用される共有については、変更通知を無効に
- アグリゲートの再配置（ ARL ）には一部の処理が一時停止するフェーズがあるため、 ARL と同時にボリュームの移動を実行しないようにします。
- Hyper-V over SMBソリューションでは、クラスタ化された仮想マシンを作成するときにゲスト内iSCSIドライブを使用します。ONTAP SMB共有のHyper-V over SMBでは共有 `.VHDX`ファイルはサポートされません。

Hyper-VまたはSQL Server over SMB構成の計画

ボリューム構成ワークシートに記入する

このワークシートを使用すると、 SQL Server および Hyper-V over SMB 構成用のボリュームを作成する際に必要となる値を簡単に記録できます。

ボリュームごとに、次の情報を指定する必要があります。

- Storage Virtual Machine（SVM）名

  SVM 名はすべてのボリュームで同じです。

- ボリューム名
- アグリゲート名

  ボリュームは、クラスタ内のノード上のアグリゲートに作成できます。

- サイズ
- ジャンクションパス

アプリケーションサーバのデータを格納するボリュームの作成時には、次の事項を考慮してください。

- ルートボリュームのセキュリティ形式が NTFS でない場合は、ボリュームの作成時にセキュリティ形式を NTFS として指定する必要があります。

  デフォルトで、ボリュームは SVM ルートボリュームのセキュリティ形式を継承します。

- ボリュームには、デフォルトのボリュームスペースギャランティを設定する必要があります。
- 必要に応じて、スペースのオートサイズ管理を設定できます。
- Snapshotスペースリザベーションを決定するオプションをに設定する必要があります `0`。
- ボリュームに適用されるSnapshotポリシーを無効にする必要があります。

  SVM Snapshotポリシーが無効になっている場合は、ボリュームのSnapshotポリシーを指定する必要はありません。ボリュームはSVMのSnapshotポリシーを継承します。SVMのSnapshotポリシーが無効になっておらず、Snapshotを作成するように設定されている場合は、Snapshotポリシーをボリュームレベルで指定し、そのポリシーを無効にする必要があります。Snapshotの作成と削除は、シャドウコピーサービス対応のバックアップとSQL Serverバックアップによって管理されます。

- ボリュームに負荷共有ミラーを設定することはできません。

アプリケーションサーバで使用される共有を作成するジャンクションパスを選択する際は、共有エントリポイントの下に結合されたボリュームが含まれないようにする必要があります。

たとえば、仮想マシンファイルを「 vol1 」、「 vol2 」、「 vol3 」、および「 vol4 」という名前の 4 つのボリュームに格納する場合は、例に示すネームスペースを作成できます。その後、アプリケーションサーバの共有をパス、、 `/data1/vol2` `/data2/vol3`、およびに `/data2/vol4`作成できます `/data1/vol1`。

```
                        Junction                            Junction
Vserver Volume          Active   Junction Path              Path Source
------- ------------ -------- --------------------   -----------
vs1     data1         true     /data1                 RW_volume
vs1     vol1          true     /data1/vol1            RW_volume
vs1     vol2          true     /data1/vol2            RW_volume
vs1     data2         true     /data2                 RW_volume
vs1     vol3          true     /data2/vol3            RW_volume
vs1     vol4          true     /data2/vol4            RW_volume
```

情報の種類	値
ボリューム*1*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*2*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*3*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*4*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*5*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*6*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
追加ボリューム：ボリューム名、アグリゲート、サイズ、ジャンクションパス _	

SMB共有設定ワークシートに記入する

このワークシートを使用して、SQL ServerおよびHyper-V over SMB構成用の継続的可用性を備えたSMB共有を作成する際に必要となる値を記録してください。

SMB共有のプロパティと設定に関する情報

共有ごとに、次の情報を指定する必要があります。

- Storage Virtual Machine（SVM）名

  SVM 名はすべての共有で同じです

- 共有名
- パス
- 共有プロパティ

  次の2つの共有プロパティを設定する必要があります。

  - `oplocks`
  - `continuously-available`

次の共有プロパティは設定しないでください。

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - シンボリックリンクを無効にする必要があります（パラメータの値 `-symlink-properties`はnull [""]にする必要があります）。

共有パスに関する情報

リモートVSSを使用してHyper-Vファイルをバックアップする場合は、Hyper-Vサーバから仮想マシンファイルの格納場所へのSMB接続を確立する際に使用する共有パスの選択が重要になります。共有はネームスペース内の任意のポイントに作成できますが、Hyper-Vサーバで使用される共有のパスに結合されたボリュームを含めることはできません。ジャンクションポイントを含む共有パスでシャドウコピー処理を実行することはできません。

データベースディレクトリ構造を作成する場合、SQL Serverはジャンクションを横断できません。ジャンクションポイントを含むSQL Serverの共有パスは作成しないでください。

たとえば、次に示すネームスペースを例にとると、仮想マシンファイルまたはデータベースファイルをボリューム「vol1」、「vol2」、「vol3」、および「vol4」に格納する場合、アプリケーションサーバの共有をパス、、 `/data1/vol2`、 `/data2/vol3`および `/data2/vol4`作成する必要があります `/data1/vol1`。

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

管理用にパスと `/data2`パスに共有を作成することはできます `/data1`が、これらの共有を使用してデータを格納するようにアプリケーションサーバを設定しないでください。

計画ワークシート

情報の種類	値
ボリューム*1*：*SMB*共有名とパス	
ボリューム*2*：*SMB*共有名とパス	
ボリューム*3*：*SMB*共有名とパス	
ボリューム*4*：*SMB*共有名とパス	
ボリューム*5*：*SMB*共有名とパス	
ボリューム*6*：*SMB*共有名とパス	
ボリューム*7*：*SMB*共有名とパス	
追加ボリューム： SMB 共有名およびパス _	

Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成の作成

Hyper-Vオヨビ**SQLServeroverSMB**テノンストツフオヘレエシヨンヲシツケンスル**ONTAP**セツテイノカイヨウ

SMBを介したノンストップオペレーションを実現するHyper-VおよびSQL Server環境を使用するためには、ONTAPの設定手順をいくつか実行する必要があります。

Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成を作成する前に、次のタスクを完了しておく必要があります。

- クラスタでタイムサービスをセットアップする必要があります。
- SVM用のネットワークをセットアップします。
- SVMを作成します。
- SVMでデータLIFインターフェイスが設定されている必要があります。
- SVMでDNSが設定されている必要があります。
- SVMに必要なネームサービスをセットアップします。
- SMBサーバを作成しておく必要があります。

関連情報

Hyper-VまたはSQL Server over SMB構成の計画

設定に関する要件と考慮事項

Kerberos認証と**NTLMv2**認証の両方が許可されていることの確認（**Hyper-V over SMB**共有）

Hyper-V over SMB のノンストップオペレーションを実行する場合、データ SVM の CIFS サーバおよび Hyper-V サーバで Kerberos 認証と NTLMv2 認証の両方が許可されていなければなりません。CIFS サーバと Hyper-V サーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。

タスクの内容

Kerberos 認証は、継続的可用性を備えた共有への接続を確立する際に必要になります。また、リモート VSS のプロセスで NTLMv2 認証が使用されます。そのため、 Hyper-V over SMB 構成に対しては、両方の認証方法を使用した接続がサポートされている必要があります。

Kerberos 認証と NTLMv2 認証の両方が許可されるように、次の設定を行う必要があります。

- Storage Virtual Machine （ SVM ）で SMB のエクスポートポリシーが無効になっている必要があります。

SVM では、 Kerberos 認証と NTLMv2 認証がどちらも常に有効になりますが、エクスポートポリシーを使用することで認証方法に基づいてアクセスを制限することが可能です。

SMB のエクスポートポリシーは省略可能で、デフォルトでは無効になっています。エクスポートポリシーが無効になっている場合、 CIFS サーバでは Kerberos 認証と NTLMv2 認証の両方がデフォルトで許可されます。

- CIFS サーバと Hyper-V サーバが属するドメインで、 Kerberos 認証と NTLMv2 認証の両方を許可する必要があります。

Kerberos 認証は、 Active Directory ドメインではデフォルトで有効になります。ただし、 NTLMv2 認証は、セキュリティポリシーの設定またはグループポリシーで禁止されている場合があります。

手順

1. 次の手順に従って、 SVM でエクスポートポリシーが無効になっていることを確認します。
   a. 権限レベルをadvancedに設定します。

      ```
      set -privilege advanced
      ```

b. CIFSサーバオプションがに設定されている `false`ことを確認し `-is-exportpolicy-enabled`ます。

vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

c. admin権限レベルに戻ります。

set -privilege admin

2. SMB のエクスポートポリシーが無効になっていない場合は無効にします。

vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

ドメインで許可されている認証方法を確認する方法については、Microsoft TechNetライブラリを参照してください。

4. ドメインで NTLMv2 認証が許可されていない場合は、 Microsoft のドキュメントに記載されたいずれかの方法で NTLMv2 認証を有効にします。

例

次に、SVM vs1でSMBのエクスポートポリシーが無効になっていることを確認するコマンドの例を示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

ONTAPでドメインアカウントがデフォルトの**UNIX**ユーザにマッピングされていることを確認する

Hyper-V および SQL Server では、継続的可用性を備えた共有への SMB 接続を作成する際にドメインアカウントを使用します。接続を作成するには、コンピュータアカウントが UNIX ユーザに正しくマッピングされている必要があります。そのための最も便利な方法は、コンピュータアカウントをデフォルトの UNIX ユーザにマッピングすることです。

タスクの内容

Hyper-V および SQL Server は、ドメインコンピュータアカウントを使用して SMB 接続を作成します。また、 SQL Server は、 SMB 接続を作成するサービスアカウントとしてドメインユーザアカウントを使用します。

ストレージ仮想マシン（SVM）を作成すると、ONTAPは自動的に次の名前のデフォルトユーザーを作成します。 `pcuser` （UIDは `65534` ）と名付けられたグループ `pcuser` （GIDは `65534` ）に追加し、デフォルトのユーザーを `pcuser`グループ。クラスタを Data ONTAP 8.2 にアップグレードする前に存在していた SVM 上で Hyper-V over SMB ソリューションを構成する場合、デフォルトのユーザーとグループが存在しない可能性があります。デフォルトの UNIX ユーザを設定していない場合は、 CIFS サーバのデフォルトの UNIX ユーザを設定する前に、デフォルトのユーザとグループを作成する必要があります。

手順

1. デフォルトの UNIX ユーザが存在するかどうかを確認します。

```
vserver cifs options show -vserver <vserver_name>
```

2. デフォルトユーザオプションが設定されていない場合は、デフォルトの UNIX ユーザとして指定できる UNIX ユーザが存在するかどうかを確認します。

```
vserver services unix-user show -vserver <vserver_name>
```

3. デフォルト ユーザー オプションが設定されておらず、デフォルト UNIX ユーザーとして指定できる UNIX ユーザーがいない場合は、デフォルト グループとデフォルト UNIX ユーザーを作成し、デフォルト ユーザーをグループに追加します。

   、デフォルトのグループには通常グループに割り当てるGIDはである必要があり `65534`ます。

   a. デフォルトグループを作成します。

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. デフォルトユーザを作成し、デフォルトグループに追加します。

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. デフォルトのユーザとデフォルトグループが正しく設定されていることを確認します。

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

4. CIFS サーバのデフォルトのユーザが設定されていない場合は、次の手順を実行します。
   a. デフォルトユーザを設定します。

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

   b. デフォルトの UNIX ユーザが正しく設定されていることを確認します。

```
vserver cifs options show -vserver <vserver_name>
```

5. アプリケーションサーバのコンピュータアカウントがデフォルトのユーザに正しくマッピングされていることを確認するには、SVMの共有にドライブをマッピングし、コマンドを使用してWindowsユーザとUNIXユーザのマッピングを確認します `vserver cifs session show`。

   の詳細については `vserver cifs options`、を"ONTAPコマンド リファレンス"参照してください。

例

が存在します。 `pcuser`ユーザーは、SVM vs1 上の CIFS サーバのデフォルト ユーザーとして割り当てられます。

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
           User             User    Group  Full
Vserver    Name             ID      ID     Name
---------- ---------------- ------ ------ ----------------
vs1        nobody           65535  65535  -
vs1        pcuser           65534  65534  -
vs1        root             0      1      -
```

```
cluster1::> vserver services unix-group show -members
Vserver         Name                 ID
vs1             daemon               1
       Users: -
vs1             nobody               65535
       Users: -
vs1             pcuser               65534
       Users: -
vs1             root                 0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

SVMルートボリュームのセキュリティ形式が**NTFS**に設定されていることを確認する

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合は、ボリュームを NTFS セキュリティ形式で作成する必要があります。ルートボリュームのセキュリティ形式には、Storage Virtual Machine（SVM）で作成されたボリュームのデフォルトが適用されるため、ルートボリュームのセキュリティ形式はNTFSに設定する必要があります。

タスクの内容

- ルートボリュームのセキュリティ形式は SVM の作成時に指定できます。
- SVMの作成時にルートボリュームのセキュリティ形式をNTFS以外に設定した場合は、あとでコマンドを使用してセキュリティ形式を変更できます `volume modify`。

手順

1. SVM のルートボリュームの現在のセキュリティ形式を確認します。

   `volume show -vserver *vserver_name* -fields vserver,volume,security-style`

2. ルートボリュームのセキュリティ形式が NTFS 以外になっている場合は、セキュリティ形式を NTFS に変

更します。

volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. SVM のルートボリュームのセキュリティ形式が NTFS に設定されていることを確認します。

volume show -vserver *vserver_name* -fields vserver,volume,security-style

例

次に、SVM vs1のルートボリュームのセキュリティ形式がNTFSになっていることを確認するコマンドの例を示します。

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

必要な**CIFS**サーバオプションが設定されていることの確認

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合、必要な CIFS サーバオプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。

タスクの内容

- SMB 2.x と SMB 3.0 が有効になっている必要があります。
- パフォーマンスが向上したコピーオフロードを使用するには、 ODX コピーオフロードが有効になっている必要があります。
- Hyper-V over SMB 解決策でリモート VSS に対応したバックアップサービスを使用する場合は、 VSS シャドウコピーサービスが有効になっている必要があります（ Hyper-V のみ）。

手順

1. Storage Virtual Machine（SVM）で必要なCIFSサーバオプションが有効になっていることを確認します。
   a. 権限レベルをadvancedに設定します。

      set -privilege advanced

   b. 次のコマンドを入力します。

vserver cifs options show -vserver *vserver_name*

次のオプションをに設定する必要があり `true`ます。

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled`（Hyper-Vのみ）

2. いずれかのオプションがに設定されていない場合は `true`、次の手順を実行します。
   a. コマンドを使用して `vserver cifs options modify`に設定します `true`。
   b. コマンドを使用して、 `vserver cifs options show`オプションがに設定されていることを確認し `true`ます。
3. admin権限レベルに戻ります。

set -privilege admin

例

次に、SVM vs1でHyper-V over SMB構成の必須オプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、 ODX コピーオフロードのオプションを有効にする必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

パフォーマンスと冗長性を確保するための**SMB**マルチチャネルの設定

ONTAP 9 .4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立できます。これにより、Hyper-V over SMBおよびSQL Server over SMB構成のスループットとフォールトトレランスが向上します。

開始する前に

SMBマルチチャネル機能は、クライアントがSMB 3.0以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMBサーバではSMB 3.0以降がデフォルトで有効になっています。

タスクの内容

SMBクライアントは、ONTAPクラスタで適切な設定が見つかると、複数のネットワーク接続を自動的に検出して使用します。

SMBセッションでの同時接続数は、導入しているNICによって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

  クライアントはNICごとに1つの接続を確立し、すべての接続にセッションをバインドします。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

  クライアントはNICごとに最大4つの接続を確立し、すべての接続にセッションをバインドします。クライアントは、10G以上の容量の複数のNICで接続を確立できます。

また、次のパラメータを変更することもできます（advanced権限）。

- `-max-connections-per-session`

  マルチチャネルセッションごとに許可される最大接続数。デフォルトの接続数は32です。

  デフォルトよりも多くの接続を有効にする場合は、クライアント設定を調整する必要があります（デフォルトの接続数は32）。

- `-max-lifs-per-session`

  マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。デフォルトは256のネットワークインターフェイスです。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAPがSMBマルチチャネルセッションを報告していることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、すべてのSMBセッションに関する情報を表示します。1つのセッションに対する複数の接続が表示されています。

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

次の例は、セッションID 1のSMBセッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

NTFSデータボリュームを作成する

Hyper-V over SMB または SQL Server over SMB アプリケーションサーバで使用する継続的可用性を備えた共有を設定する前に、 Storage Virtual Machine （ SVM ）上に NTFS データボリュームを作成する必要があります。ボリューム構成ワークシートを使用して、データボリュームを作成します。

タスクの内容

データボリュームのカスタマイズに使用できるオプションのパラメータが用意されています。ボリュームのカスタマイズの詳細については、を参照して"論理ストレージ管理"ください。

データボリュームの作成時に、次の項目を含むボリューム内にはジャンクションポイントを作成しないでください。

- ONTAP によってシャドウコピーが生成される Hyper-V ファイル
- SQL Server を使用してバックアップされる SQL Server データベースファイル

mixed セキュリティ形式または UNIX セキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームを NTFS セキュリティ形式のボリュームに変更して、ノンストップオペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMBおよびSQL Server over SMBのノンストップオペレーションは、この構成で使用するボリュームをNTFSセキュリティ形式のボリュームとして作成しないと正しく機能しません。ボリュームを削除してNTFSセキュリティ形式でボリュームを再作成するか、Windowsホストでボリュームをマッピングしてボリューム上部にACLを適用し、ボリューム内のすべてのファイルとフォルダにACLを適用します。

手順

1. 適切なコマンドを入力して、データボリュームを作成します。

ボリュームを作成する **SVM** のルートボリュームのセキュリティ形式	入力するコマンド
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
NTFS ではありません	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. ボリュームの設定が正しいことを確認します。

   volume show -vserver *vserver_name* -volume *volume_name*

継続的可用性を備えた**SMB**共有の作成

データボリュームを作成したら、アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルと SQL Server データベースファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB 共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

手順

1. 既存のデータボリュームとそのジャンクションパスに関する情報を表示します。

   volume show -vserver *vserver_name* -junction

2. 継続的可用性を備えたSMB共有を作成します。

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   ◦ 必要に応じて、共有設定にコメントを追加できます。

- デフォルトでは、オフラインファイル共有プロパティは共有に設定され、に設定されます。 `manual`
- ONTAPによって、Windowsのデフォルトの共有権限である/ `Full Control`が設定された共有が作成されます `Everyone`。

3. 共有設定ワークシートのすべての共有について同じ手順を繰り返します。
4. コマンドを使用して、設定が正しいことを確認し `vserver cifs share show`ます。
5. 継続的な可用性が確保された共有に NTFS ファイル権限を設定するには、各共有にドライブをマッピングし、 Windows のプロパティ * ウィンドウを使用してファイル権限を設定します。

例

次のコマンドを実行すると、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上に「 `d ata2` 」という名前の継続的可用性を備えた共有が作成されます。シンボリックリンクを無効にするには、パラメータをに `""`設定し `-symlink`ます。

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                  Junction
Vserver   Volume     Active   Junction Path    Path Source
--------- ---------- -------- ---------------- ------------
vs1       data       true     /data            RW_volume
vs1       data1      true     /data/data1      RW_volume
vs1       data2      true     /data/data2      RW_volume
vs1       vs1_root   -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                     Vserver: vs1
                       Share: data2
     CIFS Server NetBIOS Name: VS1
                        Path: /data/data2
            Share Properties: oplocks
                              continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

ユーザアカウント（**SMB**共有の**SQL Server**用）に**SeSecurityPrivilege**権限を追加する

SQL Server のインストールに使用するドメインユーザアカウントには、デフォルトではドメインユーザに割り当てられていない権限を必要とする特定の操作を CIFS サーバで実行するために、「すべてのユーザ」権限を割り当てる必要があります。

開始する前に

SQL Server のインストールに使用するドメインアカウントがすでに存在している必要があります。

タスクの内容

SQL Server インストーラのアカウントに権限を追加するときに、 ONTAP がドメインコントローラに照会してアカウントを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. “s eepleed” 権限を追加します。

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   パラメータの値 `-user-or-group-name`は、SQL Serverのインストールに使用するドメインユーザアカウントの名前です。

2. 権限がアカウントに適用されていることを確認します。

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

例

次のコマンドでは、 Storage Virtual Machine （ SVM ） vs1 の EXAMPLE ドメインにある SQL Server インストーラのアカウントに「 `s eepleed` 」権限を追加しています。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

VSSシャドウコピーのディレクトリ階層の設定（**Hyper-V over SMB**共有用）

必要に応じて、シャドウコピーを作成する SMB 共有のディレクトリの最大階層を設定できます。このパラメータは、 ONTAP によってシャドウコピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

開始する前に

VSS シャドウコピー機能を有効にする必要があります。

タスクの内容

デフォルトでは、最大 5 つのサブディレクトリにシャドウコピーが作成されます。値がに設定されている場合 `0`、ONTAPはすべてのサブディレクトリにシャドウコピーを作成します。

> シャドウコピーセットのディレクトリ階層は 6 個以上のサブディレクトリまたはすべてのサブディレクトリを含むことができますが、シャドウコピーセットの作成は 60 秒以内に完了しなければならないという Microsoft の要件があります。この時間内に完了できない場合、シャドウコピーセットの作成は失敗します。作成時間が制限時間を超えないようにシャドウコピーのディレクトリ階層原因を設定しないでください。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. VSS シャドウコピーのディレクトリ階層を目的のレベルに設定します。

   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
   integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

Hyper-VおよびSQL Server over SMB構成を管理します。

継続的可用性を確保するための既存の共有の設定

既存の共有を変更して、継続的可用性を備えた共有にすることができます。この共有は、Hyper-VおよびSQL Serverアプリケーションサーバが Hyper-V仮想マシンおよび構成ファイルおよびSQL Serverデータベースファイルに無停止でアクセスするために使用します。

タスクの内容

既存の共有に次の特徴がある場合、SMBを介したアプリケーションサーバでノンストップオペレーションを実現する継続的可用性を備えた共有として使用することはできません。

- その共有に共有プロパティが設定されている場合 `homedirectory`
- 共有に有効なシンボリックリンクまたはワイドリンクが含まれている場合
- 共有のルートの下にジャンクションされたボリュームが含まれている場合

次の2つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files`パラメータは（デフォルト）または `none`に設定されます `manual。
- シンボリックリンクを無効にする必要があります。

次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。現在の共有プロパティのリストに含まれている場合は、継続的可用性を備えた共有から削除する必要があります。

- `attributecache`
- `branchcache`

手順

1. 現在の共有パラメータの設定と、設定済みの共有プロパティの現在のリストを表示します。

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. 必要に応じて、コマンドを使用して共有パラメータを変更し、シンボリックリンクを無効にし、オフラインファイルをmanualに設定し `vserver cifs share modify` ます。
   - シンボリックリンクを無効にするには、パラメータの値をに `""`設定し `-symlink`ます。
   - を指定すると、パラメータを正しい設定に `manual`設定できます `-offline-files。
3. 共有プロパティを追加し、必要に応じて共有プロパティを追加し `continuously-available` `oplocks` ます。

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   共有プロパティがまだ設定されていない場合は `oplocks`、共有プロパティと一緒に追加する必要があります `continuously-available`。

4. 継続的な可用性が確保された共有でサポートされていない共有プロパティを削除します。

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   共有プロパティをカンマで区切って指定すると、1つ以上の共有プロパティを削除できます。

5. パラメータと `-offline-files`パラメータが正しく設定されていることを確認し `-symlink`ます。

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. 設定済みの共有プロパティのリストが正しいことを確認します。

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

例

次の例は、Storage Virtual Machine（SVM）「vs1」に「share1」という名前の既存の共有をSMBを介したアプリケーションサーバでのNDO用に設定する方法を示しています。

- パラメータをに設定すると、共有でシンボリックリンクが無効になります `-symlink ""`。
- `-offline-file`パラメータが変更され、に設定され `manual`ます。
- `continuously-available`共有プロパティが共有に追加されます。
- `oplocks`共有プロパティはすでに共有プロパティのリストに含まれているため、追加する必要はありません。
- `attributecache`共有プロパティが共有から削除されます。
- `browsable`共有プロパティは、SMBを介したアプリケーションサーバでのNDOに使用される継続的可用性を備えた共有では省略可能で、共有プロパティの1つとして保持されます。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Hyper-V over SMBバックアップ用のVSSシャドウコピーの有効化と無効化

VSS 対応バックアップアプリケーションを使用して、 SMB 共有に格納された Hyper-V 仮想マシンファイルをバックアップする場合は、 VSS シャドウコピーを有効にする必要があります。VSS 対応バックアップアプリケーションを使用しない場合は、 VSS シャドウコピーを無効にできます。デフォルトでは、 VSS シャドウコピーは有効になっています。

タスクの内容

VSS シャドウコピーはいつでも有効または無効にできます。

手順

1. 権限レベルをadvancedに設定します。

   set -privilege advanced

2. 次のいずれかを実行します。

VSS シャドウコピーの設定	入力するコマンド
有効	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true**
無効にする	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false**

3. admin権限レベルに戻ります。

   set -privilege admin

例

次のコマンドを実行すると、 SVM vs1 で VSS シャドウコピーが有効になります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

統計を使用して**Hyper-V**および**SQL Server over SMB**のアクティビティを監視する

ONTAPで使用できる統計オブジェクトとカウンタの確認

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	`statistics catalog object show`
使用可能な特定のオブジェクト	`statistics catalog object show -object` *`object_name`*
使用可能なカウンタ	`statistics catalog counter show -object` *`object_name`*

   詳細はこちら `statistics catalog object show`そして `statistics catalog counter show`の中で"ONTAPコマンド リファレンス" 。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次のコマンドを実行すると、advanced権限レベルで表示した場合の、クラスタ内のCIFSアクセスとSMBアクセスに関連する選択した統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

次のコマンドを実行すると、advanced権限レベルで表示したオブジェクトの一部のカウンタに関する情報が表示され `cifs`ます。

> この例で表示されているのはオブジェクトの使用可能なカウンタの一部ではありませ `cifs`ん。出力は省略されています。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

の詳細については `statistics start`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPの**SMB**統計を表示します。

パフォーマンスを監視して問題を診断するために、さまざまなSMB統計を表示することができます。

手順

1. コマンドとオプションの `statistics stop`コマンドを使用して、 `statistics start`データサンプルを収集します。
2. 次のいずれかを実行します。

統計を表示する対象	入力するコマンド
SMBのすべてのバージョン	**statistics show -object cifs**
SMB 1.0	**statistics show -object smb1**
SMB 2.xおよびSMB 3.0	**statistics show -object smb2**
ノードのSMBサブシステム	**statistics show -object nblade_cifs**

関連情報

- "statistics show"
- "statistics start"
- "statistics stop"

構成がノンストップオペレーションに対応していることを確認する

ヘルス監視を使用してノンストップオペレーションのステータスが正常かどうかを確認する

ヘルスモニタを使用すると、クラスタ全体のシステムヘルスステータスに関する情報が得られます。ヘルスモニタは Hyper-V over SMB および SQL Server over SMB 構成を監視して、アプリケーションサーバの Nondisruptive Operation （ NDO ；ノンストップオペレーション）を実現します。ステータスがデグレードの場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を確認できます。

ヘルスモニタはいくつかあります。ONTAP では、システム全体の健全性と個々のヘルスモニタの健全性の両方が監視されます。ノード接続ヘルスモニタには、 CIFS-NDO サブシステムが含まれています。モニタには一連のヘルスポリシーがあり、特定の物理的な条件によってシステムが停止する可能性がある場合にアラートをトリガーするポリシーと、システム停止が発生している場合にアラートが生成し、対処方法に関する情報を提供するポリシーがあります。SMB を介した NDO 構成では、アラートは次の 2 つの状態で生成されます。

アラートID	重大度	条件
HaNotReadyCifsNdo_Alert	メジャー	ノード上のアグリゲート内のボリュームでホストされている1つ以上のファイルが、継続的可用性を備えたSMB共有を介して開かれており、障害が発生した場合でも継続性が保証されるはずですが、パートナーとのHA関係が設定されていないか正常ではありません。
NoStandbyLifCifsNdo_Alert	マイナー	Storage Virtual Machine （ SVM ）はノードから SMB を介してアクティブにデータを提供しており、SMB ファイルは継続的可用性を備えた共有を介して継続的に開かれているが、そのパートナーノードが SVM のアクティブなデータ LIF を公開していない。

システムヘルスの監視を使用してノンストップオペレーションのステータスを表示します。

コマンドを使用すると、クラスタのシステムヘルス全体およびCIFS-NDOサブシステムのヘルスに関する情報の表示、アラートへの応答、以降のアラートの設定、ヘルスモニタの設定に関する情報の表示を行うことができます `system health`。

手順

1. 適切な操作を実行して、ヘルスステータスを監視します。

表示する項目	入力するコマンド
個々のヘルスモニタのステータス全体が反映された、システムのヘルスステータス	**system health status show**
CIFS-NDO サブシステムのヘルスステータスに関する情報	**system health subsystem show -subsystem CIFS-NDO -instance**

2. 適切な操作を実行して、 CIFS-NDO アラートの監視がどのように設定されているかに関する情報を表示します。

表示する情報	入力するコマンド
監視対象のノード、初期化状態、ステータスなど、CIFS-NDO サブシステムのヘルスモニタの設定とステータス	**system health config show -subsystem CIFS-NDO**
ヘルスモニタで生成される可能性がある CIFS-NDO アラート	**system health alert definition show -subsystem CIFS-NDO**

表示する情報	入力するコマンド
アラートが発行されるタイミングを決定する、CIFS-NDO ヘルスモニタのポリシー	**system health policy definition show -monitor node-connect**

詳細な情報を表示するには、パラメータを使用し `-instance`ます。

例

次の出力は、クラスタおよび CIFS-NDO サブシステムのヘルスステータス全体に関する情報を示しています。

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                    Subsystem: CIFS-NDO
                       Health: ok
         Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                         Node: node2
  Subsystem Refresh Interval: 5m
```

次の出力は、 CIFS-NDO サブシステムのヘルスモニタの設定とステータスに関する詳細な情報を示しています。

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

継続的可用性を備えた**SMB**共有の設定の確認

ノンストップオペレーションをサポートするには、 Hyper-V および SQL Server の SMB 共有が継続的可用性を備えた共有として設定されている必要があります。また、それ以外にも、いくつかの共有設定について確認が必要になります。計画的または計画外の停止が発生する状況でアプリケーションサーバのノンストップオペレーションをシームレスに実行できるように、共有が適切に設定されていることを確認してください。

タスクの内容

次の2つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files`パラメータは（デフォルト）または `none`に設定されます `manual。
- シンボリックリンクを無効にする必要があります。

ノンストップオペレーションが適切に実行されるようにするには、次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

手順

1. オフラインファイルがまたは `disabled`に設定されていること、およびシンボリックリンクが無効になっていることを確認し `manual`ます。

   vserver cifs shares show -vserver *vserver_name*

2. SMB 共有が継続的可用性を確保するように設定されていることを確認します。

   vserver cifs shares properties show -vserver *vserver_name*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 share1 」という名前の共有の共有設定を表示します。オフラインファイルはに設定され、シンボリックリンクは無効になってい `manual`ます（出力フィールドにハイフンが表示され `Symlink Properties`ます）。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
            Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例は、 SVM vs1 上の「 share1 」という名前の共有の共有プロパティを表示します。

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

LIFステータスの確認

Hyper-VおよびSQL Server over SMB構成のStorage Virtual Machine（SVM）をクラスタ内の各ノードにLIFを配置するように設定した場合でも、日常業務中に一部のLIFが別のノードのポートに移動することがあります。LIF のステータスを確認して、必要な措置を講じる必要があります。

タスクの内容

シームレスなノンストップオペレーションの運用支援を提供するには、クラスタ内の各ノードの SVM に少なくとも 1 つの LIF を配置し、すべての LIF をホームポートに関連付ける必要があります。設定されている LIF の中に現在ホームポートに関連付けられていないものがある場合は、ポートの問題を修正してから、対応するホームポートに LIF をリバートする必要があります。

手順

1. 設定されている SVM の LIF に関する情報を表示します。

   network interface show -vserver *vserver_name*

   この例では、「 lif1 」はホームポートに配置されていません。

```
network interface show -vserver vs1
```

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. 対応するホームポートに関連付けられていない LIF がある場合は、次の手順を実行します。

   a. それぞれの LIF について、 LIF のホームポートを確認します。

   network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

   ```
   vserver lif  home-node  home-port
   ------- ---- ---------- ---------
   vs1     lif1 node1      e0d
   ```

   b. それぞれの LIF について、 LIF のホームポートが up 状態になっているかどうかを確認します。

   network port show -node *node_name* -port *port* -fields port,link

   ```
   network port show -node node1 -port e0d -fields port,link
   ```

   ```
   node       port link
   ---------- ---- ----
   node1      e0d  up
   ```

   この例では、「lif1」をホームポートに戻す必要があります `node1:e0d`。

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

3. LIFを関連付けるホームポートのネットワークインターフェイスが状態になっていない場合は `up`、問題を解決してup状態にします。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。

4. 必要に応じて、ホームポートに LIF をリバートします。

network interface revert -vserver *vserver_name* -lif *lif_name*

network interface revert -vserver vs1 -lif lif1

の詳細については `network interface revert`、を"ONTAPコマンド リファレンス"参照してください。

5. クラスタ内の各ノードにアクティブな SVM の LIF があることを確認します。

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

SMBセッションの継続的可用性の確認

SMBセッション情報を表示する

SMB接続、SMB Session ID、セッションを使用しているワークステーションのIPアドレスなど、確立されているSMBセッションに関する情報を表示できます。セッションのSMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

タスクの内容

SVM上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのパラメータを使用すると、選択したフィールドに関する出力を表示できます `-fields`。

  と入力して、使用できるフィールドを指定できます `-fields ?`。

- パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます `-instance`。
- パラメータまたは `-instance`パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます `-fields`。

手順

1. 次のいずれかを実行します。

表示する **SMB** セッション情報	入力するコマンド
SVM上のすべてのセッション（要約形式）	**vserver cifs session show -vserver *vserver_name***
指定した接続IDのファイル	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
指定したワークステーションのIPアドレスから	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
指定したLIF IPアドレスのファイル	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
指定したノードのオブジェクト	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	指定したWindowsユーザからのセッション
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* の形式 `user_name` は `[domain]\user` です。	指定した認証メカニズムを使用している場合

表示する **SMB** セッション情報	入力するコマンド
vserver cifs session show -vserver *vserver_name* -auth-mechanism authentication_mechanism には、次のいずれかの値を `-auth-mechanism`指定できます。 • NTLMv1 • NTLMv2 • Kerberos • Anonymous	指定したプロトコルバージョンを使用している場合

表示する **SMB** セッション情報	入力するコマンド
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version には、次のいずれかの値を `-protocol-version`指定できます。 • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 継続的可用性を備えた保護とSMBマルチチャネルは、SMB 3.0以降のセッションでのみ使用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を以降に設定します。SMB3	指定したレベルの継続的可用性を備えた保護を使用しているセッション

表示する **SMB** セッション情報	入力するコマンド
vserver cifs session show -vserver *vserver_name* -continuously -available *continuously_available_protection_level* には、次のいずれかの値を `-continuously-available`指定できます。 • No • Yes • Partial	指定したSMB署名セッションステータスのセッション

例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。接続はドメインアカウントを使用して行われました。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
               Connected Time: 10m 43s
                    Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

次のコマンドを実行すると、SVM vs1上のSMB 3.0とSMBマルチチャネルを使用しているセッションに関するセッション情報が表示されます。この例では、ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するには、Kerberos認証を使用して接続を確立する必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

ONTAPで開いている**SMB**ファイルに関する情報を表示する

SMB接続とSession ID、ホスティングボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報も表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

タスクの内容

確立されたSMBセッションで開いているファイルに関する情報を表示できます。表示される情報は、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと継続的可用性を備えた保護を使用して開かれていないファイルがある場合（コマンド出力のフィールド `vserver cifs session show`の値 `-continuously-available`は `Partial`）、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

オプションのパラメータを何も指定せずにコマンドを実行することで、Storage Virtual Machine（SVM）上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show`。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションのパラメータを使用すると、選択したフィールドの出力を表示できます `-fields`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

- パラメータを使用すると、開いているSMBファイルに関する詳細情報を表示できます `-instance`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

手順

1. 次のいずれかを実行します。

表示する開いている **SMB** ファイル	入力するコマンド
SVM上のファイル（要約形式）	**vserver cifs session file show -vserver *vserver_name***
指定したノードのオブジェクト	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	指定したファイルIDのファイル
vserver cifs session file show -vserver *vserver_name* -file-id integer	指定したSMB接続IDのファイル
vserver cifs session file show -vserver *vserver_name* -connection-id integer	指定したSMB Session IDのファイル
vserver cifs session file show -vserver *vserver_name* -session-id integer	指定したホストアグリゲートのファイル
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	指定したボリュームのファイル
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	指定したSMB共有のファイル
vserver cifs session file show -vserver *vserver_name* -share *share_name*	指定したSMBパスのファイル

表示する開いている **SMB** ファイル	入力するコマンド
vserver cifs session file show -vserver *vserver_name* -path *path*	指定したレベルの継続的可用性を備えた保護を使用している
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* には、次のいずれかの値を `-continuously-available` 指定できます。 • No • Yes 継続的可用性のステータスがの場合は No、開いているファイルがテイクオーバーやギブバックからの無停止でのリカバリに対応していません。また、ハイアベイラビリティ関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。	指定した再接続状態のファイル

出力結果の絞り込みに使用できるオプションのパラメータがほかにもあります。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

SANストレージの管理

SANの概念

iSCSIを使用したSANプロビジョニング

SAN環境では、ストレージシステムはストレージターゲットデバイスを含むターゲットです。iSCSIおよびFCの場合、ストレージターゲットデバイスはLUN（論理ユニット）と呼ばれます。Non-Volatile Memory Express（NVMe）over Fibre Channelでは、ストレージターゲットデバイスをネームスペースと呼びます。

iSCSIおよびFCの場合はLUNを作成するか、NVMeの場合はネームスペースを作成してストレージを構成します。LUNまたはネームスペースには、ホストからInternet Small Computer Systems Interface（iSCSI）またはFibre Channel（FC；ファイバチャネル）プロトコルネットワークを使用してアクセスします。

iSCSIネットワークに接続するために、ホストは標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載したTCPオフロードエンジン（TOE）カード、Converged Network Adapter（CNA；統合ネットワークアダプタ）、または専用のiSCSI Host Bus Adapter（HBA；ホストバスアダプタ）を使用できます。

FCネットワークに接続するには、ホストにFC HBAまたはCNAが必要です。

サポートされるFCプロトコルは次のとおりです。

- FC
- FCoE
- NVMe

iSCSIターゲットノードのネットワーク接続と名前

iSCSIターゲットノードは、いくつかの方法でネットワークに接続できます。

- ONTAPに統合されたソフトウェアを使用して、イーサネットインターフェイスを介して接続します。
- 複数のシステムインターフェイス上。iSCSIに使用されるインターフェイスで、SMBやNFSなどの他のプロトコルのトラフィックも転送できます。
- ユニファイドターゲットアダプタ（UTA）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）を使用する。

すべてのiSCSIノードにはノード名が必要です。

iSCSI ノード名の 2 つの形式、つまり、タイプ指定子は、 _iqn と _eui _ です。SVM iSCSIターゲットでは、常にiqnタイプ指定子が使用されます。イニシエータには、iqnタイプまたはeuiタイプの指定子を使用できます。

ストレージシステムのノード名

iSCSIを実行している各SVMには、逆ドメイン名と一意のエンコード番号に基づいたデフォルトのノード名があります。

ノード名は次の形式で表示されます。

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

次の例は、一意のエンコード番号を持つストレージシステムのデフォルトのノード名を示しています。

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

iSCSIのTCPポート

iSCSIプロトコルは、TCPポート番号3260を使用するようにONTAPで設定されています。

ONTAPでは、iSCSIのポート番号の変更はサポートされていません。ポート番号3260はiSCSI仕様の一部として登録されており、他のアプリケーションやサービスでは使用できません。

関連情報

"NetAppのマニュアル：「ONTAP SANホスト構成」"

iSCSIサービスの管理

iSCSIサービスの管理

Storage Virtual Machine（SVM）のiSCSI論理インターフェイスでiSCSIサービスの可用性を管理するには、コマンドまたは `vserver iscsi interface disable`コマンドを使用し `vserver iscsi interface enable`ます。

デフォルトでは、iSCSIサービスはすべてのiSCSI論理インターフェイスで有効になっています。

ホストでのiSCSIの実装方法

iSCSIは、ハードウェアまたはソフトウェアを使用してホストに実装できます。

iSCSIは次のいずれかの方法で実装できます。

- ホストの標準イーサネットインターフェイスを使用するイニシエータソフトウェアを使用する。
- iSCSI Host Bus Adapter （ HBA ；ホストバスアダプタ）を使用する。ホストオペレーティングシステムでは、 iSCSI HBA をローカルディスクを搭載した SCSI ディスクアダプタとみなします。
- TCP / IP処理をオフロードするTCP Offload Engine（TOE）アダプタを使用する。

  iSCSIプロトコルの処理は、引き続きホストソフトウェアによって実行されます。

iSCSI認証の仕組み

iSCSIセッションの第1段階では、イニシエータがストレージシステムにログイン要求を送信してiSCSIセッションを開始します。ストレージシステムは、ログイン要求を許可または拒否するか、ログインが不要であると判断します。

iSCSI認証方式は次のとおりです。

- Challenge Handshake Authentication Protocol（CHAP）--イニシエータはCHAPユーザ名とパスワードを使用してログインします。

  CHAPパスワードを指定するか、16進数のシークレットパスワードを生成できます。CHAPユーザ名およびパスワードには、次の2種類があります。

  - インバウンド - ストレージシステムがイニシエータを認証します。

    CHAP認証を使用する場合は、インバウンド設定が必要です。

  - アウトバウンド - イニシエータがストレージシステムを認証できるようにするオプションの設定です。

    インバウンドユーザ名およびパスワードをストレージシステムで定義した場合にのみ、アウトバウンド設定を使用できます。

- deny --イニシエータはストレージシステムへのアクセスを拒否されます
- none --ストレージシステムはイニシエータの認証を必要としません

イニシエータとその認証方法の一覧を定義できます。このリストにないイニシエータに適用されるデフォルトの認証方法を定義することもできます。

関連情報

"Data ONTAP での Windows マルチパス・オプション：ファイバ・チャネルおよび iSCSI"

iSCSIイニシエータのセキュリティ管理

ONTAP は、 iSCSI イニシエータのセキュリティを管理するためのさまざまな機能を備えています。iSCSI イニシエータのリストと各イニシエータに対する認証方法の定義、認証リスト内のイニシエータと関連する認証方法の表示、認証リストに対するイニシエータの追加と削除、リストにないイニシエータに対するデフォルトの iSCSI イニシエータ認証方法の定義を行うことができます。

iSCSIエンドポイントの分離

既存のiSCSIセキュリティコマンドでは、IPアドレス範囲を指定することも、複数のIPアドレスを指定することもできます。

すべてのiSCSIイニシエータは、ターゲットとのセッションまたは接続を確立する際に、発信元IPアドレスを提供する必要があります。この新機能は、発信元IPアドレスがサポート対象外または不明な場合にイニシエータがクラスタにログインできないようにすることで、一意の識別方式を提供します。サポート対象外または不明なIPアドレスから発信されたイニシエータではログインがiSCSIセッションレイヤで拒否されるため、イニシエータはクラスタ内のLUNまたはボリュームにアクセスできません。

既存のエントリの管理に役立つ2つの新しいコマンドを使用して、この新機能を実装します。

イニシエータのアドレス範囲を追加する

iSCSIイニシエータのセキュリティ管理を改善するには、IPアドレスの範囲を追加するか、コマンドを使用して複数のIPアドレスを追加し `vserver iscsi security add-initiator-address-range`ます。

```
cluster1::> vserver iscsi security add-initiator-address-range
```

イニシエータのアドレス範囲を削除する

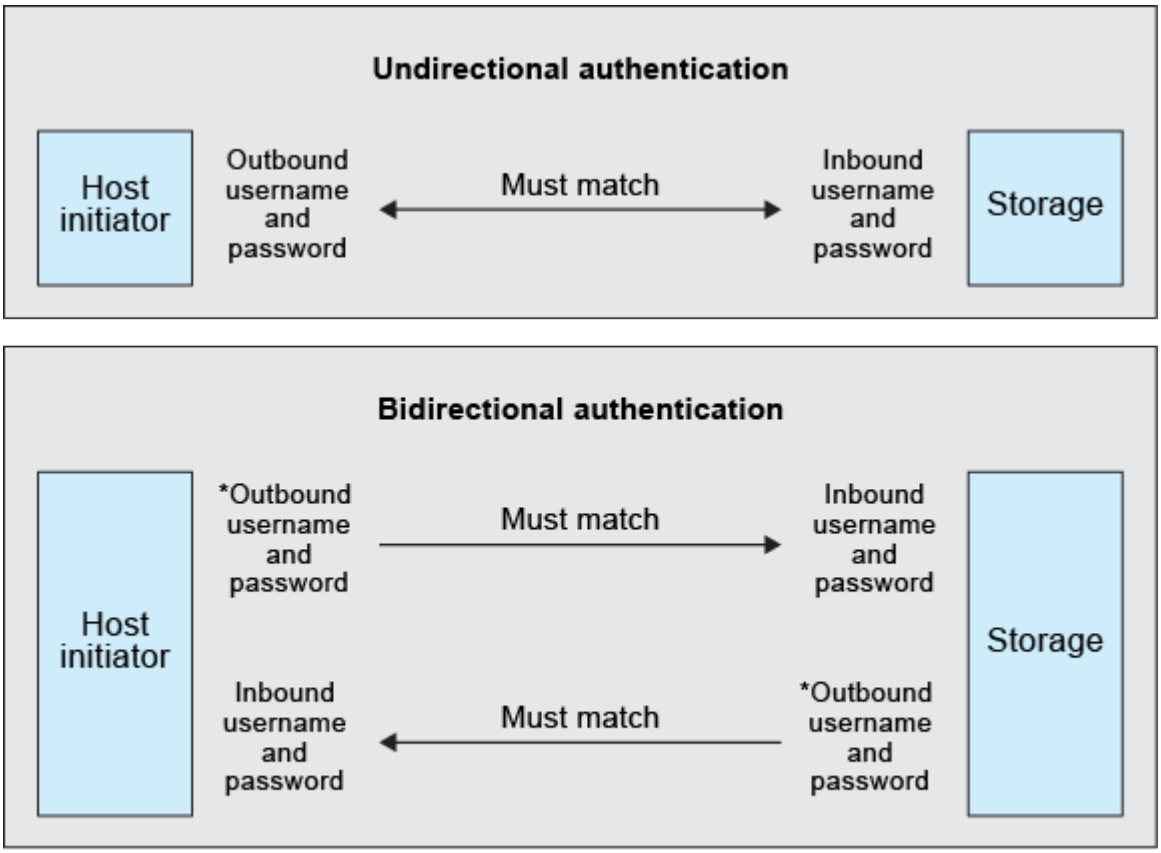
IPアドレスの範囲または複数のIPアドレスを削除するには、コマンドを使用し `vserver iscsi security remove-initiator-address-range`ます。

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

ONTAPの iSCSI イニシエータの CHAP 認証について学習します

Challenge Handshake Authentication Protocol（CHAP）を使用すると、iSCSIイニシエータとターゲット間の認証された通信が可能CHAP認証を使用する場合は、イニシエータとストレージシステムの両方でCHAPユーザ名とパスワードを定義します。

iSCSIセッションの第1段階では、イニシエータがストレージシステムにログイン要求を送信してセッションを開始します。ログイン要求には、イニシエータのCHAPユーザ名とCHAPアルゴリズムが含まれます。ストレージシステムはCHAPチャレンジで応答します。イニシエータはCHAP応答を提供します。ストレージシステムは応答を検証し、イニシエータを認証します。CHAPパスワードは、応答の計算に使用されます。



認証	アウトバウンド	インバウンド	マッチ？
単方向	ホストイニシエーターのユーザー名とパスワード	ストレージのユーザー名とパスワード	一致する必要があります
双方向	ホストイニシエーターのユーザー名とパスワード	ストレージのユーザー名とパスワード	一致する必要があります
双方向	ストレージのユーザー名とパスワード	ホストイニシエーターのユーザー名とパスワード	一致する必要があります

ホスト イニシエーターのアウトバウンド ユーザー名とパスワードは、ストレージ システムのアウトバウンド ユーザー名とパスワードとは異なる必要があります。

CHAP認証の使用に関するガイドライン

CHAP 認証を使用する場合は、次のガイドラインに従ってください。

- インバウンドユーザ名とパスワードをストレージシステムで定義する場合は、イニシエータのアウトバウンドCHAP設定にも同じユーザ名とパスワードを使用する必要があります。ストレージシステムでアウトバウンドユーザ名とパスワードも定義して双方向認証を有効にする場合は、イニシエータのインバウンドCHAP設定にも同じユーザ名とパスワードを使用する必要があります。
- ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名とパスワードを使用できません。
- CHAPユーザ名には1~128バイトを指定できます。

  システムでは null ユーザー名は許可されません。

- CHAPパスワード（secrets）には1~512バイトを指定できます。

  パスワードには16進値または文字列を使用できます。16 進数値の場合は、プレフィックス「`0x`」または「`0X`」を付けて値を入力する必要があります。

  システムでは null パスワードは許可されません。

ONTAPでは'CHAPパスワード（シークレット）に特殊文字'英語以外の文字'数字'およびスペースを使用できますただし、これはホストの制限の対象となります。これらのいずれかが特定のホストで許可されていない場合、それらを使用することはできません。

たとえば、Microsoft iSCSIソフトウェアイニシエータでは、IPsec暗号化を使用しない場合、イニシエータとターゲットの両方のCHAPパスワードを12バイト以上にする必要があります。パスワードの最大長は、IPsecが使用されているかどうかに関係なく16バイトです。

追加の制限については、イニシエーターのドキュメントを参照してください。

iSCSIインターフェイスアクセスリストを使用したイニシエータインターフェイスの制限によるパフォーマンスとセキュリティの向上

iSCSI インターフェイスアクセスリストを使用して、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。これにより、パフォーマンスとセキュリティが向上

します。

イニシエータがiSCSIコマンドを使用して検出セッションを開始すると、アクセスリストにあるLIF（ネットワークインターフェイス）に関連付けられたIPアドレスがイニシエータ `SendTargets`に渡されます。デフォルトでは、すべてのイニシエータが SVM 内のすべての iSCSI LIF にアクセスできます。アクセスリストを使用すると、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。

ONTAPのインターネットストレージネームサービス（iSNS）

Internet Storage Name Service（iSNS）は、TCP / IPストレージネットワーク上のiSCSIデバイスの自動検出と管理を可能にするプロトコルです。iSNSサーバでは、ネットワーク上でアクティブなiSCSIデバイスに関する情報（IPアドレス、iSCSIノード名IQN、ポータルグループなど）が維持されます。

iSNSサーバはサードパーティベンダーから入手できます。ネットワーク内に iSNS サーバがあり、イニシエータとターゲットで使用するように設定および有効化されている場合、 Storage Virtual Machine （ SVM ）の管理 LIF を使用して、その SVM のすべての iSCSI LIF を iSNS サーバに登録できます。登録が完了すると、 iSCSI イニシエータは iSNS サーバを照会して、その SVM のすべての LIF を検出できるようになります。

iSNSサービスを使用する場合は、Storage Virtual Machine（SVM）をInternet Storage Name Service（iSNS）サーバに適切に登録する必要があります。

ネットワークにiSNSサーバがない場合は、各ターゲットがホストから認識できるように手動で設定する必要があります。

iSNSサーバの機能

iSNSサーバは、Internet Storage Name Service（iSNS）プロトコルを使用して、ネットワーク上のアクティブなiSCSIデバイスに関する情報（IPアドレス、iSCSIノード名（IQN）、ポータルグループなど）を維持します。

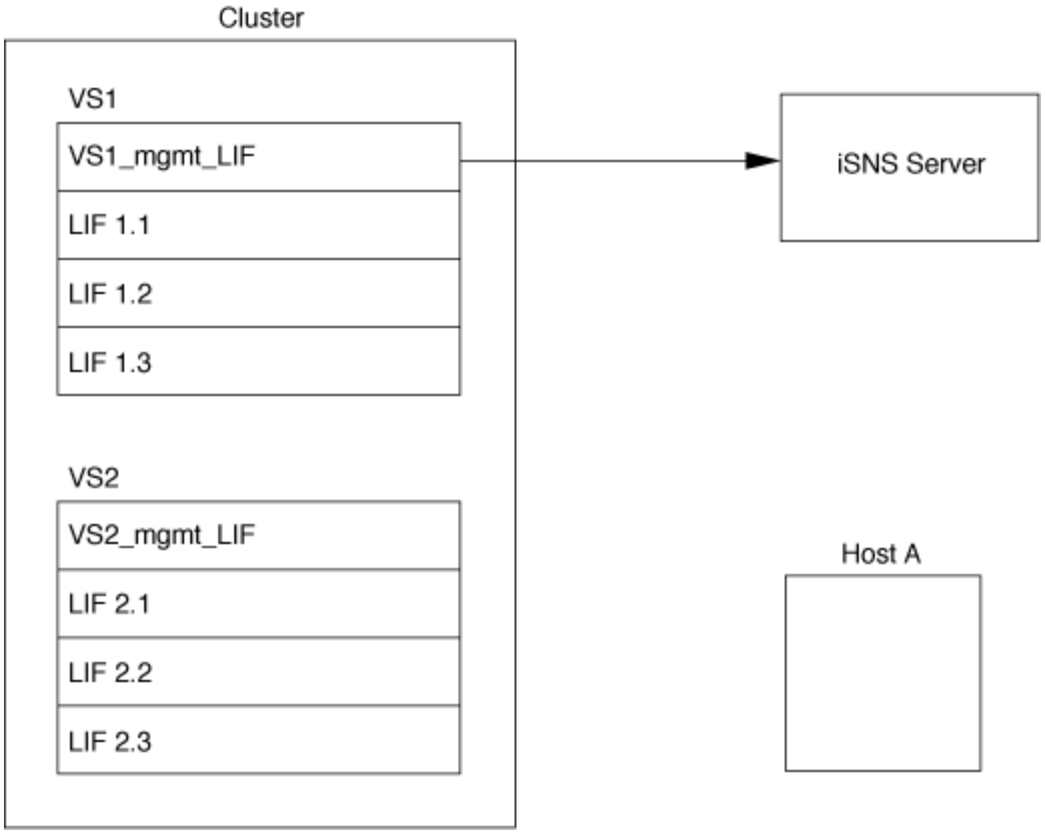
iSNSプロトコルを使用すると、IPストレージネットワーク上のiSCSIデバイスの自動検出と管理が可能になります。iSCSIイニシエータは、iSNSサーバに照会してiSCSIターゲットデバイスを検出できます。

NetAppでは、iSNSサーバの提供や再販は行われません。これらのサーバは、NetAppでサポートされているベンダーから入手できます。

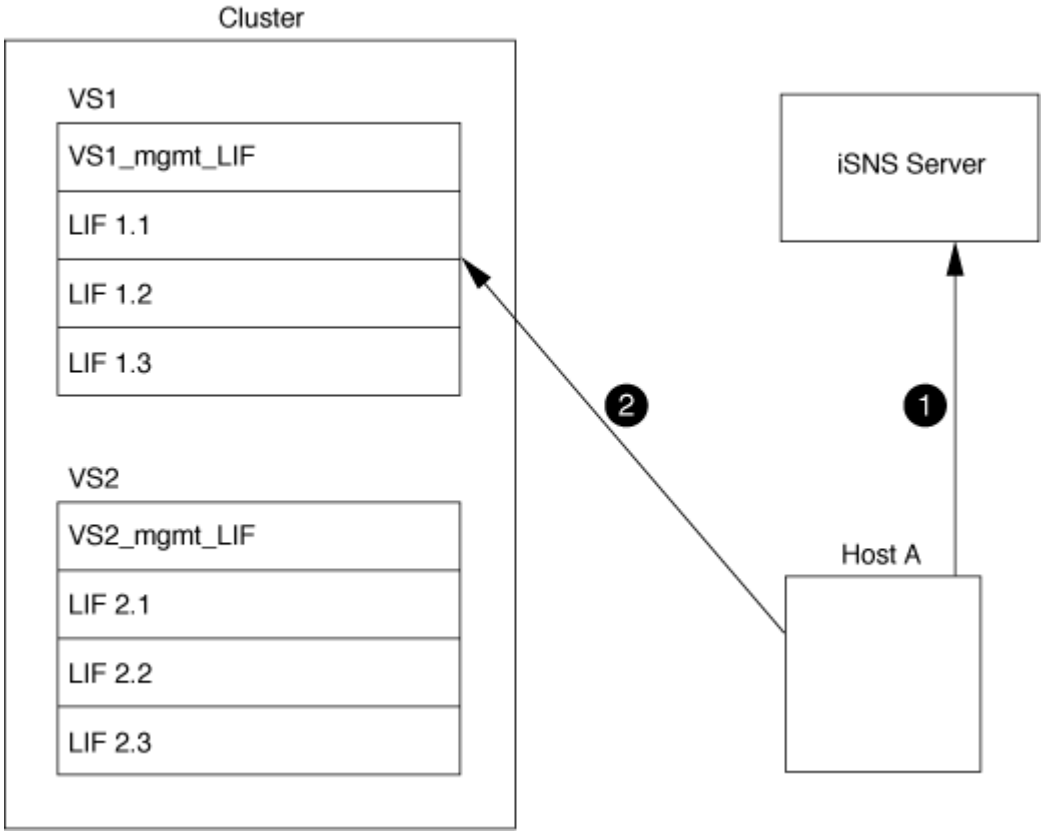
SVMとiSNSサーバの連動

iSNS サーバは、 Storage Virtual Machine （ SVM ）の管理 LIF を介して各 SVM と通信します。管理 LIF は、特定の SVM のすべての iSCSI ターゲットのノード名、エイリアス、およびポータル情報を iSNS サーバに登録します。

次の例では、SVM「VS1」はSVM管理LIF「VS1_mgmt_LIF'」を使用してiSNSサーバに登録しています。iSNS に登録中、 SVM はすべての iSCSI LIF を SVM 管理 LIF を介して iSNS サーバに送信します。iSNSの登録が完了すると、iSNSサーバには「VS1」でiSCSIを提供するすべてのLIFのリストが格納されます。クラスタに複数のSVMが含まれている場合は、iSNSサービスを使用するために、各SVMを個別にiSNSサーバに登録する必要があります。



次の例では、iSNSサーバによるターゲットへの登録が完了すると、ホストAがiSNSサーバを介して「VS1」のすべてのLIFを検出できるようになります（手順1を参照）。ホストAが「VS1」のLIFの検出を完了すると、ホストAは「VS1」の任意のLIFとの接続を確立できます（手順2を参照）。「VS2」の管理LIF「VS2_mgmt_LIF」がiSNSサーバに登録されるまで、ホストAは「VS2」内のLIFを認識しません。



ただし、インターフェイスアクセスリストを定義した場合、ホストはインターフェイスアクセスリストに定義されているLIFのみを使用してターゲットにアクセスできます。

一度 iSNS が設定されると、 SVM の設定を変更するたびに ONTAP によって iSNS サーバが自動的に更新されます。

設定を変更してからONTAPからiSNSサーバに更新情報が送信されるまでには、数分程度の遅れが生じる可能性があります。iSNSサーバのiSNS情報を強制的に更新します。 `vserver iscsi isns update`の詳細については `vserver iscsi isns update`、を"ONTAPコマンド リファレンス"参照してください。

iSNSの管理用コマンド

ONTAPには、iSNSサービスを管理するためのコマンドが用意されています。

状況	使用するコマンド
iSNSサービスを設定する	`vserver iscsi isns create`
iSNSサービスを開始する	`vserver iscsi isns start`
iSNSサービスを変更する	`vserver iscsi isns modify`
iSNSサービス設定を表示します。	`vserver iscsi isns show`
登録済みのiSNS情報を強制的に更新します。	`vserver iscsi isns update`
iSNSサービスを停止する	`vserver iscsi isns stop`
iSNSサービスを削除する	`vserver iscsi isns delete`
コマンドのマニュアルページを表示する	`man` *`command name`*

の詳細については `vserver iscsi isns`、を"ONTAPコマンド リファレンス"参照してください。

FCを使用したSANプロビジョニング

ONTAP で FC SAN を実装する方法について理解する際に必要となる重要な概念について説明します。

FCターゲットノードをネットワークに接続する方法

ストレージシステムとホストにはアダプタが搭載されているため、ケーブルを使用してFCスイッチに接続できます。

ノードを FC SAN に接続すると、各 SVM の LIF の World Wide Port Name （ WWPN ；ワールドワイドポート名）がスイッチのファブリックネームサービスに登録されます。SVM の WWNN と各 LIF の WWPN は、ONTAP によって自動的に割り当てられます。

FCを使用してホストからノードに直接接続することはできません。NPIVが必要なため、スイッチを使用する必要があります。iSCSIセッションでは、通信はネットワークルーティングされた接続または直接接続された接続で機能します。ただし、これらの方法はどちらもONTAPでサポートされています。

FCノードの識別方法

FCが設定された各SVMは、World Wide Node Name（WWNN；ワールドワイドノード名）で識別されます。

WWPNの使用方法

WWPN により、 FC をサポートするように設定されている SVM 内の各 LIF が識別されます。これらのLIFは、クラスタ内の各ノードの物理FCポート（ノードでFCまたはFCoEとして設定されたFCターゲットカード、UTA、またはUTA2）を使用します。

- igroupの作成

  ホストのHBAのWWPNは、イニシエータグループ（igroup）の作成に使用されます。igroupは、特定のLUNへのホストアクセスの制御に使用されます。igroupを作成するには、FCネットワーク内のイニシエータの一連のWWPNを指定します。ストレージシステム上のLUNをigroupにマッピングすると、そのグループ内のすべてのイニシエータに、そのLUNへのアクセスを許可できます。ホストのWWPNがLUNにマッピングされたigroupに含まれていない場合、そのホストはLUNにアクセスできません。つまり、LUNはそのホストではディスクとして表示されません。

  また、ポートセットを作成して、特定のターゲットポートでのみLUNが認識されるようにすることもできます。ポートセットは、FCターゲットポートをグループ化したものです。igroupはポートセットにバインドできます。igroup内のすべてのホストは、ポートセット内のターゲットポートからのみLUNにアクセスできます。

- FC LIFを一意に識別

  WWPNはFC論理インターフェイスを一意に識別します。ホストオペレーティングシステムでは、WWNNとWWPNを組み合わせて使用してSVMとFC LIFを識別します。一部のオペレーティングシステムでは、ホスト上でLUNが同じターゲットIDで表示されるようにするためにパーシスタントバインディングが必要です。

World Wide Nameの割り当ての仕組み

WWNは、ONTAPでシーケンシャルに作成されます。ただし、ONTAPによる割り当て方法が原因で、シーケンシャルではない順序で割り当てられているように見える場合があります。

各アダプタにはWWPNとWWNNが事前に設定されていますが、ONTAPでは事前設定された値は使用されません。代わりに、ONTAPはオンボードイーサネットポートのMACアドレスに基づいて、独自のWWPNまたはWWNNを割り当てます。

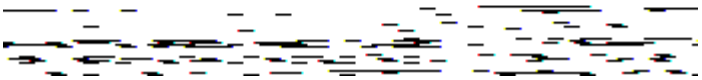
WWNが割り当て時にシーケンシャルでないように見える理由は次のとおりです。

- WWN は、クラスタ内のすべてのノードと Storage Virtual Machine （ SVM ）で一意に割り当てられます。
- 解放されたWWNはリサイクルされ、使用可能な名前のプールに再び追加されます。

FCスイッチの識別方法

Fibre Channelスイッチには、デバイス自体に1つのWorld Wide Node Name（WWNN；ワールドワイドノード名）、デバイスの各ポートに1つのWorld Wide Port Name（WWPN；ワールドワイドポート名）があります。

たとえば、次の図は、16ポートBrocadeスイッチの各ポートにWWPNがどのように割り当てられているかを示しています。特定のスイッチのポート番号の詳細については、そのスイッチに対応するベンダー提供のマニュアルを参照してください。



ポート* 0 *、WWPN 20： **00** ：00：60：69：51：06：b4

ポート * 1 * 、 WWPN 20 ： **01** 00 ： 60 ： 69 ： 51 ： 06 ： b4

ポート * 14 * 、 WWPN 20 ： **0e** ： 00 ： 60 ： 69 ： 51 ： 06 ： B4

ポート * 15 * 、 WWPN 20 ： **0f** ： 00 ： 60 ： 69 ： 51 ： 06 ： B4

NVMeを使用したSANプロビジョニング

SAN.4以降では、ONTAP 9環境でNVMe/FCがサポートされます。NVMe/FCでは、FCおよびiSCSIでLUNをプロビジョニングしてigroupにマッピングするのと同じように、ネームスペースとサブシステムをプロビジョニングし、ネームスペースをサブシステムにマッピングできます。

NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリの容量です。ネームスペースはFCプロトコルやiSCSIプロトコルのLUNに相当し、NVMeサブシステムはigroupに相当します。NVMeサブシステムはイニシエータに関連付けることができます。これにより、サブシステム内のネームスペースに関連付けられたイニシエータがアクセスできるようになります。

NVMeネームスペースは機能に似ていますが、LUNでサポートされるすべての機能がサポートされるわけではありません。

ONTAP 9 .5以降では、NVMeによるホスト側のデータアクセスをサポートするにはライセンスが必要です。ONTAP 9でNVMeが有効になっている場合は、ONTAP 9にアップグレードしたあと90日間の猶予期間が与えられます。5.を使用している場合は"ONTAP One"、NVMeライセンスが含まれます。ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

関連情報

"NetAppテクニカルレポート4684：『Implementing and Configuring Modern SANs with NVMe/FC』"

SANホリユウム

SANボリュームについて

ONTAPには、基本的なボリュームプロビジョニングオプションとして、シックプロビジョニング、シンプロビジョニング、セミシックプロビジョニングの3つが用意されています。各オプションでは、ボリュームスペースおよびONTAPブロック共有テクノロジのスペース要件がさまざまな方法で管理されます。これらのオプションの仕組みを理解することで、環境に最も適したオプションを選択できるようになります。

> SAN LUNとNAS共有を同じFlexVol volumeに配置することは推奨されません。SAN LUN用とFlexVol NAS共有用にそれぞれ別 々 のFlexVolボリュームをプロビジョニングする必要があります。これにより、管理とレプリケーションの導入が簡易化され、Active IQ Unified Manager（旧OnCommand Unified Manager）でのFlexVolボリュームのサポート方法と同様に機能します。

ボリュームのシンプロビジョニング

シンプロビジョニング ボリュームは、作成時に追加のスペースが確保されません。ボリュームにデータが書き込まれるときに、書き込み処理に対応するために必要なアグリゲート内のストレージをボリュームが要求します。シンプロビジョニング ボリュームを使用する場合はアグリゲートをオーバーコミットできますが、アグリゲートの空きスペースが不足すると、必要なスペースをボリュームが確保できなくなる可能性があります。

シンプロビジョニングFlexVol volumeを作成するには、そのオプションをに `none`設定し `-space-guarantee`ます。

ボリュームのシックプロビジョニング

シックプロビジョニングは、ボリューム内のブロックにいつでも書き込むことができるように、作成時にアグリゲートから十分なストレージが確保されます。シックプロビジョニングを利用するようにボリュームを設定した場合は、ONTAPの任意のStorage Efficiency機能（圧縮や重複排除など）を使用して、さらに大容量のストレージ要件にも事前に対応できます。

シックプロビジョニングFlexVol volumeを作成するには、その（サービスレベル目標）オプションをに `thick`設定し `-space-slo`ます。

ボリュームのセミシックプロビジョニング

セミシックプロビジョニングを使用するボリュームを作成すると、ONTAPはボリュームサイズに対応するためにアグリゲートからストレージスペースを確保します。ブロック共有テクノロジでブロックが使用されているためにボリュームの空きスペースが不足している場合、ONTAPは保護データオブジェクト（Snapshot、FlexCloneファイルおよびLUN）を削除して保持しているスペースを解放します。上書きに必要なスペースを確保できる速度でONTAPが保護データオブジェクトを削除できるかぎり、書き込み処理は引き続き成功します。これは「ベストエフォート」書き込み保証と呼ばれます。

- 注： * セミシックプロビジョニングを使用するボリュームでは、次の機能はサポートされていません。
- 重複排除、圧縮、コンパクションなどのStorage Efficiencyテクノロジ
- Microsoftオフロードデータ転送（ODX）

セミシックプロビジョニングFlexVol volumeを作成するには、その（サービスレベル目標）オプションをに

`semi-thick`設定し `-space-slo`ます。

スペースリザーブファイルおよびスペースリザーブ**LUN**での使用

スペースリザーブファイルまたはスペースリザーブLUNは、ストレージの作成時にストレージが割り当てられるファイルまたはLUNです。ネットアップではこれまで、スペース・リザベーションが無効になっているLUN （スペース・リザーブなしの LUN ）を「シン・プロビジョニング LUN 」と呼んできました。

- 注意： * スペースリザーブなしのファイルは、一般的に「シンプロビジョニングされたファイル」とは呼ばれません。

次の表に、スペースリザーブファイルおよびスペースリザーブLUNで使用できる3つのボリュームプロビジョニングオプションの主な違いを示します。

ボリュームのプロビジョニング	**LUN/file** のスペースリザベーション	上書き	保護データ [2]	ストレージ効率 [3]
シック	サポート対象	保証された ^1	保証	サポート対象
シン	効果なし	なし	保証	サポート対象
セミシック	サポート対象	ベストエフォート ^1 ^	ベストエフォート	サポート対象外

- メモ *

1. 上書きを保証したり、ベストエフォートで上書きを保証できるようにするには、LUNまたはファイルでスペースリザベーションが有効になっている必要があります。
2. 保護データには、Snapshot、自動削除の対象としてマークされたFlexCloneファイルおよびLUN（バックアップクローン）が含まれます。
3. Storage Efficiencyには、重複排除、圧縮、自動削除の対象としてマークされていないFlexCloneファイルとLUN（アクティブクローン）、およびFlexCloneサブファイル（コピーオフロードに使用）が含まれます。

SCSIシンプロビジョニング**LUN**のサポート

ONTAPは、T10 SCSIシンプロビジョニングLUNとNetAppシンプロビジョニングLUNをサポートしています。T10 SCSIシンプロビジョニングを使用すると、ホストアプリケーションは、ブロック環境向けのLUNのスペース再生機能やスペース監視機能などのSCSI機能をサポートできます。T10 SCSIシンプロビジョニングがSCSIホストソフトウェアでサポートされている必要があります。

LUNのT10シンプロビジョニングのサポートを有効または無効にするには、ONTAP設定を使用し `space-allocation`ます。ONTAPの設定を使用し `space-allocation enable`て、LUNでT10 SCSIシンプロビジョニングを有効にします。

その `[-space-allocation {enabled|disabled}]`コマンドの"ONTAPコマンド リファレンス" T10 シン プロビジョニングのサポートを有効/無効にする方法、および LUN で T10 SCSI シン プロビジョニングを有効にする方法については、さらに詳しい情報があります。

ボリュームにシンプロビジョニング、シックプロビジョニング、またはセミシックプロビジョニングを設定できます。

タスクの内容

このオプションをに `thick`設定する `-space-slo`と、次の処理が実行されます。

- ボリューム全体がアグリゲートに事前に割り当てられます。コマンドまたは `volume modify`コマンドを使用してボリュームのオプションを設定する `-space-guarantee`ことはできません `volume create`。
- 上書きに必要なスペースの100%がリザーブされます。コマンドを使用してボリュームのオプションを設定する `-fractional-reserve`ことはできません。 `volume modify`

このオプションをに `semi-thick`設定する `-space-slo`と、次の処理が実行されます。

- ボリューム全体がアグリゲートに事前に割り当てられます。コマンドまたは `volume modify`コマンドを使用してボリュームのオプションを設定する `-space-guarantee`ことはできません `volume create`。
- スペースは上書き用にリザーブされません。コマンドを使用して、ボリュームのオプションを設定 `-fractional-reserve`できます `volume modify`。
- Snapshotの自動削除が有効になります。

ステップ

1. ボリュームのプロビジョニングオプションを設定します。

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   AFFシステムおよびAFF以外のDPボリュームでは、この `-space-guarantee`オプションのデフォルトはです `none`。それ以外の場合は、デフォルトでになり `volume`ます。既存のFlexVolボリュームの場合は、コマンドを使用し `volume modify`てプロビジョニングオプションを設定します。

   次のコマンドを使うと、 SVM vs1 上の vol1 にシンプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   次のコマンドを使うと、 SVM vs1 上の vol1 にシックプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   次のコマンドを使うと、 SVM vs1 上の vol1 にセミシックプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

SANボリュームの構成オプション

LUNを含むボリュームにさまざまなオプションを設定する必要があります。ボリュームオプションの設定方法によって、ボリューム内のLUNで使用できるスペースの量が決まります。

自動拡張

自動拡張は有効または無効にすることができます。有効にすると、ONTAPでボリュームのサイズを事前に設定した最大サイズまで自動的に拡張できます。ボリュームの自動拡張をサポートするには、使用可能なスペースを包含アグリゲートに確保する必要があります。そのため、自動拡張を有効にする場合は、包含アグリゲートの空きスペースを監視し、必要に応じて追加してください。

自動拡張をトリガーしてSnapshotの作成をサポートすることはできません。自動拡張が有効になっていても、ボリュームに十分なスペースがないとSnapshotの作成は失敗します。

自動拡張が無効な場合、ボリュームのサイズに変更はありません。

自動縮小

自動縮小は有効または無効にすることができます。有効にすると、ボリュームで消費されるスペースの量が事前に設定したしきい値を下回った場合に、ONTAPでボリューム全体のサイズを自動的に縮小できます。これにより、ボリュームで未使用の空きスペースの自動的な解放が開始されて、ストレージ効率が向上します。

Snapshotの自動削除

Snapshotの自動削除では、次のいずれかの状況が発生すると、Snapshotが自動的に削除されます。

- ボリュームがフルに近い状態の場合
- Snapshotリザーブスペースがほぼフルです。
- オーバーライトリザーブスペースがフルです。

古いものから新しいもの、または新しいものから順にSnapshotを削除するようにSnapshotの自動削除を設定できます。Snapshotの自動削除では、クローンボリュームまたはLUN内のSnapshotにリンクされているSnapshotは削除されません。

自動拡張とSnapshotの自動削除の両方が有効になっている場合にボリュームで追加のスペースが必要になると、デフォルトでは、ONTAPは最初に自動拡張をトリガーして、必要なスペースを確保しようとします。自動拡張で十分なスペースが確保されない場合は、Snapshotの自動削除がトリガーされます。

Snapshotリザーブ

Snapshotリザーブは、Snapshot用にリザーブされるボリューム内のスペースの量を定義します。Snapshotリザーブに割り当てられたスペースを他の目的に使用することはできません。スナップショット予約用に割り当てられたすべての領域が使用されると、スナップショットはボリューム上の追加の領域を消費し始めます。

SAN環境でのボリューム移動に関する要件

LUN またはネームスペースを含むボリュームを移動する場合は、一定の要件を満たす必要があります。

- ボリュームに 1 つ以上の LUN が含まれている場合は、クラスタ内の各ノードに接続する LUN （ LIF ）ごとに少なくとも 2 つのパスが必要です。

  これにより、単一点障害（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

- ボリュームにネームスペースが含まれている場合は、クラスタで ONTAP 9.6 以降が実行されている必要があります。

  ボリューム移動は、ONTAP 9を実行するNVMe構成ではサポートされません。5.

フラクショナルリザーブの設定に関する考慮事項

フラクショナルリザーブは、 _lun overwrite reserve _ とも呼ばれ、 FlexVol ボリューム内のスペースリザーブ LUN およびファイルのオーバーライトリザーブを無効にすることができます。これはストレージ利用率を最大限に高めるのに役立ちますが、スペース不足による書き込み処理の失敗が悪影響を及ぼす環境では、この構成に伴う要件を理解しておく必要があります。

フラクショナルリザーブ設定はパーセンテージで表され、有効な値は `0`と `100`パーセントのみです。フラクショナルリザーブ設定はボリュームの属性です。

フラクショナルリザーブを設定して `0`ストレージ利用率を高めます。ただし、ボリュームの空きスペースがなくなると、ボリュームギャランティがに設定されていても、ボリュームに格納されたデータにアクセスするアプリケーションでデータを利用できなくなる可能性があります `volume`。ただし、ボリュームを適切に構成して使用すれば、書き込みが失敗する可能性を最小限に抑えることができます。 `0`次の要件の_all_が満たされている場合、ONTAPはフラクショナルリザーブがに設定されたボリュームに対して「ベストエフォート」書き込み保証を提供します。

- 重複排除を使用していない
- 圧縮を使用していない
- FlexCloneサブファイルは使用されていません
- すべてのFlexCloneファイルとFlexClone LUNで自動削除が有効になっている

  これはデフォルト設定ではありません。FlexCloneファイルやFlexClone LUNの自動削除は、作成時に設定するか作成後に変更して明示的に有効にする必要があります。

- ODXコピー オフロードとFlexCloneコピー オフロードを使用していない
- ボリュームギャランティがに設定されている `volume`
- ファイルまたはLUNのスペースリザベーション： `enabled`
- ボリュームのSnapshotリザーブの設定： `0`
- ボリュームSnapshotの自動削除は `enabled`、コミットメントレベルが、 `destroy`削除リストが、

`lun_clone,vol_clone,cifs_share,file_clone,sfsr`トリガーが `volume

この設定では、必要に応じてFlexCloneファイルとFlexClone LUNも削除されます。

変更率が高いと、上記の必要な設定をすべて使用していても、まれにSnapshotの自動削除が遅れてボリュームのスペースが不足することがあります。

また、必要に応じてボリュームの自動拡張機能を使用することで、ボリュームSnapshotが自動的に削除される可能性を減らすことができます。自動拡張機能を有効にする場合は、関連付けられたアグリゲートの空きスペースを監視する必要があります。アグリゲートの空きスペースがなくなり、ボリュームを拡張できなくなると、ボリュームの空きスペースが不足したときに削除されるSnapshotが増える可能性があります。

上記の設定要件をすべて満たすことができず、ボリュームのスペース不足を防ぐ必要がある場合は、ボリュームのフラクショナルリザーブ設定をに設定する必要があります `100`。これにより、事前に確保する必要がある空きスペースは増えますが、上記のテクノロジを使用する場合でもデータ変更処理が確実に実行されるようになります。

フラクショナル リザーブ設定のデフォルト値と有効値は、ボリュームのギャランティによって異なります。

ボリュームギャランティ	デフォルトのフラクショナルリザーブ	有効な値
ボリューム	100	0、100
なし	0	0、100

SANホスト側のスペース管理

シンプロビジョニング環境では、ホストファイルシステムで解放されたスペースをストレージシステムから管理するプロセスを、ホスト側のスペース管理によって実行します。

ホストファイルシステムには、新しいデータの格納に使用できるブロックと、上書きしてはならない有効なデータが含まれているブロックを追跡するためのメタデータが含まれています。このメタデータはLUNまたはネームスペース内に格納されます。ホストファイルシステムでファイルが削除されると、ファイルシステムのメタデータが更新され、そのファイルのブロックが空きスペースとしてマークされます。ファイルシステム内の合計空きスペースが再計算され、新しく解放されたブロック分のスペースが組み入れられます。一方、ストレージ システム側では、こうしたメタデータの更新が、ホストによって実行される他の書き込みとまったく相違ないものとして認識されます。このため、ストレージ システム側では、削除が行われた事実が検知されません。

その結果、ホスト側と基盤のストレージ システム側で報告される空きスペース容量に不一致が生じます。たとえば、新しくプロビジョニングされた200GBのLUNがストレージ システムによってホストに割り当てられているとします。この場合、ホストとストレージ システムの双方で、200GBの空きスペースが報告されます。ここでホストに100GBのデータが書き込まれた場合、この時点では、ホストもストレージ システムも、使用済みスペースが100GB、未使用スペースが100GBと報告します。

次に、ホストから50GBのデータが削除されました。このとき、ホスト側では使用済みスペースが50GB、未使用スペースが150GBであると報告されます。一方、ストレージ システム側で報告される数値は、依然として使用済みスペース100GB、未使用スペース100GBとなります。

ホスト側のスペース管理では、さまざまな方法を使用して、ホストとストレージ システム間のスペースの差分を調整します。

SnapCenterによるホスト管理の簡易化

SnapCenterソフトウェアを使用すると、iSCSIストレージやFCストレージに関連する管理作業とデータ保護作業を簡単に行うことができます。SnapCenterは、WindowsとUNIXホストに対応するオプションの管理パッケージです。

SnapCenterソフトウェアを使用すると、複数のストレージシステムに分散できるストレージプールから仮想ディスクを簡単に作成できます。また、ストレージプロビジョニングタスクを自動化し、ホストデータと整合性のあるスナップショットおよびスナップショットからのクローンの作成プロセスを簡易化できます。

の詳細については、NetAppの製品ドキュメントを参照してください "SnapCenter"。

関連リンク

"SANプロトコルのONTAPスペース割り当てを有効にする"

igroupについて

イニシエータグループ（igroup）は、FCプロトコルホストWWPNまたはiSCSIホストノード名のテーブルです。igroupを定義してLUNにマッピングすることで、どのイニシエータがLUNにアクセスできるかを制御できます。

通常は、ホストのすべてのイニシエータポートまたはソフトウェアイニシエータがLUNにアクセスできることが必要です。マルチパスソフトウェアを使用している場合、またはクラスタホストがある場合は、各イニシエータポートまたは各クラスタホストのソフトウェアイニシエータが同じLUNへの冗長パスを必要とします。

LUNにアクセスできるイニシエータを指定するigroupは、LUNの作成前または作成後に作成できますが、LUNをigroupにマッピングする前にigroupを作成する必要があります。

イニシエータグループには複数のイニシエータを含めることができ、複数のigroupに同じイニシエータを含めることができます。ただし、イニシエータが同じ複数のigroupに1つのLUNをマッピングすることはできません。1つのイニシエータを、ostypeが異なる複数のigroupのメンバーにすることはできません。

igroupによる**LUN**アクセスの提供例

複数のigroupを作成して、ホストで使用できるLUNを定義できます。たとえば、ホストクラスタを使用している場合、複数のigroupを使用して、クラスタ内の1つのホストだけ、またはすべてのホストから特定のLUNが認識されるように設定できます。

次の表は、ストレージシステムにアクセスしている4つの異なるホストについて、4つのigroupによってLUNにアクセスできるようにする方法を示しています。クラスタ化されたホスト（Host3とHost4）は、両方とも同じigroup（group3）のメンバーであり、このigroupにマッピングされたLUNにアクセスできます。group4というigroupにはHost4のWWPNが含まれ、パートナーには表示されないローカルの情報が格納されます。

HBA WWPN 、 **IQN** 、または **EUI** のホスト	**igroup**	**igroup** に追加されている **WWPN** 、 **IQN** 、 **EUI**	**igroup** にマッピングされている **LUN**
Host1、シングルパス（iSCSIソフトウェアイニシエータ） iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2、マルチパス（HBA×2） 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3、マルチパス、Host4でクラスタ構成 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
Host4、マルチパス、クラスタ構成（Host3には認識されない） 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

igroupのイニシエータのWWPNとiSCSIノード名を指定する

イニシエータのiSCSIノード名およびWWPNは、igroupの作成時に指定することも、あとから追加することもできます。LUNの作成時にイニシエータのiSCSIノード名とWWPNを指定するように選択した場合は、必要に応じてあとで削除できます。

Host Utilitiesのマニュアルの手順に従って、WWPNを取得し、特定のホストに関連付けられているiSCSIノード名を確認します。ESXソフトウェアを実行するホストでは、Virtual Storage Consoleを使用します。

VMwareとMicrosoftのコピーオフロードによるストレージ仮想化

VMwareとMicrosoftのコピーオフロードによるストレージ仮想化の概要

VMwareとMicrosoftは、パフォーマンスとネットワークスループットを向上させるために、コピーオフロード処理をサポートしています。コピーオフロード機能を使用するには、VMwareとWindowsのオペレーティングシステム環境の要件を満たすようにシステ

ムを設定する必要があります。

仮想環境でVMwareとMicrosoftのコピーオフロードを使用する場合は、LUNをアライメントする必要があります。LUNをアライメントしないと、パフォーマンスが低下する可能性があります。

仮想**SAN**環境を使用する利点

Storage Virtual Machine（SVM）とLIFを使用して仮想環境を作成すると、SAN環境をクラスタ内のすべてのノードに拡張できます。

- 分散管理

  SVM内の任意のノードにログインして、クラスタ内のすべてのノードを管理できます。

- データアクセスの向上

  MPIOとALUAを使用すると、SVMのすべてのアクティブなiSCSI LIFまたはFC LIFを介してデータにアクセスできます。

- LUNアクセスの制御

  SLMとポートセットを使用すると、イニシエータがLUNへのアクセスに使用できるLIFを制限できます。

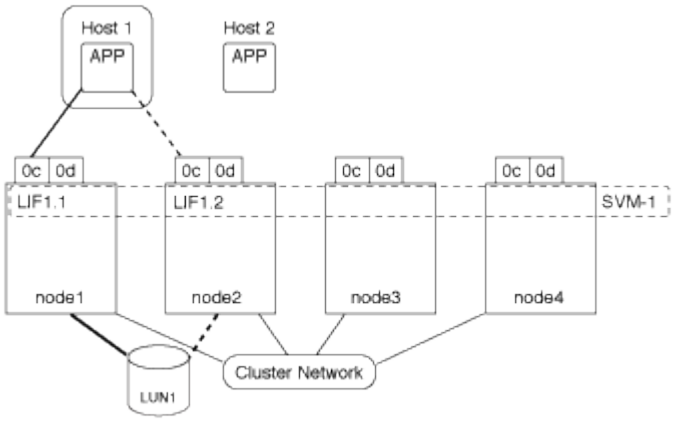
仮想環境での**LUN**へのアクセスの仕組み

仮想環境では、ホスト（クライアント）は LIF を使用して、最適パスおよび非最適パス経由で LUN にアクセスします。

LIF は、 SVM を物理ポートに接続する論理インターフェイスです。複数のSVMが同じポート上に複数のLIFを設定できますが、1つのLIFは1つのSVMに属します。LUNには、SVMのLIFを介してアクセスできます。

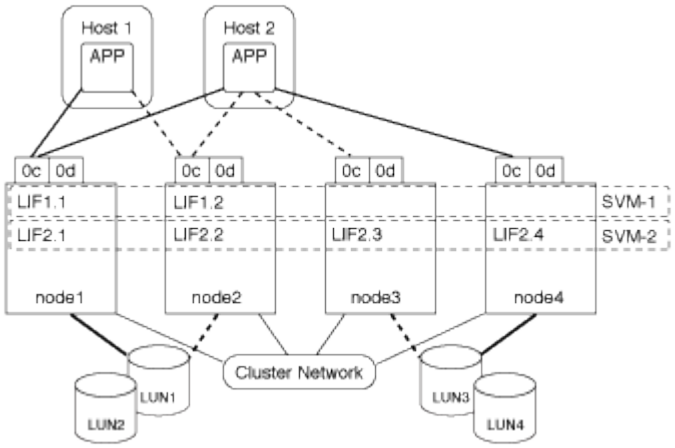
クラスタ内の**1**つの**SVM**を使用した**LUN**へのアクセス例

次の例では、ホスト1がSVM-1のLIF1.1とLIF1.2に接続してLUN1にアクセスします。LIF1.1 は物理ポート node1 ： 0c を、 LIF1.2 は node2 ： 0c を使用します。LIF1.1 と LIF1.2 は SVM-1 のみに属しています。SVM-1 のノード 1 またはノード 2 で新しい LUN を作成した場合は、その LUN でもこれらの同じ LIF を使用できます。新しい SVM を作成した場合は、両方のノードの物理ポート 0c または 0d を使用して新しい LIF を作成できます。



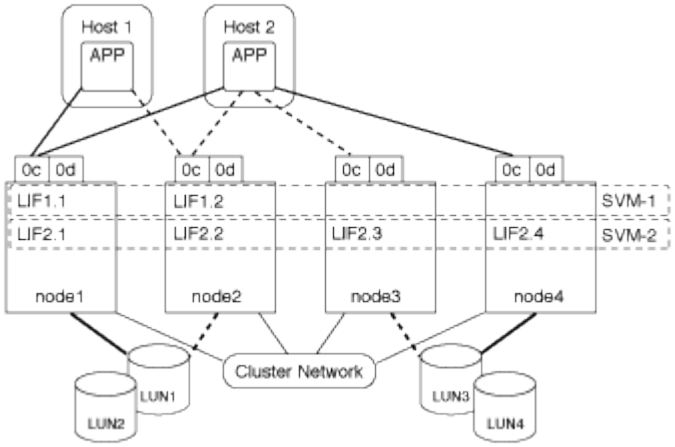
クラスタ内の複数の**SVM**を使用した**LUN**へのアクセス例

1つの物理ポートで複数のLIFをサポートし、異なるSVMを接続できます。LIF は特定の SVM に関連付けられているため、クラスタノードは受信データトラフィックを正しい SVM に送信できます。次の例では、 1~4 の各ノードに、各ノードの物理ポート 0c を使用して SVM-2 用の LIF を 1 つずつ設定しています。ホスト1はSVM-1のLIF1.1とLIF1.2に接続してLUN1にアクセスします。ホスト 2 は、 SVM-2 の LIF2.1 と LIF2.2 に接続して LUN2 にアクセスします。両方のSVMがノード1とノード2の物理ポート0cを共有しています。SVM-2 には追加の LIF があり、ホスト 2 はこの LIF を使用して LUN3 と LUN4 にアクセスします。これらの LIF はノード 3 とノード 4 の物理ポート 0c を使用します。複数のSVMでノードの物理ポートを共有できます。



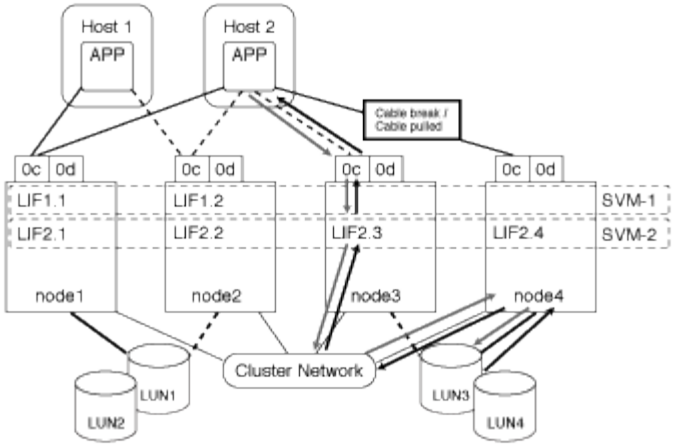
ホストシステムから**LUN**へのアクティブパスまたは最適パスの例

アクティブパスまたは最適パスでは、データトラフィックはクラスタネットワークを経由せずに、 LUN への最短ルートをとります。LUN1へのアクティブパスまたは最適パスは、物理ポート0cを使用して、ノード1のLIF1.1を経由します。ホスト 2 には、アクティブパスまたは最適パスが 2 つあります。 1 つは node1 へのパスで、 LIF2.1 は物理ポート 0c を共有し、もう 1 つは node4 、 LIF2.4 は物理ポート 0c を使用します。



ホストシステムから**LUN**へのアクティブパスまたは非最適（間接）パスの例

アクティブパスまたは非最適（間接）パスでは、データトラフィックはクラスタネットワークを経由します。この問題は、ホストからのアクティブパスまたは最適パスがすべて使用できず、トラフィックを処理できない場合にのみ発生します。ホスト 2 から SVM-2 LIF2.4 へのパスが失われた場合は、クラスタネットワークを経由して LUN3 と LUN4 にアクセスします。ホスト 2 からのアクセスには、ノード 3 の LIF2.3 が使用されます。トラフィックは、クラスタネットワークスイッチに入ったあと、 LUN3 と LUN4 にアクセスできるようノード 4 にバックアップされます。次に、クラスタネットワークスイッチ経由で逆方向に戻り、 LIF2.3 経由でホスト 2 にバックアウトされます。このアクティブパスまたは非最適パスは、 LIF2.4 へのパスがリストアされるか、ノード 4 のもう 1 つの物理ポートで SVM-2 の新しい LIF が確立されるまで使用されます。



ESXホストの**VMware VAAI**パフォーマンスの向上

ONTAP では、 ESX ホストで ESX 4.1 以降が実行されている場合、 VMware vStorage APIs for Array Integration （ VAAI ）の一部の機能がサポートされます。これらの機能は、ESXホストからストレージシステムに処理をオフロードし、ネットワークスループットを向上させるのに役立ちます。これらの機能は、適切な環境でESXホストによって自動的に有効になります。

VAAI 機能は、次の SCSI コマンドをサポートします。

- `EXTENDED_COPY`

  この機能により、ホストは、データ転送の際にホストに影響を与えることなく、 LUN 間または LUN 内のデータ転送を開始できます。その結果、 ESX CPU サイクルが節約され、ネットワークスループットが増加します。拡張コピー機能は「コピーオフロード」とも呼ばれ、仮想マシンのクローニングなどで使用されます。ESX ホストからコピーオフロード機能が呼び出されると、ホストネットワークを経由せずにストレージシステム内でデータがコピーされます。コピーオフロードでは、次の方法でデータが転送されます。

  - LUN 内で組み合わせることができます
  - ボリューム内の LUN 間
  - Storage Virtual Machine （ SVM ）内の異なるボリューム上の LUN 間
  - クラスタ内の異なる SVM 上の LUN 間：この機能を呼び出すことができない場合、 ESX ホストはコピー処理の標準の読み取りコマンドと書き込みコマンドを自動的に使用します。

- `WRITE_SAME`

  この機能により、すべてゼロなどの繰り返しパターンをストレージアレイに書き込む処理がオフロードされます。この機能は、ファイルをゼロで埋める場合などに使用されます。

- `COMPARE_AND_WRITE`

  特定のファイルへの同時アクセス制限がバイパスされ、仮想マシンのブートなどの処理が高速になります。

VAAI 環境を使用するための要件

VAAI 機能は ESX オペレーティングシステムの一部であり、環境を正しく設定すると、 ESX ホストによって自動的に起動されます。

環境の要件は次のとおりです。

- ESX ホストで ESX 4.1 以降が実行されている必要があります。
- VMwareデータストアをホストするNetAppストレージシステムでONTAPが実行されている必要があります。
- （コピーオフロードのみ） VMware コピー操作のソースとデスティネーションの両方が同じクラスタ内の同じストレージシステムでホストされている。

> コピーオフロード機能は、現時点では、異なるストレージシステムでホストされている VMware データストア間のコピーに対応していません。

VAAI機能がESXでサポートされているかどうかの確認

ESX オペレーティングシステムで VAAI 機能がサポートされているかどうかを確認するには、 vSphere Client を確認するか、他の方法でホストにアクセスします。ONTAP はデフォルトで SCSI コマンドをサポートします。

ESX ホストの詳細設定を確認して、 VAAI 機能が有効になっているかどうかを確認できます。次の表に、 SCSI コマンドと対応する ESX コントロールの名前を示します。

SCSIコマンド	ESX コントロール名（ VAAI 機能）
extended_copy の実行が可能です	`HardwareAcceleratedMove`
WRITE_Same	`HardwareAcceleratedInit`
_ と _ を比較します	`HardwareAcceleratedLocking`

Microsoftオフロードデータ転送（ODX）

Microsoft Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _ コピーオフロード _ とも呼ばれ、この機能を使用すると、ストレージデバイス内または互換性があるストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。

ODX以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でホストに転送されます。ホストは、データをネットワーク経由でデスティネーションに転送します。ODXファイル転送では、ホストを経由せずに、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースとデスティネーションの間で直接実行されるため、同じボリューム内でコピーを実行するとパフォーマンスが大幅に向上します。たとえば、同じボリュームコピーのコピー時間の短縮、クライアントでのCPUとメモリの使用量の削減、ネットワークI/O帯域幅の使用量の削減などが挙げられます。複数のボリュームにコピーが存在する場合は、ホストベースのコピーに比べてパフォーマンスが大幅に向

上することはありません。

SAN環境でODXを使用できるのは、ホストとストレージシステムの両方でODXがサポートされている場合のみです。ODXをサポートしていてODXが有効になっているクライアントコンピュータでは、ファイルの移動またはコピー時にオフロードされたファイル転送が自動的かつ透過的に使用されます。ODXは、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

ODXの使用要件

コピーオフロードにODXを使用する場合は、ボリュームのサポートに関する考慮事項、システム要件、およびソフトウェア機能の要件を理解しておく必要があります。

ODXを使用するには、システムが次の要件を満たしている必要があります。

- ONTAP

  サポート対象のバージョンのONTAPでは、ODXが自動的に有効になります。

- 最小ソースボリューム：2GB

  最適なパフォーマンスを得るには、ソースボリュームが260GBを超えている必要があります。

- WindowsクライアントでのODXのサポート

  ODXは、Windows Server 2012以降およびWindows 8以降でサポートされます。サポートされているWindowsクライアントの最新情報については、Interoperability Matrixを参照してください。

  "NetApp Interoperability Matrix Tool"

- コピーアプリケーションによるODXのサポート

  データ転送を実行するアプリケーションでODXがサポートされている必要があります。ODXをサポートするアプリケーションの処理は次のとおりです。

  - 仮想ハードディスク（VHD）の作成と変換、スナップショットの管理、仮想マシン間でのファイルのコピーなど、Hyper-Vの管理操作
  - エクスプローラでの操作
  - Windows PowerShell の copy コマンド
  - Windows コマンドプロンプトのコピーコマンド Microsoft TechNet ライブラリに、 Windows サーバおよびクライアントでサポートされている ODX アプリケーションの詳細が記載されている。

- 圧縮されたボリュームを使用する場合は、圧縮グループサイズを8Kにする必要があります。

  32Kの圧縮グループサイズはサポートされていません。

ODXは、次のボリュームタイプでは機能しません。

- 容量が2GB未満のソースボリューム
- 読み取り専用ボリューム
- "FlexCacheホリユウム"

ODXはFlexCache元のボリュームでサポートされます。

- "セミシックプロビジョニングされたボリューム"

特殊なシステムファイル要件

qtreeで見つかったODXファイルを削除できます。テクニカルサポートから指示がないかぎり、他のODXシステムファイルは削除または変更しないでください。

ODX機能を使用すると、システムのすべてのボリュームにODXシステムファイルが存在します。これらのファイルを使用すると、ODX転送中に使用されるデータのポイントインタイム表示が可能になります。次のシステムファイルは、データのオフロード先のLUNまたはファイルを含む各ボリュームのルートレベルにあります。

- `.copy-offload`（非表示のディレクトリ）
- `.tokens`（非表示ディレクトリの下にあるファイル `.copy-offload`）

コマンドを使用すると、ODXファイルを含むqtreeを削除できます `copy-offload delete-tokens -path dir_path -node node_name`。

ODXのユースケース

SVMでODXを使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODXをサポートするWindowsサーバおよびクライアントでは、リモートサーバ間でデータをコピーするデフォルトの方法として、コピーオフロードが使用されます。Windowsサーバまたはクライアントで ODXがサポートされていない場合や、ODXコピーオフロードがいずれかの時点で失敗した場合、コピー処理または移動処理は、その処理の従来の読み取りと書き込みにフォールバックされます。

ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとSVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- クラスタ間

  ソースLUNとデスティネーションLUNは、クラスタの異なるノードにある異なるボリュームにあります。これはSANでのみサポートされ、SMBでは機能しません。

その他にも、次のような特殊なユースケースがあります。

- ONTAP ODXの実装では、ODXを使用して、SMB共有とFCまたはiSCSIで接続された仮想ドライブの間でファイルをコピーできます。

  Windowsエクスプローラ、Windows CLI（PowerShell）、Hyper-V、またはODXをサポートするその他のアプリケーションでODXコピーオフロードを使用すると、SMB共有と接続されたLUNが同じクラスタにある場合に、それらの間でシームレスにファイルをコピーまたは移動できます。

- Hyper-Vでは、その他にもODXコピーオフロードのユースケースがいくつか用意されています。

  - Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク（VHD）ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

    これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

  - 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。

> Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

SAN管理

SANプロビジョニング

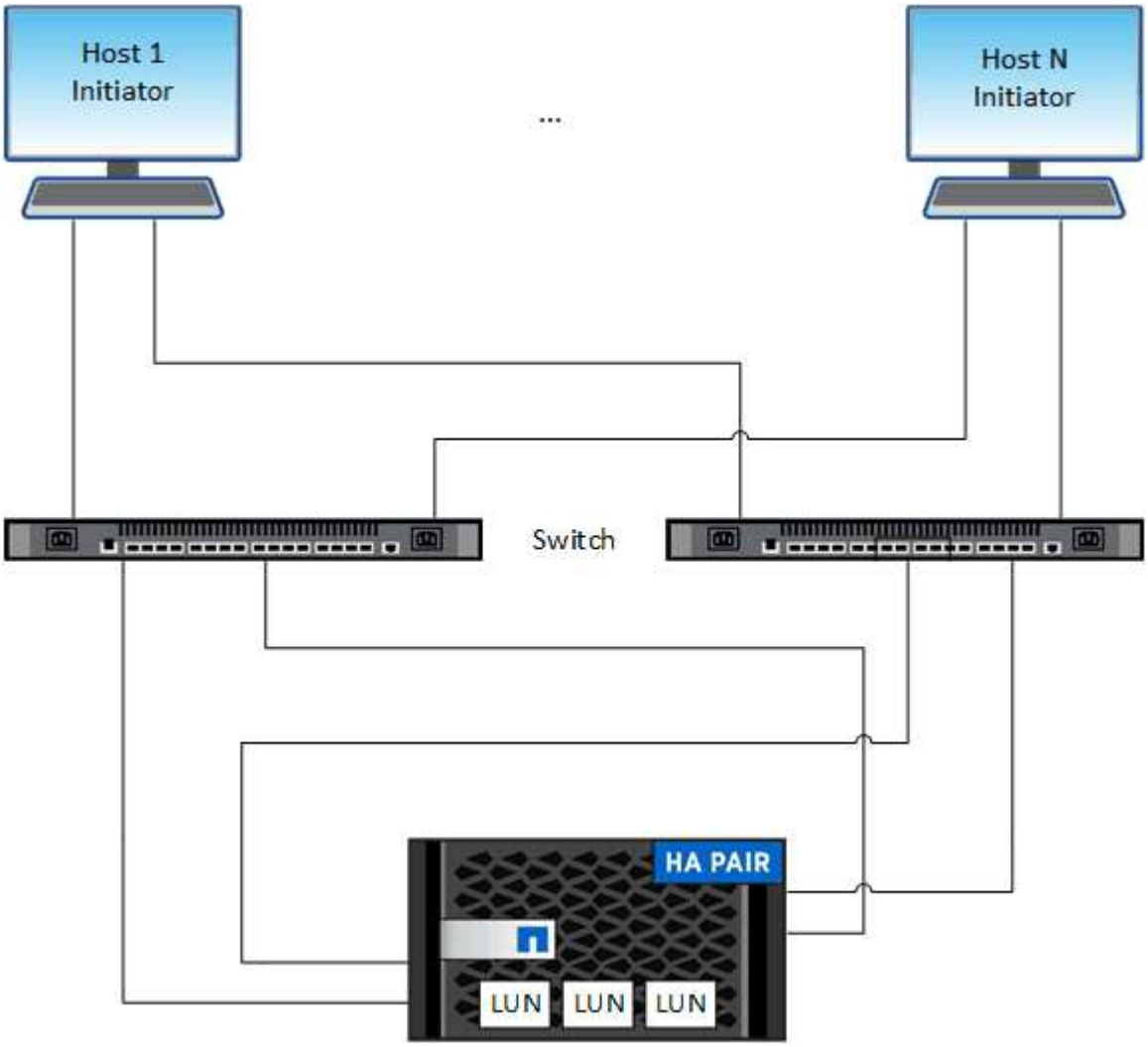
SAN管理の概要

このセクションでは、ONTAP 9 .7以降のリリースで、ONTAPコマンドラインインターフェイス（CLI）およびSystem Managerを使用してSAN環境を構成および管理する方法について説明します。

従来のSystem Manager（ONTAP 9 .7以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- "iSCSIプロトコル"
- "FC/FCoE プロトコル"

SAN環境では、iSCSIプロトコルとFCプロトコルを使用してストレージを提供できます。



iSCSIおよびFCでは、ストレージターゲットはLUN（論理ユニット）と呼ばれ、ホストには標準のブロックデバイスとして認識されます。LUNを作成し、イニシエータグループ（igroup）にマッピングします。イニシエータグループはFCホストのWWPSおよびiSCSIホストノード名のテーブルであり、どのイニシエータがどのLUNにアクセスできるかを制御します。

FCターゲットは、FCスイッチおよびホスト側アダプタを介してネットワークに接続し、World-Wide Port Name（WWPN）で識別されます。iSCSIターゲットは、標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載したTCPオフロードエンジン（TOE）カード、統合ネットワークアダプタ（CNA）または専用のホストバスアダプタ（HBA）を介してネットワークに接続し、iSCSI Qualified Name（IQN）で識別されます。

詳細情報

ASA R2ストレージシステム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、またはASA A20）がある場合は、を参照してください"ASA R2ストレージシステムのドキュメント"。

NetAppオールフラッシュSANアレイ（ASA）は、ONTAP 9以降で使用できます。7.ASAは、実績のあるAFF NetAppプラットフォーム上に構築された、オールフラッシュのSAN専用ソリューションです。

ASA プラットフォームには次のものがあります。

- ASA A150
- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800

ONTAP 9.16.0以降では、ASA R2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、またはASA A20）で、SAN専用のシンプルなONTAPエクスペリエンスを利用できます。ASA R2システムを使用している場合は、を参照してください"ASA R2システムのマニュアル"。

ASAプラットフォームでは、マルチパスに対称アクティブ/アクティブ構成を使用します。すべてのパスがアクティブかつ最適化されているため、ストレージフェイルオーバーが発生した場合、ホストはALUAによるフェイルオーバーパスの移行を待機してI/Oを再開する必要はありません。これにより、フェイルオーバーにかかる時間が短縮されます。

ASAのセットアップ

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

System Managerの指示に従って、ASA用のクラスタの初期化、ローカル階層の作成、プロトコルの設定、およびストレージのプロビジョニングに必要な手順を実行できます。

ONTAPクラスタセットアップの開始です。

ASAのホスト設定とユーティリティ

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

特定のホスト用のをサポートサイトからダウンロードできます"NetApp Host Utilities ソフトウェア"。

ASAシステムの識別方法

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

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

パーソナリティ*は*オールフラッシュSANアレイ*と表示されます。

- * CLIから*：コマンドを入力します `san config show`。

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

  の詳細については `san config show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

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

FCoE用のスイッチの設定

既存のイーサネットインフラでFCサービスを実行するには、FCoE用にスイッチを設定する必要があります。

開始する前に

- SAN構成がサポートされている必要があります。

  サポートされる構成の詳細については、を参照してください "NetApp Interoperability Matrix Tool"。

- ユニファイドターゲットアダプタ（UTA）がストレージシステムにインストールされている必要があります。

  UTA2を使用する場合は、modeに設定する必要があります `cna`。

- Converged Network Adapter（CNA；統合ネットワークアダプタ）がホストにインストールされている必要があります。

手順

1. スイッチのドキュメントを参照して、FCoE用にスイッチを設定します。
2. クラスタ内の各ノードのDCB設定が正しく設定されていることを確認します。

   ```
   run -node node1 -command dcb show
   ```

   DCB設定はスイッチ上で行います。設定が正しくない場合は、スイッチのマニュアルを参照してください。

3. FCターゲットポートのオンラインステータスがのときに、FCoEログインが機能していることを確認します `true`。

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   FCターゲットポートのオンラインステータスがの場合は `false`、スイッチのマニュアルを参照してくだ

さい。

関連情報

- "NetApp Interoperability Matrix Tool"
- "NetAppテクニカルレポート3800：『Fibre Channel over Ethernet（FCoE）End-to-End Deployment Guide』"
- "Cisco MDS 9000 NX-OSおよびSAN-OSソフトウェア構成ガイド"
- "Brocade製品"

システム要件

LUNのセットアップでは、LUNを作成し、igroupを作成して、LUNをigroupにマッピングします。LUNをセットアップするには、システムが一定の前提条件を満たしている必要があります。

- 使用するSAN構成がサポート対象としてInteroperability Matrixで確認されている必要があります。
- SAN環境が、使用しているONTAPソフトウェアのバージョンに対応するに記載されたSANホスト数とコントローラ数の制限を満たしている必要があります "NetApp Hardware Universe"。
- サポートされているバージョンのHost Utilitiesがインストールされている必要があります。

  詳細については、Host Utilitiesのマニュアルを参照してください。

- LUNの所有者ノードと所有者ノードのHAパートナーにSAN LIFが必要です。

関連情報

- "NetApp Interoperability Matrix Tool"
- "ONTAP SANホスト構成"
- "NetAppテクニカルレポート4017：『ファイバチャネルSANのベストプラクティス』"

LUNを作成する際の注意事項

クラスタでLUNのセットアップを開始する前に、LUNに関する次のガイドラインを確認しておく必要があります。

LUNの実際のサイズが少し異なる理由

LUNのサイズについては、次の点に注意してください。

- LUNを作成する場合、LUNの実際のサイズはLUNのOSタイプによって多少異なります。LUNの作成後にLUNのOSタイプを変更することはできません。
- 最大LUNサイズでLUNを作成する場合は、LUNの実際のサイズが若干小さくなる可能性があることに注意してください。ONTAPは、制限を切り捨ててわずかに小さくします。
- 各LUNのメタデータ用に、包含アグリゲートに約64KBのスペースが必要です。LUNの作成時には、包含アグリゲートにLUNのメタデータ用の十分なスペースがあることを確認する必要があります。アグリゲートにLUNのメタデータ用のスペースが十分にないと、一部のホストがLUNにアクセスできなくなる可能性があります。

LUN IDの割り当てに関するガイドライン

通常、デフォルトのLUN IDは0で始まり、LUNをマッピングするたびに1ずつ割り当てられます。ホストはLUN IDをLUNの場所とパス名に関連付けます。有効なLUN ID番号の範囲はホストによって異なります。詳細については、Host Utilitiesに付属のマニュアルを参照してください。

LUNをigroupにマッピングする場合のガイドライン

- LUNは、igroupに一度だけマッピングできます。
- ベストプラクティスとして、1つのLUNをigroupを介して1つの特定のイニシエータにのみマッピングすることを推奨します。
- 1つのイニシエータを複数のigroupに追加できますが、イニシエータをマッピングできるLUNは1つだけです。
- 同じigroupにマッピングされた2つのLUNに同じLUN IDを使用することはできません。
- igroupとポートセットには、同じプロトコルタイプを使用する必要があります。

プロトコルFCまたはiSCSIライセンスを確認して追加する

FCまたはiSCSIでStorage Virtual Machine（SVM）のブロックアクセスを有効にするには、ライセンスが必要です。FCとiSCSIのライセンスはに含まれて"ONTAP One"います。

例 **14.** 手順

System Manager

ONTAP Oneをお持ちでない場合は、ONTAP System Manager（9.7以降）でFCまたはiSCSIのライセンスを確認して追加します。

1. System Managerで、*[クラスタ]>[設定]>[ライセンス]*を選択します
2. ライセンスが表示されない場合は、を選択し + Add てライセンスキーを入力します。
3. 「* 追加」を選択します。

CLI

ONTAP Oneをお持ちでない場合は、ONTAP CLIを使用してFCまたはiSCSIのライセンスを確認して追加します。

1. FCまたはiSCSIのアクティブなライセンスがあることを確認します。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- --------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FCまたはiSCSIのアクティブなライセンスがない場合は、ライセンス コードを追加します。

```
license add -license-code <your_license_code>
```

SANストレージのプロビジョニング

この手順では、FCまたはiSCSIプロトコルがすでに設定されている既存のStorage VMに新しいLUNを作成します。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"ストレージをプロビジョニングします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

新しいStorage VMを作成してFCプロトコルまたはiSCSIプロトコルを設定する必要がある場合は、または
を参照してください"FC用のSVMの設定""SVMをiSCSI用に設定する"。

FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータス
はdownになります。

LUNは、ホストにはディスク デバイスとして表示されます。

LUNの作成時、Asymmetric Logical Unit Access（ALUA）は常に有効になります。ALUAの設定
は変更できません。

イニシエータをホストするには、SVM内のすべてのFC LIFで単一イニシエータ ゾーニングを使用する必要が
あります。

ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニ
ングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。

例 **15.** 手順

System Manager

ONTAP System Manager（9.7以降）でFCまたはiSCSIプロトコルを使用して、SANホスト用のストレージを提供するLUNを作成します。

System Manager Classic（9.7以前で利用可能）を使用してこのタスクを実行するには、 "Red Hat Enterprise Linux向けのiSCSIの設定"

手順

1. ホストに適切なをインストールし"SANホストユーティリティ"ます。
2. System Manager で、 * Storage > LUNs * をクリックし、 * Add * をクリックします。
3. LUNの作成に必要な情報を入力します。
4. ONTAP のバージョンに応じて、「その他のオプション」をクリックすると、次のいずれかの操作を実行できます。

オプション	以降で使用可能
• 親ボリュームではなくLUNにQoSポリシーを割り当てる ◦ * その他のオプション > ストレージと最適化 * ◦ パフォーマンスサービスレベル * を選択します。 ◦ ボリューム全体ではなく個々の LUN に QoS ポリシーを適用するには、 * これらのパフォーマンス制限を各 LUN に適用 * を選択します。 デフォルトでは、パフォーマンス制限はボリュームレベルで適用されます。	ONTAP 9 10.1
• 既存のigroupを使用して新しいイニシエータグループを作成する ◦ * 「その他のオプション」 > 「ホスト情報」 * ◦ 既存のイニシエータグループを使用して新しいイニシエータグループを選択します * 。 他のigroupを含むigroupは、作成後にOSタイプを変更することはできません。	ONTAP 9 .9.1
• igroupまたはホストイニシエータに説明を追加する この説明は、igroupまたはホストイニシエータのエイリアスとして機能します。 ◦ * 「その他のオプション」 > 「ホスト情報」 *	ONTAP 9 .9.1

• 既存のボリュームにLUNを作成する デフォルトでは、新しいボリュームに新しいLUNが作成されます。 ◦ * その他のオプション > LUN の追加 * ◦ ［ * グループ関連の LUN * ］ を選択します。	ONTAP 9 .9.1
• QoSを無効にするかカスタムQoSポリシーを選択 ◦ * その他のオプション > ストレージと最適化 * ◦ パフォーマンスサービスレベル * を選択します。 ONTAP 9.9.1以降では、カスタムのQoSポリシーを選択した場合、指定したローカル階層への手動配置を選択することもできます。	ONTAP 9.8

5. FCの場合は、FCスイッチをWWPNでゾーニングします。イニシエータごとに1つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
6. ホストでLUNを検出します。

   VMware vSphereでは、Virtual Storage Console（VSC）を使用してLUNを検出、初期化してください。
7. LUNを初期化し、必要に応じてファイルシステムを作成します。
8. ホストからLUNのデータの読み取りと書き込みができることを確認します。

CLI

ONTAP CLIでFCまたはiSCSIプロトコルを使用して、SANホスト用のストレージを提供するLUNを作成します。

1. FCまたはiSCSIのライセンスがあることを確認します。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FCまたはiSCSIのライセンスがない場合は、コマンドを使用し `license add`ます。

```
license add -license-code <your_license_code>
```

3. SVMでプロトコルサービスを有効にします。

   ◦ iSCSIの場合：*

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   ◦ FCの場合：*

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. 各ノードにSVM用のLIFを2つ作成します。

```
network interface create -vserver <svm_name> -lif <lif_name> -role
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
<port_name> -address <ip_address> -netmask <netmask>
```

   NetAppでは、データを提供する各SVMについて、ノードごとに少なくとも1つのiSCSI LIFまたはFC LIFがサポートされます。ただし、冗長性を確保するためにはノードごとに2つのLIFが必要です。iSCSIの場合は、別 々 のイーサネットネットワークにあるノードごとに少なくとも2つのLIFを設定することを推奨します。

5. LIFが作成され、動作ステータスがになっていることを確認し `online`ます。

```
network interface show -vserver <svm_name> <lif_name>
```

6. LUNを作成します。

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

   LUN名は255文字以内で、スペースは使用できません。

   NVFAILオプションは、ボリュームにLUNが作成されると自動的に有効になります。

7. igroupを作成します。

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. LUNをigroupにマッピングします。

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. LUNが正しく設定されていることを確認します。

```
lun show -vserver <svm_name>
```

10. 必要に応じて、"ポートセットを作成してigroupにバインドします"。
11. 特定のホストでブロックアクセスを有効にするには、ホストのマニュアルの手順に従います。
12. Host Utilitiesを使用してFCまたはiSCSIマッピングを完了し、ホスト上のLUNを検出します。

関連情報

- "SANの管理の概要"
- "ONTAP SANホスト構成"
- "System ManagerでのSANイニシエータグループの表示と管理"
- "NetAppテクニカルレポート4017：『ファイバチャネルSANのベストプラクティス』"

NVMeプロビジョニング

NVMeの概要

SAN環境では、Non-Volatile Memory Express（NVMe）プロトコルを使用してストレージを提供できます。NVMeプロトコルは、ソリッドステートストレージのパフォーマンスを最大限に引き出すように最適化されています。

NVMeでは、ストレージターゲットをネームスペースと呼びます。NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性ストレージの容量で、ホストには標準のブロックデバイスとして提供されます。FCおよびiSCSIでLUNをプロビジョニングしてigroupにマッピングするのと同じように、ネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングします。

NVMeターゲットは、FCスイッチを使用する標準のFCインフラ、またはイーサネットスイッチとホスト側アダプタを使用する標準のTCPインフラを通じてネットワークに接続されます。

NVMeのサポートは、ONTAPのバージョンによって異なります。詳細は、を参照してください "NVMeのサポートと制限" 。

NVMeとは

Nonvolatile Memory express（NVMe）プロトコルは、不揮発性ストレージメディアへのアクセスに使用される転送プロトコルです。

NVMe over Fabrics（NVMeoF）は仕様で定義されたNVMeの拡張機能であり、PCIe以外の接続を介し

たNVMeベースの通信を可能にします。このインターフェイスを使用すると、外部ストレージエンクロージャをサーバに接続できます。

NVMeは、フラッシュテクノロジから高パフォーマンスの永続的メモリテクノロジまで、不揮発性メモリを搭載したストレージデバイスに効率的にアクセスできるように設計されています。そのため、ハードディスクドライブ用に設計されたストレージプロトコルと同じ制限はありません。フラッシュデバイスとソリッドステートデバイス（SSD）は、不揮発性メモリ（NVM）の一種です。NVMは、停電時にコンテンツを保持するメモリの一種です。NVMeは、そのメモリにアクセスできる方法です。

NVMeには、データ転送の速度、生産性、スループット、容量の向上などのメリットがあります。具体的な特徴は次のとおりです。

- 最大64、000個のキューを保持できるように設計されています。

  各キューには、最大64、000個のコマンドを同時に実行できます。

- NVMeは複数のハードウェアベンダーやソフトウェアベンダーでサポートされている
- フラッシュテクノロジによりNMVeの生産性が向上し、応答時間が短縮
- NVMe では、 SSD に送信される「検索」ごとに複数のデータ要求を行うことができます。

  NVMe は「要求」のデコードにかかる時間が短く、マルチスレッドプログラムでスレッドロックを必要としません。

- CPUレベルでのボトルネックを防止する機能をサポートし、システムの拡張に応じて並外れた拡張性を実現します。

NVMeネームスペースについて

NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリ（NVM）の容量です。ネームスペースは、Storage Virtual MachineでNVMeプロトコルが設定されている場合に使用され、FCプロトコルおよびiSCSIプロトコルのLUNに相当します。

NVMeホストには、1つ以上のネームスペースがプロビジョニングされて接続されています。各ネームスペースは、さまざまなブロックサイズをサポートできます。

NVMeプロトコルは、複数のコントローラ経由でネームスペースへのアクセスを提供します。ほとんどのオペレーティングシステムでサポートされているNVMeドライバを使用すると、ソリッドステートドライブ（SSD）ネームスペースは標準ブロックデバイスとして表示され、このデバイス上にファイルシステムやアプリケーションを変更することなく導入できます。

ネームスペースID（NSID）は、コントローラがネームスペースへのアクセスを提供するために使用する識別子です。ホストまたはホストグループのNSIDを設定する場合は、ホストからボリュームへのアクセスも設定します。論理ブロックは一度に1つのホストグループにのみマッピングでき、1つのホストグループに重複するNSIDはありません。

NVMeサブシステムについて

NVMeサブシステムには、1つ以上のNVMeコントローラ、ネームスペース、NVMサブシステムポート、NVMストレージメディア、およびコントローラとNVMストレージメディア間のインターフェイスが含まれます。作成したNVMeネームスペースは、デフォルトではサブシステムにマッピングされません。新規または既存のサブシステムにマッピングすることもできます。

関連情報

- "NVMe ストレージをプロビジョニングする"ASA、AFF、FASシステムの学習
- "NVMeネームスペースをサブシステムにマッピングする"ASA AFFおよびFASシステムについて学習します。
- "SANホストとクラウドクライアントを設定"
- ASA R2（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、またはASA A20）ストレージシステムでの操作方法を学習します"SANストレージのプロビジョニング"。

NVMeのライセンス要件

ONTAP 9 .5以降では、NVMeをサポートするにはライセンスが必要です。ONTAP 9でNVMeが有効になっている場合は、ONTAP 9にアップグレードしたあと90日間の猶予期間が与えられます。5.

ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

NVMeの設定、サポート、制限事項

SAN.4以降では、ONTAP 9環境でこの"Non-Volatile Memory Express（NVMe）"プロトコルを使用できます。FC-NVMeでは、物理的なセットアップとゾーニングの手法を従来のFCネットワークと同じにしますが、FC-SCSIよりも帯域幅が広く、IOPSが高く、レイテンシが低減されます。

NVMeのサポートと制限事項は、ONTAPのバージョン、プラットフォーム、構成によって異なります。特定の設定の詳細については、を参照して"NetApp Interoperability Matrix Tool"ください。サポートされる制限については、を参照してください"Hardware Universe"。

クラスタあたりの最大ノード数は、Hardware Universeの*サポートされるプラットフォームの混在*で確認できます。

構成

- NVMe構成は、単一ファブリックまたはマルチファブリックを使用してセットアップできます。
- SANをサポートするSVMごとに管理LIFを1つ設定する必要があります。
- 組み込みブレードスイッチの場合を除き、異機種混在のFCスイッチファブリックの使用はサポートされていません。

  特定の例外については、を"NetApp Interoperability Matrix Tool"参照してください。

- カスケードファブリック、パーシャルメッシュファブリック、フルメッシュファブリック、コアエッジファブリック、およびディレクタファブリックは、FCスイッチをファブリックに接続する業界標準の方法であり、すべてサポートされます。

  ファブリックは1つまたは複数のスイッチで構成でき、ストレージコントローラは複数のスイッチに接続できます。

ONTAPのバージョンに応じて、次のNVMe機能がサポートされます。

ONTAPバージョン	NVMeのサポート
9.17.1	• VMware ワークロード用のSnapMirrorアクティブ同期 NVMe/FC および NVMe/TCP ホスト アクセス。 VMware での NVMe/TCP は、VMware バグ ID: TR1049746 の解決に依存します。
9.15.1	• NVMe/TCPテノ4ノオトMetroCluster IPコウセイ
9.14.1	• サブシステムでのホストプライオリティの設定（ホストレベルのQoS）
9.12.1	• NVMe/FCテノ4ノオトMetroCluster IPコウセイ • ONTAP 9より前のフロントエンドNVMeネットワークでは、MetroCluster構成はサポートされません。12.1. • MetroCluster構成はNVMe/TCPではサポートされません。
9.10.1	ネームスペースのサイズ変更
9.9.1	• 同じボリューム上でのネームスペースとLUNの共存
9.8	• プロトコルの共存 SCSI、NAS、NVMeの各プロトコルを同じStorage Virtual Machine（SVM）に共存させることができます。 ONTAP 9.8より前のバージョンでは、SVMで使用できるプロトコルはNVMeのみです。

9.6	• ネームスペース用に512バイトブロック、4096バイトブロック デフォルト値は4096です。512は、ホストオペレーティングシステムが4096バイトブロックをサポートしていない場合にのみ使用してください。 • ネームスペースがマッピングされたボリュームの移動
9.5	• マルチパスHAペアのフェイルオーバー/ギブバック

プロトコル

サポートされるNVMeプロトコルは次のとおりです。

プロトコル	ONTAPバージョン	許可するユーザ
TCP	9.10.1	デフォルト
FC	9.4	デフォルト

ONTAP 9 .8以降では、同じStorage Virtual Machine（SVM）にSCSI、NAS、NVMeの各プロトコルを設定できます。ONTAP 9.7以前では、SVMで使用できるプロトコルはNVMeのみです。

ネームスペース

NVMeネームスペースを使用するときは、次の点に注意してください。

- ONTAP 9.15.1以前のONTAPでは、NVMeを使用したnvme DataSet Management（deallocate）コマンドによるスペース再生はサポートされていません。
- SnapRestoreを使用してLUNからネームスペースをリストアしたり、LUNからネームスペースをリストアしたりすることはできません。
- ネームスペースのスペースギャランティは、それを含むボリュームのスペースギャランティと同じです。
- Data ONTAP 7-Modeから移行するボリュームでネームスペースを作成することはできません。
- ネームスペースでは、次のものはサポートされません。
  - 名前変更
  - ボリューム間での移動
  - ボリューム間でのコピー
  - オンデマンド コピー

その他の制限事項

ONTAPの次の機能は、**NVMe**構成ではサポートされません。

- Virtual Storage Console

- 永続的予約

次の考慮事項は**ONTAP 9.4**を実行しているノードだけに該当します。

- NVMe LIFとネームスペースは同じノードでホストされている必要があります。
- NVMe LIFを作成する前に、NVMeサービスを作成しておく必要があります。

関連情報

"最新SANのベストプラクティス"

NVMe用の**Storage VM**の設定

ノードでNVMeプロトコルを使用する場合は、SVMをNVMe専用に設定する必要があります。

開始する前に

FCアダプタまたはイーサネットアダプタでNVMeがサポートされている必要があります。サポートされているアダプタについては、を "NetApp Hardware Universe"参照してください。

例 **16.** 手順

System Manager

ONTAP System Manager（9.7以降）でNVMe用のStorage VMを設定します。

新しい**Storage VM**に**NVMe**を設定するには	既存の**Storage VM**に**NVMe**を設定するには
1. System Managerで、* Storage > Storage VM*をクリックし、* Add *をクリックします。 2. Storage VMの名前を入力してください。 3. アクセスプロトコル*として「* nvme」を選択します。 4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。	1. System Manager で、 * Storage > Storage VM*をクリックします。 2. 設定するStorage VMをクリックします。 3. [設定]*タブをクリックし、NVMeプロトコルの横にあるをクリックし ます。 4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。

CLI

ONTAP CLIを使用してNVMe用のStorage VMを設定します。

1. 既存のSVMを使用しない場合は作成します。

```
vserver create -vserver <SVM_name>
```

   a. SVMが作成されたことを確認します。

```
vserver show
```

2. クラスタにNVMeまたはTCP対応アダプタがインストールされていることを確認します。

   NVMeの場合：

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   TCPの場合：

```
network port show
```

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

3. ONTAP 9.7以前を実行している場合は、SVMからすべてのプロトコルを削除します。

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

ONTAP 9.8以降では、NVMeを追加するときに他のプロトコルを削除する必要はありません。

4. SVMにNVMeプロトコルを追加します。

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. ONTAP 9.7以前を実行している場合は、SVMで許可されているプロトコルがNVMeだけであることを確認します。

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

列にはNVMeプロトコルのみが表示されます `allowed protocols`。

6. NVMeサービスを作成します。

```
vserver nvme create -vserver <SVM_name>
```

7. NVMeサービスが作成されたことを確認します。

```
vserver nvme show -vserver <SVM_name>
```

SVMのが `Administrative Status`と表示されます `up`。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。

8. NVMe/FC LIFを作成します。
   - ONTAP 9 .9.1以前の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - ONTAP 9.10.1 以降の場合、FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- ONTAP 9.10.1 以降の場合、TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. HAパートナーノードにNVMe/FC LIFを作成します。
   - ONTAP 9 .9.1以前の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - ONTAP 9.10.1 以降の場合、FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

   - ONTAP 9.10.1 以降の場合、TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. NVMe/FC LIFが作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

11. LIFと同じノードにボリュームを作成します。

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

auto効率化ポリシーに関する警告メッセージが表示された場合は、無視してかまいません。

NVMeストレージのプロビジョニング

次の手順に従って、既存のStorage VMでNVMe対応ホスト用のネームスペースを作成し、ストレージをプロビジョニングします。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、"以下の手順を実行します"ストレージをプロビジョニングします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。

開始する前に

Storage VMがNVMe用に設定されていて、FCまたはTCP転送のセットアップが完了している必要があります。

System Manager

ONTAP System Manager（9.7以降）を使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

手順

1. System Manager で、 * Storage > NVMe 名前空間 * をクリックし、 * Add * をクリックします。

   新しいサブシステムを作成する必要がある場合は、 * その他のオプション * をクリックします。

2. ONTAP 9.8 以降を実行していて、 QoS を無効にする場合やカスタムの QoS ポリシーを選択する場合は、「その他のオプション」をクリックし、「 * ストレージおよび最適化 * 」で「 * パフォーマンスサービスレベル * 」を選択します。
3. FCスイッチをWWPNでゾーニングします。イニシエータごとに1つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
4. ホストで、新しいネームスペースを検出します。
5. ネームスペースを初期化し、ファイルシステムでフォーマットします。
6. ホストがネームスペースのデータを読み書きできることを確認します。

CLI

ONTAP CLIを使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

この手順では、NVMeプロトコル用に設定済みの既存のStorage VMにNVMeネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングしてホストシステムからのデータアクセスを許可します。

Storage VMをNVMe用に設定する必要がある場合は、を参照してください"NVMe用のSVMの設定"。

手順

1. SVMがNVMe用に設定されていることを確認します。

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe`が列の下に表示されます `allowed-protocols`。

2. NVMeネームスペースを作成します。

   パラメータで参照するボリュームは、すでに存在している必要があります。存在していない場合は、このコマンドを実行する前にボリュームを `-path`作成する必要があります。

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. NVMeサブシステムを作成します。

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

NVMeサブシステム名では大文字と小文字が区別されます。1~96文字で指定する必要があります。特殊文字を使用できます。

4. サブシステムが作成されたことを確認します。

```
vserver nvme subsystem show -vserver <svm_name>
```

`nvme`列の下にサブシステムが表示され `Subsystem`ます。

5. ホストからNQNを取得します。
6. ホストNQNをサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

ネームスペースは1つのサブシステムにのみマッピングできます。

8. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <svm_name> -instance
```

サブシステムがと表示され `Attached subsystem`ます。

NVMeネームスペースをサブシステムにマッピングする

NVMeネームスペースをサブシステムにマッピングすると、ホストからのデータアクセスが可能になります。NVMeネームスペースは、ストレージのプロビジョニング時にサブシステムにマッピングすることも、ストレージのプロビジョニング後にマッピングすることもできます。

ONTAP 9.17.1以降では、 SnapMirror Active Sync構成を使用している場合、ホストをNVMeサブシステムに追

加する際に、SVMを近接VServerとしてホストに追加できます。NVMeサブシステム内のネームスペースのアクティブ最適化パスは、近接VServerとして設定されているSVMからのみホストに公開されます。

ONTAP 9 14.1以降では、特定のホストのリソース割り当てに優先順位を付けることができます。デフォルトでは、NVMeサブシステムに追加されたホストには標準優先度が与えられます。ONTAPのコマンドラインインターフェイス（CLI）を使用して、デフォルト優先度を手動で標準から高に変更できます。高い優先度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。

ONTAP 9 .13.1以前でサブシステムに追加されたホストに高い優先度を設定する場合は、を使用できますホスト優先度の変更。

開始する前に

ネームスペースとサブシステムはすでに作成されている必要があります。ネームスペースとサブシステムを作成する必要がある場合は、を参照してください"NVMeストレージのプロビジョニング"。

NVMe名前空間をマップする

手順

1. ホストからNQNを取得します。
2. ホストNQNをサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

ホストのデフォルト優先度をregularからhighに変更する場合は、オプションを使用し `-priority high` ます。このオプションは、`ONTAP 9.14.1`以降で使用できます。の詳細については `vserver nvme subsystem host add`、を"ONTAPコマンド リファレンス"参照してください。

SVMを `proximal-vserver` SnapMirrorアクティブ同期構成でホストをNVMeサブシステムに追加する際に、 `-proximal-vservers`オプション。このオプションは、ONTAP 9.17.1以降で使用できます。ソースSVM、デスティネーションSVM、またはその両方を追加できます。このコマンドを実行しているSVMがデフォルトです。

3. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

ネームスペースは1つのサブシステムにのみマッピングできます。の詳細については `vserver nvme subsystem map add`、を"ONTAPコマンド リファレンス"参照してください。

4. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

サブシステムがと表示され `Attached subsystem` ます。の詳細については `vserver nvme`

`namespace show`、を"ONTAPコマンド リファレンス"参照してください。

LUNの管理

LUNのQoSポリシー グループの編集

ONTAP 9.10.1 以降では、System Manager を使用して、複数の LUN に対して同時に QoS (Quality of Service) ポリシーを割り当てたり削除したりすることができます。

QoSポリシーがボリュームレベルで割り当てられている場合は、ボリュームレベルで変更する必要があります。QoSポリシーをLUNレベルで編集できるのは、元 々 LUNレベルで割り当てられていた場合のみです。

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 編集するLUNを選択します。

   一度に複数のLUNを編集する場合は、それらのLUNが同じStorage Virtual Machine（SVM）に属している必要があります。同じSVMに属していないLUNを選択した場合、QoSポリシーグループを編集するオプションは表示されません。

3. [* その他 *] をクリックし、 [* QoS ポリシーグループの編集 *] を選択します。

LUNをネームスペースに変換する

ONTAP 9 .11.1以降では、ONTAP CLIを使用して、既存のLUNをNVMeネームスペースにインプレース変換できます。

開始する前に

- 指定したLUNにigroupへの既存のマッピングが含まれていないことを確認してください。
- LUN は、MetroCluster が設定された SVM 内または SnapMirror アクティブ同期関係内に存在してはなりません。
- LUNはプロトコルエンドポイントではなく、プロトコルエンドポイントにバインドしないでください。
- LUNにゼロ以外のプレフィックスやサフィックスストリームを使用することはできません。
- Snapshotの一部であったり、読み取り専用LUNとしてSnapMirror関係のデスティネーション側であったりすることはできません。

ステップ

1. LUNをNVMeネームスペースに変換します。

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

LUNのオフライン化

ONTAP 9 .10.1以降では、System Managerを使用してLUNをオフラインにすることができます。LUN.10.1より前のバージョンでは、ONTAP CLIを使用してONTAP 9をオフラインにする必要があります。

System Manager

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 単一のLUNまたは複数のLUNをオフラインにする

実行する操作	操作
単一の LUN をオフラインにします	LUN名の横にあるをクリック ⋮ し、*[Take Offline]* を選択します。
複数の LUN をオフラインにします	1. オフラインにするLUNを選択します。 2. 「 * 詳細」をクリックし、「 * オフラインにする * 」を選択します。

CLI

CLIを使用してオフラインにできるLUNは一度に1つだけです。

ステップ

1. LUNをオフラインにします。

```
lun offline <lun_name> -vserver <SVM_name>
```

ONTAPでLUNのサイズを変更する

LUNのサイズは増やすことも減らすこともできます。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"ストレージ ユニットのサイズを拡大します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

Solaris LUNのサイズは変更できません。

LUNのサイズを拡張する

LUNを拡張できるサイズは、ONTAPのバージョンによって異なります。

ONTAPのバージョン	LUNの最大サイズ
ONTAP 9.12.1P2以降	AFF、FAS、ASAプラットフォームの場合は128TB
ONTAP 9.8以降	• オールフラッシュSANアレイ（ASA）プラットフォームの場合は128TB • ASA以外のプラットフォームの場合は16TB
ONTAP 9.5 、 9.6 、 9.7	16TB
ONTAP 9 .4以前	元のLUNサイズの10倍。ただし、LUNの最大サイズである16TBを超えないようにする必要があります。たとえば、100GBで作成したLUNは1、000GBまでしか拡張できません。LUNの実際の最大サイズが正確に16TBであるとは限りません。ONTAPは、制限を切り捨ててわずかに小さくします。

サイズを拡張するためにLUNをオフラインにする必要はありません。ただし、サイズを拡張したあとにホストでLUNを再スキャンして、サイズの変更を認識できるようにする必要があります。

例 **17.** 手順

System Manager

ONTAP System Manager（9.7以降）でLUNのサイズを拡張します。

1. System Manager で、 * Storage > LUNs * をクリックします。
2. をクリック ⋮ し、*[編集]*を選択します。
3. Storage and Optimization では、**LUN**のサイズが拡張され、 Save *が表示されます。

CLI

ONTAP CLIを使用してLUNのサイズを拡張します。

1. LUNのサイズを拡張します。

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

   の詳細については `lun resize`、を"ONTAPコマンド リファレンス"参照してください。

2. 拡張したLUNのサイズを確認します。

```
lun show -vserver <SVM_name>
```

ONTAP処理では、LUNの実際の最大サイズが想定値よりわずかに小さく切り捨てられます。また、LUNの実際のサイズは、LUNのOSタイプによって多少異なる場合があります。サイズ変更後の正確な値を確認するに

は、アドバンス・モードで次のコマンドを実行します。

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

+
の詳細については `lun show`、を"ONTAPコマンド リファレンス"参照してください。

1. ホストのLUNを再スキャンします。
2. ホストのマニュアルに従って、新しく作成したLUNサイズをホストファイルシステムが認識できるようにします。

LUNのサイズを縮小する

LUNのサイズを縮小する前に、ホストはLUNデータを含むブロックを小さいLUNサイズの境界に移行する必要があります。LUNデータを含むブロックを切り捨てずにLUNを適切に縮小するには、SnapCenterなどのツールを使用する必要があります。LUNのサイズを手動で縮小することは推奨されません。

LUNのサイズを縮小すると、サイズが縮小されたことがONTAPからイニシエータに自動的に通知されます。ただし、ホストが新しいLUNサイズを認識するために、ホストで追加の手順が必要になる場合があります。ホストのファイル構造のサイズの縮小に固有の情報については、ホストのマニュアルを参照してください。

LUNの移動

Storage Virtual Machine（SVM）内のボリューム間でLUNを移動できますが、SVM間でLUNを移動することはできません。SVM内のボリューム間で移動されたLUNはただちに移動され、接続が失われることはありません。

開始する前に

LUNでSelective LUN Map（SLM；選択的LUNマップ）を使用している場合は、LUNを移動する前に、デスティネーションノードとそのHAパートナーを含める必要があり"SLMレポートノードリストの変更"ます。

タスクの内容

重複排除、圧縮、コンパクションなどのStorage Efficiency機能は、LUNの移動時には維持されません。LUNの移動の完了後に再適用する必要があります。

Snapshotによるデータ保護はボリュームレベルで行われます。そのため、移動したLUNにはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用のSnapshotが確立されていない場合、LUNのSnapshotは作成されません。また、LUNのすべてのSnapshotは、Snapshotが削除されるまで元のボリュームに残ります。

次のボリュームにはLUNを移動できません。

- SnapMirrorデスティネーションボリューム
- SVMルートボリューム

次のタイプのLUNは移動できません。

- ファイルから作成されたLUN
- NVFail状態のLUN
- 負荷共有関係にあるLUN
- プロトコルエンドポイントクラスのLUN

クラスタ内のノードが異なるONTAPバージョンを使用している場合、ソースがデスティネーションよりも新しいバージョンである場合にのみ、異なるノード上のボリューム間でLUNを移動できます。例えば、ソースボリュームのノードがONTAP 9.15.1で、デスティネーションボリュームのノードがONTAP 9.16.1の場合、LUNを移動することはできません。同じONTAPバージョンのノード上のボリューム間ではLUNを移動できます。

1TB以上のos_type Solaris LUNの場合、LUNの移動中にホストでタイムアウトが発生することがあります。このタイプのLUNでは、移動を開始する前にLUNをアンマウントする必要があります。

例 **18.** 手順

System Manager

ONTAP System Manager（9.7以降）でLUNを移動します。

ONTAP 9 .10.1以降では、単一のLUNを移動する際にSystem Managerを使用して新しいボリュームを作成できます。ONTAP 9 .8および9.9.1では、LUNの移動を開始する前に、LUNの移動先となるボリュームを用意しておく必要があります。

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 移動するLUNを右クリックし、 ⋮ *[LUNの移動]*を選択します。

   ONTAP 9.10.1 では、 LUN を既存のボリューム * または新しいボリューム * に移動するように選択します。

   新しいボリュームの作成を選択した場合は、ボリュームの仕様を指定します。
3. [移動（ Move ）] をクリックします。

CLI

ONTAP CLIを使用してLUNを移動します。

1. LUNを移動します。

   ```
   lun move start
   ```

   ごく短時間、元のボリュームとデスティネーションボリュームの両方でLUNが表示されます。これは移動が完了するまでの一時的な状態で、想定内の動作です。
2. 移動のステータスを追跡し、正常に完了したことを確認します。

   ```
   lun move show
   ```

関連情報

- "選択的LUNマップ"

LUNの削除

不要になった LUN は Storage Virtual Machine （ SVM ）から削除できます。

開始する前に

LUNを削除する前に、そのigroupからLUNのマッピングを解除する必要があります。

手順

1. アプリケーションまたはホストがLUNを使用していないことを確認します。
2. igroupからLUNのマッピングを解除します。

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. LUNを削除します。

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. LUNが削除されたことを確認します。

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type      Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

LUNヲコピースルサイノコウリョジコウ

LUNをコピーする前に、特定の事項について理解しておく必要があります。

クラスタ管理者は、コマンドを使用して、クラスタ内のStorage Virtual Machine（SVM）間でLUNをコピーできます `lun copy`。クラスタ管理者は、Storage Virtual Machine（SVM）間のLUNコピー処理を実行する前に、コマンドを使用してSVMピア関係を確立する必要があります `vserver peer create`。ソースボリュームにSISクローン用の十分なスペースが必要です。

スナップショット内のLUNは、コマンドのソースLUNとして使用できます `lun copy`。コマンドを使用してLUNをコピーする `lun copy`と、LUNコピーに対する読み取りと書き込みがすぐに可能になります。ソースLUNは、LUNコピーを作成しても変更されません。ソースLUNとLUNコピーは、LUNシリアル番号が異なる一意のLUNとして存在します。ソースLUNに加えられた変更はLUNコピーには反映されず、LUNコピーに加えられた変更はソースLUNにも反映されません。ソースLUNのLUNマッピングは新しいLUNにコピーされないため、LUNコピーをマッピングする必要があります。

Snapshotによるデータ保護はボリュームレベルで行われます。そのため、ソースLUNのボリュームとは異なるボリュームにLUNをコピーする場合、デスティネーションLUNにはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用のSnapshotが確立されていない場合、LUNコピーのSnapshotは作成されません。

LUNのコピーはノンストップオペレーションです。

次のタイプのLUNはコピーできません。

- ファイルから作成されたLUN

- NVFAIL状態のLUN
- 負荷共有関係にあるLUN
- プロトコルエンドポイントクラスのLUN

の詳細については `lun copy`、を"ONTAPコマンド リファレンス"参照してください。

LUNの構成済みスペースと使用済みスペースを確認する

LUN の設定済みスペースと実際に使用されているスペースを把握しておくと、スペース再生時に再生可能なスペースの量、データを含むリザーブスペースの量、および LUN の設定済みの合計サイズと実際に使用されているサイズを特定するのに役立ちます。

ステップ

1. LUNの設定済みスペースと実際に使用されているスペースを表示します。

   ```
   lun show
   ```

   次の例は、vs3というStorage Virtual Machine（SVM）内のLUNの設定済みスペースと実際に使用されているスペースを示しています。

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- ------------------      ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

   の詳細については `lun show`、を"ONTAPコマンド リファレンス"参照してください。

ストレージQoSを使用してLUNへのI/Oパフォーマンスを制御および監視

LUN への入出力（ I/O ）パフォーマンスは、 LUN をストレージ QoS ポリシーグループに割り当てることによって制御できます。I/O パフォーマンスを制御することで、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりできます。

タスクの内容

ポリシーグループは最大スループット制限（ 100MB/s など）を適用します。ポリシーグループは最大スループットを指定せずに作成することもでき、ワークロードの制御に先立ってパフォーマンスを監視できます。

FlexVolボリュームとLUNを含むStorage Virtual Machine（SVM）をポリシーグループに割り当てることもできます。

ポリシーグループへの LUN の割り当てについては、次の要件に注意してください。

- LUN は、ポリシーグループが属する SVM に含まれている必要があります。

  SVM は、ポリシーグループを作成するときに指定します。

- LUN をポリシーグループに割り当てた場合、その LUN を含むボリュームまたは SVM をポリシーグループに割り当てることはできなくなります。

ストレージQoSの使用方法の詳細については、を参照して"システムアドミニストレーションリファレンス"ください。

手順

1. コマンドを使用し `qos policy-group create`て、ポリシーグループを作成します。

   の詳細については `qos policy-group create`、を"ONTAPコマンド リファレンス"参照してください。

2. `lun create`コマンドまたは `lun modify`コマンドでパラメータを指定し `-qos-policy-group`て、LUNをポリシーグループに割り当てます。

   の詳細については `lun`、を"ONTAPコマンド リファレンス"参照してください。

3. パフォーマンスデータを表示するには、コマンドを使用し `qos statistics`ます。
4. 必要に応じて、コマンドを使用し `qos policy-group modify`てポリシーグループの最大スループット制限を調整します。

   の詳細については `qos policy-group modify`、を"ONTAPコマンド リファレンス"参照してください。

LUNを効果的に監視するためのツール

LUN を効果的に監視し、スペース不足になるのを防ぐためのツールが用意されています。

- Active IQ Unified Manager は、環境内のすべてのクラスタのすべてのストレージを管理するための無償ツールです。
- System Manager は、 ONTAP に組み込まれているグラフィカルユーザインターフェイスです。クラスタレベルで必要なストレージを手動で管理できます。
- OnCommand Insight を使用すると、ストレージインフラの状況を一元的に確認できます。また、自動監視やアラートの機能、および LUN 、ボリューム、アグリゲートでストレージスペース不足が発生したときにレポートする機能を設定できます。

移行した**LUN**の機能と制限事項

SAN環境では、7-ModeボリュームをONTAPに移行する際にサービスの中断が必要です。移行を完了するには、ホストをシャットダウンする必要があります。移行後は、ONTAPでデータの提供を開始する前にホスト構成を更新する必要があります。

ホストをシャットダウンできる時間帯にメンテナンスのスケジュールを設定して、移行を完了する必要があり

ます。

Data ONTAP 7-ModeからONTAPに移行されたLUNには、LUNの管理方法に影響する特定の機能と制限があります。

移行したLUNでは、次の操作を実行できます。

- コマンドを使用してLUNを表示する `lun show`
- コマンドを使用して、7-Modeボリュームから移行したLUNのインベントリを表示する `transition 7-mode show`
- 7-Mode Snapshotからボリュームをリストアする

  ボリュームをリストアすると、Snapshotにキャプチャされたすべてのが移行されます。
- コマンドを使用して、7-Mode Snapshotから単一のLUNをリストアする `snapshot restore-file`
- 7-Mode Snapshot内のLUNのクローンを作成する
- 7-Mode Snapshotにキャプチャされたから一連のブロックをリストアする
- 7-Mode Snapshotを使用したボリュームのFlexCloneの作成

移行したLUNでは、次の操作は実行できません。

- Snapshotでバックアップされたボリューム内にキャプチャされたLUNクローンにアクセスする

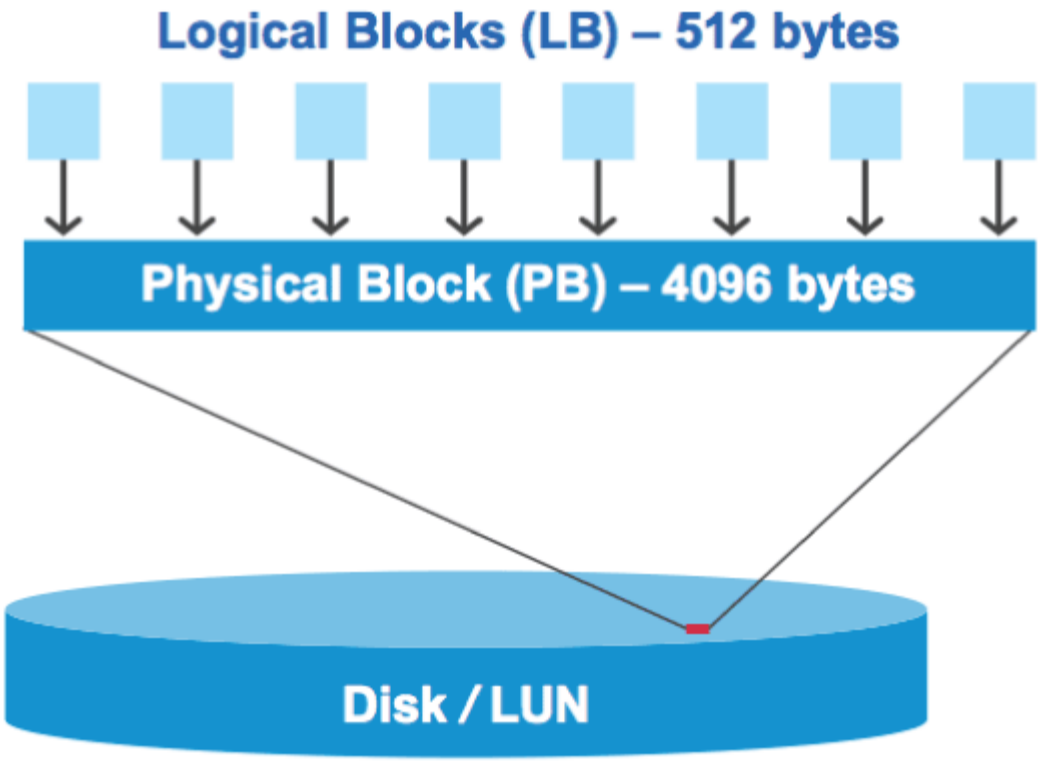
関連情報

- "コピーベースの移行"
- "lun show"

適切にアライメントされた**LUN**での**I/O**ミスアライメントの概要

ONTAPでは、適切にアライメントされたLUNでI/Oのミスアライメントが報告されることがあります。一般に、これらのミスアライメントの警告は、LUNが適切にプロビジョニングされていて、パーティションテーブルが正しいことに確信があれば無視してかまいません。

LUNとハードディスクはどちらもストレージをブロックとして提供します。ホスト上のディスクのブロックサイズは512バイトであるため、LUNはそのサイズのブロックをホストに提供しますが、実際にはより大きな4KBのブロックを使用してデータを格納します。ホストで使用される512バイトのデータブロックを論理ブロックと呼びます。LUNがデータの格納に使用する4KBのデータブロックを物理ブロックと呼びます。つまり、4KBの各物理ブロックに512バイトの論理ブロックが8個あります。



ホストオペレーティングシステムは、任意の論理ブロックで読み取りまたは書き込みのI/O処理を開始できます。I/O処理は、物理ブロック内の最初の論理ブロックで開始されたときにのみアライメントされたとみなされます。I/O処理が物理ブロックの始点でもない論理ブロックから開始された場合、I/Oはミスアライメントされているとみなされます。ONTAPは、LUNのミスアライメントを自動的に検出して報告します。ただし、ミスアライメントI/Oがあるからといって、LUNもミスアライメントされているとは限りません。適切にアライメントされたLUNで、ミスアライメントI/Oが報告される可能性があります。

さらに調査が必要な場合は、"NetAppナレッジベース: LUN 上の未調整 IO を識別するにはどうすればよいでしょうか?"

アライメントの問題を修正するためのツールの詳細については、 + を参照してください

- "Windows Unified Host Utilities 7.1"
- "SANストレージのドキュメントのプロビジョニング"

LUNのOSタイプを使用したI/Oアライメントの実現

ONTAP 9 .7以前の場合は、OSのパーティショニングスキームでI/Oがアライメントされるように、オペレーティングシステムに最も近い推奨ONTAP LUN値を使用する必要があります `ostype`。

ホストオペレーティングシステムで採用されているパーティション方式は、I/Oのミスアライメントの主な要因です。一部のONTAP LUN `ostype`値では、「プレフィックス」と呼ばれる特別なオフセットを使用して、アライメント対象のホストオペレーティングシステムが使用するデフォルトのパーティショニングスキームを有効にします。

> 場合によっては、I/Oアライメントを実行するためにカスタムのパーティショニングテーブルが必要になることがあります。ただし、「prefix」の値がより大きい値の `0`場合 `ostype`、カスタムパーティションを使用するとミスアライメントI/Oが発生する可能性があります。

ONTAP 9.7以前でプロビジョニングされたLUNの詳細については、"NetAppナレッジベース: LUN 上の非整列 IO を識別する方法" 。

デフォルトでは、ONTAP 9 .8以降でプロビジョニングされる新しいLUNには、すべてのLUN OSタイプでプレフィックスおよびサフィックスサイズが0に設定されます。I/Oは、デフォルトでサポートされるホストOSとアライメントされている必要があります。

Linux固有のI/Oアライメントに関する考慮事項

Linuxディストリビューションでは、データベース、各種ボリュームマネージャ、ファイルシステムのrawデバイスなど、さまざまな方法でLUNを使用できます。rawデバイスまたは論理ボリューム内の物理ボリュームとして使用される場合、LUNにパーティションを作成する必要はありません。

RHEL 5以前およびSLES 10以前で、ボリュームマネージャを使用せずにLUNを使用する場合は、アライメントされたオフセットから始まる1つのパーティション（8個の論理ブロックの偶数倍のセクター）を持つようにLUNをパーティショニングする必要があります。

Solaris LUN固有のI/Oアライメントに関する考慮事項

ostypeと `solaris_efi`ostypeのどちらを使用するかを決定する際には、さまざまな要因を考慮する必要があり `solaris`ます。

詳細については、を参照してください "Solaris Host Utilities Installation and Administration Guide"。

ESXブートLUNがミスアライメントとして報告される

ESXブートLUNとして使用されるLUNは、通常、ミスアライメントとしてONTAPから報告されます。ESXではブートLUNに複数のパーティションが作成されるため、アライメントが非常に困難になります。ミスアライメントされたI/Oの総量は小さいため、ミスアライメントされたESXブートLUNは通常、パフォーマンス上の問題にはなりません。VMwareを使用してLUNが正しくプロビジョニングされていれば、 `ostype`対処は不要です。

関連情報

"VMware vSphereをはじめとする仮想環境、NetAppストレージシステム向けのゲストVMファイルシステムのパーティション/ディスクアライメント"

LUNがオフラインになった場合の問題の対処方法

書き込みに使用できるスペースがない場合、LUNはデータの整合性を維持するためにオフラインになります。LUNのスペースが不足してオフラインになる原因はさまざまですが、いくつかの方法で問題に対処できます。

状況	可能です
アグリゲートがフルです	• ディスクを追加します。 • コマンドを使用して `volume modify`、使用可能なスペースがあるボリュームを縮小します。 • 使用可能なスペースがあるスペースギャランティボリュームがある場合は、コマンドを使用して `volume modify`ボリュームのスペースギャランティをに変更します `none`。
ボリュームがフルですが、包含アグリゲートに利用可能なスペースがあります	• スペースギャランティボリュームの場合は、コマンドを使用し `volume modify`てボリュームのサイズを拡張します。 • シンプロビジョニングボリュームの場合は、コマンドを使用し `volume modify`てボリュームの最大サイズを拡張します。 ボリュームの自動拡張が有効になっていない場合は、を使用 `volume modify -autogrow-mode`して有効にします。 • コマンドを使用してSnapshotを手動で削除する `volume snapshot delete`か、コマンドを使用し `volume snapshot autodelete modify`てSnapshotを自動的に削除します。

関連情報

"ディスクとローカル階層（アグリゲート）の管理"

"論理ストレージ管理"

ホストで**iSCSI LUN**が表示されない場合のトラブルシューティング

iSCSI LUNは、ホストではローカルディスクとして表示されます。ストレージシステムのLUNをホストでディスクとして使用できない場合は、構成設定を確認する必要があります。

構成設定	対処方法：
ケーブル接続	ホストとストレージシステムの間のケーブルが正しく接続されていることを確認します。

構成設定	対処方法：
ネットワーク接続	ホストとストレージシステムの間にTCP / IP接続が確立されていることを確認します。 • ストレージシステムのコマンドラインから、iSCSIに使用されているホストインターフェイスをpingします。 `ping -node node_name -destination host_ip_address_for_iSCSI` • ホストのコマンドラインから、iSCSIに使用されているストレージシステムインターフェイスをpingします。 `ping -node node_name -destination host_ip_address_for_iSCSI`
システム要件	構成のコンポーネントが認定されていることを確認します。また、ホストオペレーティングシステム（OS）のサービスパックレベル、イニシエータバージョン、ONTAPバージョンなどのシステム要件を満たしていることも確認してください。Interoperability Matrixに最新のシステム要件が記載されています。
ジャンボフレーム	ご使用の構成でジャンボフレームを使用している場合は、ネットワークパス（ホストのイーサネットNIC、ストレージシステム、スイッチ）上のすべてのデバイスでジャンボフレームが有効になっていることを確認します。
iSCSIサービスステータス	iSCSIサービスのライセンスが設定され、ストレージシステムで開始されていることを確認します。
イニシエータログイン	イニシエータがストレージシステムにログインしていることを確認します。ログインしているイニシエータがコマンド出力に表示されない場合は `iscsi initiator show`、ホストのイニシエータ設定を確認します。また、ストレージシステムがイニシエータのターゲットとして設定されていることを確認します。
iSCSIノード名（IQN）	正しいイニシエータのノード名をigroup設定で使用していることを確認します。ホストでは、イニシエータのツールとコマンドを使用してイニシエータのノード名を表示できます。igroupおよびホストに設定されているイニシエータのノード名が一致している必要があります。
LUNマツヒンク	LUNがigroupにマッピングされていることを確認します。ストレージシステムコンソールでは、次のいずれかのコマンドを使用できます。 • `lun mapping show`すべてのLUN、およびLUNがマッピングされているigroupを表示します。 • `lun mapping show -igroup`特定のigroupにマッピングされているLUNを表示します。

構成設定	対処方法：
iSCSI LIFの有効化	iSCSI論理インターフェイスが有効になっていることを確認します。

関連情報

- "NetApp Interoperability Matrix Tool"
- "lun mapping show"

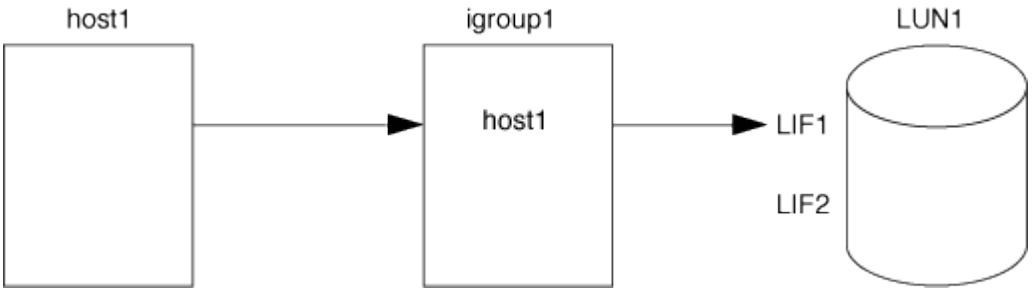
igroupとポートセットを管理します。

ポートセットと**igroup**によって**LUN**アクセスを制限する方法

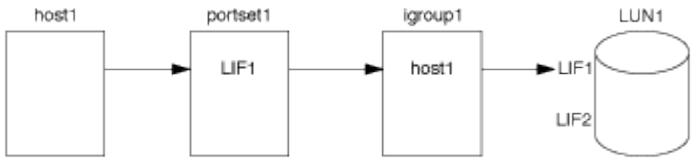
Selective LUN Map（SLM；選択的LUNマップ）に加えて、igroupおよびポートセットを使用してLUNへのアクセスを制限することができます。

ポートセットとSLMを併用すると、特定のターゲットのアクセスを特定のイニシエータだけに制限できます。SLMとポートセットを併用する場合、LUNには、そのLUNを所有するノードおよびノードのHAパートナーのポートセットに含まれる一連のLIF経由でアクセスできます。

次の例では、initiator1にポートセットがありません。ポートセットがない場合、initiator1はLIF1とLIF2の両方を介してLUN1にアクセスできます。



ポートセットを使用すると、LUN1へのアクセスを制限できます。次の例では、initiator1はLIF1経由でのみLUN1にアクセスできます。ただし、LIF2がportset1に含まれていないため、LIF2を介してLUN1にアクセスすることはできません。



関連情報

- 選択的LUNマップ
- ポートセットを作成してigroupにバインドする

SANイニシエータと**igroup**の表示と管理

System Managerを使用して、イニシエータグループ（igroup）とイニシエータを表示および管理できます。

タスクの内容

- イニシエータグループは、どのホストがストレージシステム上の特定のLUNにアクセスできるかを識別します。
- イニシエータとイニシエータグループを作成したあと、それらを編集したり削除したりすることもできます。
- SANイニシエータグループおよびイニシエータを管理するには、次のタスクを実行できます。
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

SANイニシエータグループの表示と管理

System Managerを使用して、イニシエータグループ（igroup）のリストを表示できます。リストから追加の処理を実行できます。

手順

1. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストがページに表示されます。リストが大きい場合は、ページの右下隅にあるページ番号をクリックして、リストの追加ページを表示できます。

   igroupに関するさまざまな情報が列に表示されます。9.11.1以降では、igroupの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると、詳細が表示されます。

2. （オプション）：リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。
   - * 検索 *
   - *ダウンロード*リスト。
   - *リストの*または*隠す*列を表示します。
   - *リスト内のデータをフィルタリングします。
3. リストから操作を実行できます。
   - をクリックし てigroupを追加します。
   - igroup名をクリックすると、そのigroupの詳細が表示されます。* Overview *ページが表示されます。

     概要*ページでは、igroupに関連付けられているLUNを確認できます。また、処理を開始してLUNの作成やLUNのマッピングを行うこともできます。「*すべてのSANイニシエータ」をクリックしてメインリストに戻ります。

   - igroupにカーソルを合わせ、igroup名の横にあるをクリックして、 igroupを編集または削除します。
   - igroup名の左側の領域にカーソルを合わせ、チェックボックスをオンにします。イニシエータグループに追加をクリックすると、そのigroupを別のigroupに追加できます。
   - Storage VM *列で、Storage VMの名前をクリックして詳細を確認します。

SANイニシエータの表示と管理

System Managerを使用して、イニシエータのリストを表示できます。リストから追加の処理を実行できます。

手順

1. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストがページに表示されます。

2. イニシエータを表示するには、次の手順に従います。

   - FCイニシエータの一覧を表示するには、* FCイニシエータ*タブをクリックします。
   - iSCSIイニシエータのリストを表示するには、* iSCSIイニシエータ*タブをクリックします。

     各列には、イニシエータに関するさまざまな情報が表示されます。

   9.11.1以降では、イニシエータの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると、詳細が表示されます。

3. （オプション）：リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。
   - * Search *：特定のイニシエータを一覧表示します。
   - *ダウンロード*リスト。
   - *リストの*または*隠す*列を表示します。
   - *リスト内のデータをフィルタリングします。

ネストされた**igroup**を作成する

ONTAP 9.9.1以降では、他の既存のigroupで構成されるigroupを作成できます。

1. System Manager で、 * Host > SAN Initiator Groups * をクリックし、 * Add * をクリックします。
2. igroup 名 * と * 概要 * を入力します。

   この説明はigroupエイリアスとして機能します。

3. Storage VM * および * Host Operating System * を選択します。

   ネストされたigroupのOSタイプは、作成後は変更できません。

4. イニシエータグループメンバー * で、 * 既存のイニシエータグループ * を選択します。
   - Search * を使用して、追加する igroup を検索して選択できます。

igroupを複数の**LUN**にマッピング

ONTAP 9.9.1以降では、igroupを複数のLUNに同時にマッピングできます。

1. System Manager で、 * Storage > LUNs * をクリックします。
2. マッピングするLUNを選択します。
3. [* 詳細 *] をクリックし、 [* イニシエータ・グループへのマップ *] をクリックします。

   選択したigroupが選択したLUNに追加されます。既存のマッピングは上書きされません。

ポートセットを作成して**igroup**にバインドする

を使用するだけでなく"選択的LUNマップ（SLM）"、ポートセットを作成してigroupにバインドし、イニシエータがLUNへのアクセスに使用するLIFをさらに制限することもできます。

ポートセットをigroupにバインドしない場合、igroup内のすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナーのすべてのLIFを介してマッピングされたLUNにアクセスできます。

開始する前に

少なくとも1つのLIFと1つのigroupが必要です。

インターフェイスグループを使用しないかぎり、iSCSIとFCの冗長性を確保するために推奨されるLIFの数は2つです。インターフェイスグループに推奨されるLIFは1つだけです。

タスクの内容

ノード上にLIFが3つ以上あり、特定のイニシエータを一部のLIFに制限する場合は、ポートセットとSLMを併用する方が効果的です。ポートセットを使用しない場合は、LUNへのアクセス権を持つすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナー経由でノード上のすべてのターゲットにアクセスできます。

例 **19.** 手順

System Manager

ONTAP 9 .10.1以降では、System Managerを使用してポートセットを作成し、igroupにバインドできます。

ONTAP 9.10.1より前のリリースでポートセットを作成してigroupにバインドする必要がある場合は、ONTAP CLI手順 を使用する必要があります。

ONTAP 9.12.1 以降では、既存のポートセットがない場合は、ONTAP CLI 手順を使用して最初のポートセットを作成する必要があります。

1. System Manager で、 * Network > Overview > portsets * をクリックし、 * Add * をクリックします。
2. 新しいポートセットの情報を入力し、 * Add * をクリックします。
3. [*Hosts] ＞ [SAN Initiator Groups] をクリックします
4. ポートセットを新しい igroup にバインドするには、 * Add * をクリックします。

   ポートセットを既存のigroupにバインドするには、igroupを選択してをクリックし、 *[イニシエータグループの編集]*をクリックします。

関連情報

"イニシエータとigroupの表示と管理"

CLI

1. 適切なLIFを含むポートセットを作成します。

   `portset create -vserver` *`vserver_name`* `-portset` *`portset_name`* `-protocol` *`protocol`* `-port-name` *`port_name`*

   FCを使用する場合は、パラメータをに `fcp`指定します `protocol`。iSCSIを使用する場合は、パラメータをに `iscsi`指定します `protocol`。

2. igroupをポートセットにバインドします。

   `lun igroup bind -vserver` *`vserver_name`* `-igroup` *`igroup_name`* `-portset` *`portset_name`*

   の詳細については `lun igroup bind`、を"ONTAPコマンド リファレンス"参照してください。

3. ポートセットとLIFが正しいことを確認します。

   `portset show -vserver` *`vserver_name`*

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

ポートセットを管理します。

"選択的LUNマップ（SLM）"また、ポートセットを使用して、イニシエータがLUNへのアクセスに使用するLIFをさらに制限することもできます。

ONTAP 9 .10.1以降では、System Managerを使用して、ポートセットに関連付けられているネットワークインターフェイスを変更したり、ポートセットを削除したりできます。

ポートセットに関連付けられているネットワークインターフェイスの変更

1. System Managerで、*[ネットワーク]>[概要]>[ポートセット]*を選択します。
2. 編集するポートセットを選択し、*[ポートセットの編集]*を選択します。

ポートセットを削除します。

1. System Manager で、 * Network > Overview > portsets * をクリックします。
2. 単一のポートセットを削除するには、ポートセットを選択し、*[ポートセットの削除]*を選択します。

   複数のポートセットを削除するには、ポートセットを選択し、 * 削除 * をクリックします。

選択的**LUN**マップの概要

Selective LUN Map（SLM；選択的LUNマップ）を使用すると、ホストからLUNへのパスの数が削減されます。SLMで新しいLUNマップを作成すると、LUNを所有するノードとそのHAパートナーのパス経由でのみLUNにアクセスできます。

SLMを使用すると、ホストごとに1つのigroupを管理できます。また、ポートセットの操作やLUNの再マッピングを必要としない、無停止のLUN移動処理もサポートされます。

"ポートセット"SLMと併用すると、特定のターゲットのアクセスを特定のイニシエータだけに制限できます。SLMとポートセットを併用する場合、LUNには、そのLUNを所有するノードおよびノードのHAパートナーのポートセットに含まれる一連のLIF経由でアクセスできます。

すべての新しいLUNマップでは、SLMがデフォルトで有効になります。

SLMが**LUN**マップで有効になっているかどうかを確認する

ONTAP 9リリースで作成されたLUNと以前のバージョンから移行されたLUNが環境内に混在している場合は、特定のLUNで選択的LUNマップ（SLM）が有効になっているかどうかを確認しなければならないことがあります。

コマンドの出力に表示される情報を使用して、LUNマップでSLMが有効になっているかどうかを確認できます `lun mapping show -fields reporting-nodes, node`。SLMが有効になっていない場合は、コマンド出力の「reporting-nodes」列の下のセルにと表示されます。SLMが有効な場合、「nodes」列の下に表示されるノードのリストが「reporting-nodes」列に複製されます。

の詳細については `lun mapping show`、を"ONTAPコマンド リファレンス"参照してください。

SLMレポートノードリストの変更

LUNまたはLUNを含むボリュームを同じクラスタ内の別のハイアベイラビリティ（HA）ペアに移動する場合は、最適化されたアクティブなLUNパスが維持されるように、移動を開始する前に選択的LUNマップ（SLM）のレポートノードリストを変更する必要があります。

手順

1. デスティネーションノードとそのパートナーノードをアグリゲートまたはボリュームのレポートノードリストに追加します。

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

一貫した命名規則がある場合は、の代わりにを使用して、複数のLUNマッピングを同時に変更できます `igroup_prefix*` `igroup_name`。

2. ホストを再スキャンして、新しく追加したパスを検出します。
3. OSで必要な場合は、マルチパス ネットワークI/O（MPIO）構成に新しいパスを追加します。
4. 必要な移動処理のためのコマンドを実行して、処理が完了するまで待ちます。
5. I/Oがアクティブな最適パス経由で処理されていることを確認します。

```
lun mapping show -fields reporting-nodes
```

6. レポート ノード リストから、前のLUN所有者とそのパートナー ノードを削除します。

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. 既存のLUNマップからLUNが削除されていることを確認します。

```
lun mapping show -fields reporting-nodes
```

8. ホストOSの古いデバイスのエントリを削除します。
9. 必要に応じて、マルチパス構成ファイルを変更します。
10. ホストを再スキャンして古いパスが削除されたことを確認します。+ ホストを再スキャンする手順については、ホストのマニュアルを参照してください。

iSCSIプロトコルを管理します。

最適なパフォーマンスを実現するためのネットワークの設定

イーサネットネットワークによってパフォーマンスは大きく異なります。特定の設定値を選択することで、iSCSIに使用するネットワークのパフォーマンスを最大限に高めることができます。

手順

1. ホストポートとストレージポートを同じネットワークに接続します。

   同じスイッチに接続することを推奨します。ルーティングを使用することはできません。

2. 最も速度の速いポートを選択し、それらをiSCSI専用にします。

   10GbEポートが最適です。最小要件は1GbEポートです。

3. すべてのポートでイーサネット フロー制御を無効にします。

   CLIを使用してイーサネットポートのフロー制御を設定するには、を参照してください"ネットワーク管理"。

4. ジャンボフレームを有効にする（通常MTUは9000）。

   イニシエータ、ターゲット、スイッチを含むデータパス内のすべてのデバイスでジャンボフレームがサポートされている必要があります。そうしないと、ジャンボフレームを有効にすると、ネットワークのパフォーマンスが大幅に低下します。

SVMを**iSCSI**用に設定する

iSCSI用にStorage Virtual Machine（SVM）を設定するには、SVM用のLIFを作成し、それらのLIFにiSCSIプロトコルを割り当てる必要があります。

タスクの内容

iSCSIプロトコルを使用してデータを提供する各SVMについて、各ノードに少なくとも1つのiSCSI LIFが必要です。冗長性を確保するために、ノードごとに少なくとも2つのLIFを作成する必要があります。

例 **20.** 手順

System Manager

ONTAP System Manager（9.7以降）でiSCSI用のStorage VMを設定します。

新しい**Storage VM**で**iSCSI**を設定する方法	既存の**Storage VM**で**iSCSI**を設定する方法
1. System Managerで、* Storage > Storage VM*をクリックし、* Add *をクリックします。 2. Storage VMの名前を入力してください。 3. アクセスプロトコル*として「* iSCSI *」を選択します。 4. Enable iSCSI（iSCSIを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。+各ノードに少なくとも2つのネットワークインターフェイスが必要です。 5. [保存（ Save ）] をクリックします。	1. System Manager で、 * Storage > Storage VM*をクリックします。 2. 設定するStorage VMをクリックします。 3. [設定]*タブをクリックし、iSCSIプロトコルの横にあるをクリックし ます。 4. Enable iSCSI（iSCSIを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。+各ノードに少なくとも2つのネットワークインターフェイスが必要です。 5. [保存（ Save ）] をクリックします。

CLI

ONTAP CLIを使用してiSCSI用にStorage VMを設定します。

1. SVMがiSCSIトラフィックをリスンするようにします。

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. iSCSIに使用する各ノードにSVM用のLIFを作成します。

   - ONTAP 9.6以降：

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - ONTAP 9.5以前：

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. LIFが正しく設定されたことを確認します。

   ```
   network interface show -vserver vserver_name
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

4. iSCSIが稼働していること、およびそのSVMのターゲットIQNを確認します。

   ```
   vserver iscsi show -vserver vserver_name
   ```

5. ホストから、LIFへのiSCSIセッションを作成します。

関連情報

- "NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"

イニシエータのセキュリティポリシー方式を定義する

イニシエータとその認証方法のリストを定義できます。また、ユーザ定義の認証方法がないイニシエータに適用されるデフォルトの認証方法を変更することもできます。

タスクの内容

製品のセキュリティポリシーアルゴリズムを使用して一意のパスワードを生成することも、使用するパスワードを手動で指定することもできます。

一部のイニシエータが16進数のCHAPシークレットパスワードをサポートしていません。

手順

1. コマンドを使用し `vserver iscsi security create`て、イニシエータのセキュリティポリシー方式を作成します。

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. 画面に表示されるコマンドに従ってパスワードを追加します。

   インバウンドとアウトバウンドのCHAPユーザ名とパスワードを使用して、イニシエータiqn.1991-05.com.microsoft:host1のセキュリティポリシー方式を作成します。

関連情報

- iSCSI認証の仕組み
- CHAP認証

SVMの**iSCSI**サービスを削除する

Storage Virtual Machine（SVM）の不要になったiSCSIサービスは削除できます。

開始する前に

iSCSI サービスを削除するには、 iSCSI サービスの管理ステータスが「所有」状態である必要があります。コマンドを使用すると、管理ステータスをdownに切り替えることができます `vserver iscsi modify`。

手順

1. コマンドを使用し `vserver iscsi modify`て、LUNへのI/Oを停止します。

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. コマンドを使用し `vserver iscsi delete`て、SVMからiSCSIサービスを削除します。

```
vserver iscsi delete -vserver vs_1
```

3. を使用 `vserver iscsi show command`して、iSCSIサービスがSVMから削除されたことを確認します。

```
vserver iscsi show -vserver vs1
```

iSCSIセッションのエラーリカバリに関する詳細情報の取得

iSCSIセッションのエラーリカバリレベルを上げると、iSCSIエラーリカバリに関する詳細情報を取得できます。高いレベルのエラーリカバリを使用すると、iSCSIセッションのパフォーマンスが若干低下する可能性があります。

タスクの内容

ONTAPは、iSCSIセッションに対してエラーリカバリレベル0を使用するようにデフォルトで設定されています。エラーリカバリレベル1または2に対応したイニシエータを使用している場合は、エラーリカバリレベルを上げるように選択できます。変更したセッションのエラーリカバリレベルは、新しく作成されたセッションにのみ影響し、既存のセッションには影響しません。

ONTAP 9 .4以降では、 `max-error-recovery-level`コマンドおよび `iscsi modify`コマンドでオプションはサポートされません `iscsi show`。

手順

1. advancedモードに切り替えます。

```
set -privilege advanced
```

2. コマンドを使用して、現在の設定を確認します `iscsi show`。

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
------- ------------------------
vs3     0
```

3. コマンドを使用して、エラーリカバリレベルを変更します `iscsi modify`。

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

SVMをiSNSサーバに登録

iSNSサーバに登録するようにStorage Virtual Machine（SVM）を設定するには、コマンドを使用し `vserver iscsi isns`ます。

タスクの内容

コマンドは、 `vserver iscsi isns create`SVMをiSNSサーバに登録します。SVM には、 iSNS サーバの設定や管理を行うコマンドはありません。iSNS サーバを管理するには、 iSNS サーバのベンダーが提供するサーバ管理ツールまたはインターフェイスを使用します。

手順

1. iSNS サーバで、 iSNS サービスが開始しており、サービスを提供可能な状態であることを確認します。
2. データポートにSVM管理LIFを作成します。

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

   の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。
3. SVMにiSCSIサービスを作成します（存在しない場合）。

   ```
   vserver iscsi create -vserver SVM_name
   ```
4. iSCSIサービスが正常に作成されたことを確認します。

   ```
   iscsi show -vserver SVM_name
   ```
5. SVMのデフォルトルートが存在することを確認します。

   ```
   network route show -vserver SVM_name
   ```
6. SVMのデフォルトルートが存在しない場合は、デフォルトルートを作成します。

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

   の詳細については `network route create`、を"ONTAPコマンド リファレンス"参照してください。
7. iSNSサービスに登録するようにSVMを設定します。

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   IPv4アドレスファミリーとIPv6アドレスファミリーの両方がサポートされます。iSNS サーバのアドレスファミリーは、 SVM 管理 LIF のアドレスファミリーと同じである必要があります。

   たとえば、IPv4アドレスを使用するSVM管理LIFを、IPv6アドレスを使用するiSNSサーバに接続することはできません。
8. iSNSサービスが実行されていることを確認します。

   ```
   vserver iscsi isns show -vserver SVM_name
   ```
9. iSNSサービスが実行されていない場合は開始します。

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

ストレージシステムの**iSCSI**エラーメッセージを解決する

iSCSI関連の一般的なエラーメッセージは、コマンドで確認できます `event log`

`show`。これらのメッセージの意味と、特定された問題の解決方法を把握する必要があります。

次の表に、最も一般的なエラーメッセージと、それらを解決する手順を示します。

メッセージ	説明	対処方法：
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	このインターフェイスの iSCSI サービスが有効になっていません。	インターフェイスでiSCSIサービスを有効にするには、コマンドを使用し `iscsi interface enable`ます。例： `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	指定されたイニシエータに対して CHAP が正しく設定されていません。	CHAP 設定をチェックします。ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名およびパスワードを使用できません。 • ストレージシステムのインバウンドクレデンシャルは、イニシエータのアウトバウンドクレデンシャルと一致する必要があります • ストレージシステムのアウトバウンドクレデンシャルは、イニシエータのインバウンドクレデンシャルと一致する必要があります

の詳細については `event log show`、を"ONTAPコマンド リファレンス"参照してください。

iSCSI LIFの自動フェイルオーバーの有効化または無効化

ONTAP 9.11.1以降にアップグレードした場合は、ONTAP 9.10.1以前で作成したすべてのiSCSI LIFでLIFの自動フェイルオーバーを手動で有効にする必要があります。

ONTAP 9 .11.1以降では、オールフラッシュSANアレイプラットフォームでiSCSI LIFに対してLIFの自動フェイルオーバーを有効にすることができます。ストレージフェイルオーバーが発生すると、iSCSI LIFはホームノードまたはポートからHAパートナーノードまたはポートに自動的に移行され、フェイルオーバーの完了後に再び移行されます。または、iSCSI LIFのポートが正常な状態でなくなった場合、そのLIFは現在のホームノードの正常なポートに自動的に移行され、ポートが正常な状態に戻った時点で元のポートに戻ります。を使用すると、iSCSIで実行されているSANワークロードは、フェイルオーバー後にI/Oサービスを迅速に再開できます。

ONTAP 9 .11.1以降では、次のいずれかの条件に該当する場合、新しく作成したiSCSI LIFでLIFの自動フェイルオーバーがデフォルトで有効になります。

- SVMにiSCSI LIFがありません

- LIFの自動フェイルオーバーがSVMのすべてのiSCSI LIFで有効になっている

iSCSI LIFの自動フェイルオーバーの有効化

ONTAP 9.10.1以前で作成したiSCSI LIFでは、デフォルトでLIFの自動フェイルオーバーが有効になっていません。SVM上にLIFの自動フェイルオーバーが有効になっていないiSCSI LIFがある場合、新しく作成したLIFでもLIFの自動フェイルオーバーは有効になりません。LIFの自動フェイルオーバーが有効になっていない状態でフェイルオーバーが発生すると、iSCSI LIFは移行されません。

詳細については、をご覧ください "LIFのフェイルオーバーとギブバック"。

ステップ

1. iSCSI LIFの自動フェイルオーバーを有効にします。

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

SVM上のすべてのiSCSI LIFを更新するには、の代わりに `lif`を使用し `-lif*`ます。

iSCSI LIFの自動フェイルオーバーを無効にする

ONTAP 9 10.1以前で作成したiSCSI LIFに対するiSCSI LIFの自動フェイルオーバーを有効にしていた場合は、無効にすることもできます。

ステップ

1. iSCSI LIFの自動フェイルオーバーを無効にします。

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

SVM上のすべてのiSCSI LIFを更新するには、の代わりに `lif`を使用し `-lif*`ます。

関連情報

- "LIFの作成"
- シユトウ"LIFを移行する"
- シユトウ"LIFをホームポートにリバートします。"
- "LIFのフェイルオーバーを設定する"

FCプロトコルを管理します。

FC用のSVMの設定

FC用にStorage Virtual Machine（SVM）を設定するには、SVM用のLIFを作成し、それらのLIFにFCプロトコルを割り当てる必要があります。

開始する前に

FCライセンス（"ONTAP Oneに付属"）があり、有効になっている必要があります。FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはになります。 `down`LIFとSVMを動作させるには、FCサービスを有効にする必要があります。イニシエータをホストするには、SVM内のすべてのFC LIFで単一イニシエータゾーニングを使用する必要があります。

タスクの内容

NetAppでは、FCプロトコルを使用してデータを提供する各SVMについて、ノードごとに少なくとも1つのFC LIFがサポートされます。ノードごとに1つのLIFを接続した状態で、ノードごとに2つのLIFと2つのファブリックを使用する必要があります。これにより、ノードレイヤとファブリックで冗長性が確保されます。

例 **21.** 手順

System Manager

ONTAP System Manager（9.7以降）でiSCSI用のStorage VMを設定します。

新しい**Storage VM**で**FC**を設定する方法	既存の**Storage VM**に**FC**を設定するには
1. System Managerで、* Storage > Storage VM*をクリックし、* Add *をクリックします。 2. Storage VMの名前を入力してください。 3. アクセスプロトコル*として「* FC」を選択します。 4. [FCを有効にする]をクリックします。+ FCポートが自動的に割り当てられます。 5. [保存（ Save ）] をクリックします。	1. System Manager で、 * Storage > Storage VM*をクリックします。 2. 設定するStorage VMをクリックします。 3. [Settings]*タブをクリックし、FCプロトコルの横にあるをクリックし ⚙ ます。 4. Enable FC（FCを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。+ FCポートが自動的に割り当てられます。 5. [保存（ Save ）] をクリックします。

CLI

1. SVMでFCサービスを有効にします。

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. FCを提供する各ノードのSVM用のLIFを2つ作成します。

   - ONTAP 9.6以降：

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - ONTAP 9.5以前：

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. LIFが作成され、動作ステータスがになっていることを確認し `online`ます。

   ```
   network interface show -vserver vserver_name lif_name
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "NetAppのサポート"
- "NetApp Interoperability Matrix Tool"

- クラスタSAN環境でのLIFに関する考慮事項

SVMのFCサービスを削除する

Storage Virtual Machine（SVM）の不要になったFCサービスは削除できます。

開始する前に

SVM の FC サービスを削除するには、事前に管理ステータスを「所有」にする必要があります。管理ステータスをdownに設定するには、コマンドまたは `vserver fcp stop`コマンドを使用し `vserver fcp modify`ます。

手順

1. コマンドを使用し `vserver fcp stop`て、LUNへのI/Oを停止します。

   ```
   vserver fcp stop -vserver vs_1
   ```

2. コマンドを使用し `vserver fcp delete`て、SVMからサービスを削除します。

   ```
   vserver fcp delete -vserver vs_1
   ```

3. を使用し `vserver fcp show`て、FCサービスがSVMから削除されたことを確認します。

   ```
   vserver fcp show -vserver vs_1
   ```

FCoEジャンボフレーム用のMTUの推奨設定

Fibre Channel over Ethernet（FCoE）の場合は、CNAのイーサネットアダプタ部分のジャンボフレームを9000 MTUで設定する必要があります。CNAのFCoEアダプタ部分については、ジャンボフレームを1500 MTU以上に設定する必要があります。イニシエータ、ターゲット、および介在するすべてのスイッチがジャンボフレームをサポートし、ジャンボフレーム用に設定されている場合にのみ、ジャンボフレームを設定します。

NVMeプロトコルを管理します。

SVMのNVMeサービスを開始する

Storage Virtual Machine（SVM）でNVMeプロトコルを使用する前に、SVMでNVMeサービスを開始する必要があります。

開始する前に

システムでNVMeプロトコルが許可されている必要があります。

次のNVMeプロトコルがサポートされます。

プロトコル	先頭のドキュメント	許可するユーザ
TCP	ONTAP 9 10.1	デフォルト
FCP	ONTAP 9.4	デフォルト

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. NVMeプロトコルが許可されていることを確認します。

   ```
   vserver nvme show
   ```

3. NVMeプロトコルサービスを作成します。

   ```
   vserver nvme create
   ```

4. SVMでNVMeプロトコルサービスを開始します。

   ```
   vserver nvme modify -status -admin up
   ```

SVMからNVMeサービスを削除する

必要に応じて、Storage Virtual Machine（SVM）からNVMeサービスを削除できます。

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. SVMでNVMeサービスを停止します。

   ```
   vserver nvme modify -status -admin down
   ```

3. NVMeサービスを削除します。

   ```
   vserver nvme delete
   ```

ネームスペースのサイズを変更する

ONTAP 9 .10.1以降では、ONTAP CLIを使用してNVMeネームスペースのサイズを拡張または縮小できます。System Managerを使用して、NVMeネームスペースのサイズを拡張できます。

ネームスペースのサイズを拡張する

System Manager

1. Storage > NVMe Namespaces * をクリックします。
2. 拡張するネームスペースにカーソルを合わせ、をクリックし、 *[編集]*をクリックします。
3. 容量 * で、ネームスペースのサイズを変更します。

CLI

1. 次のコマンドを入力します。 `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

ネームスペースのサイズを縮小する

NVMeネームスペースのサイズを縮小するには、ONTAP CLIを使用する必要があります。

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. ネームスペースのサイズを縮小します。

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
   ```

ネームスペースを**LUN**に変換する

開始する前に

11.1以降では、**ONTAP CLI**を使用して、既存の**NVMe**ネームスペースをインプレースで**ONTAP 9**に変換できます。

- 指定したNVMeネームスペースにサブシステムへの既存のマッピングが含まれていないことを確認してください。
- ネームスペースをSnapshotの一部にしたり、SnapMirror関係のデスティネーション側で読み取り専用ネームスペースとして使用したりすることはできません。
- NVMeネームスペースは特定のプラットフォームとネットワークカードでのみサポートされるため、この機能は特定のハードウェアでのみ機能します。

手順

1. 次のコマンドを入力して、NVMeネームスペースをLUNに変換します。

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

   の詳細については `lun convert-from-namespace`、を"ONTAPコマンド リファレンス"参照してください。

NVMe経由のインバンド認証の設定

12.1以降でONTAP 9は、ONTAPコマンドラインインターフェイス（CLI）を使用して、DH-HMAC-CHAP認証を使用して、NVMe/TCPおよびNVMe/FCプロトコルを介し

たNVMeホストとコントローラ間のインバンド（セキュア）双方向および単方向認証を設定できます。ONTAP 9.14.1以降では、インバンド認証をSystem Managerで設定できます。

インバンド認証を設定するには、各ホストまたはコントローラにDH-HMAC-CHAPキーを関連付ける必要があります。DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。NVMeホストまたはコントローラがピアを認証するには、ピアに関連付けられたキーを認識している必要があります。

単方向認証では、コントローラではなくホストにシークレットキーが設定されます。双方向認証では、ホストとコントローラの両方にシークレットキーが設定されます。

SHA-256がデフォルトのハッシュ関数で、2048ビットがデフォルトのDHグループです。

System Manager

14.1以降では、サブシステムの作成または更新、NVMeネームスペースの作成またはクローニング、新しいONTAP 9ネームスペースを使用した整合グループの追加時に、System Managerを使用してインバンド認証を設定できます。

手順

1. System Managerで、**[ホスト]>[NVMe**サブシステム**]***をクリックし、[追加]*をクリックします。
2. NVMeサブシステム名を追加し、Storage VMとホストオペレーティングシステムを選択します。
3. ホストのNQNを入力します。
4. [Host NQN]の横にある*[Use in-band authentication]*を選択します。
5. ホストシークレットとコントローラシークレットを指定します。

   DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。

6. ホストごとに使用するハッシュ関数とDHグループを選択します。

   ハッシュ関数とDHグループを選択しない場合、SHA-256がデフォルトのハッシュ関数として割り当てられ、2048ビットがデフォルトのDHグループとして割り当てられます。

7. 必要に応じて、*[追加]*をクリックし、必要に応じて手順を繰り返してホストを追加します。
8. [保存（ Save ）] をクリックします。
9. インバンド認証が有効になっていることを確認するには、*[システムマネージャ]>[ホスト]>[NVMeサブシステム]>[グリッド]>[ピークビュー]*をクリックします。

   ホスト名の横にあるトランスペアレントキーアイコンは、単方向モードがイネーブルであることを示します。ホスト名の横にある不透明キーは、双方向モードが有効であることを示します。

CLI

手順

1. NVMeサブシステムにDH-HMAC-CHAP認証を追加します。

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   の詳細については `vserver nvme subsystem host add`、を"ONTAPコマンド リファレンス"参照してください。

2. DH-HMAC CHAP認証プロトコルがホストに追加されたことを確認します。

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

の詳細については `vserver nvme subsystem host show`、を"ONTAPコマンド リファレンス"参照してください。

3. NVMeコントローラの作成時にDH-HMAC CHAP認証が実行されたことを確認します。

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

関連情報

- "vserver nvme subsystem controller show"

NVMe経由のインバンド認証を無効にする

DH-HMAC-CHAPを使用してNVMe経由のインバンド認証を設定している場合は、いつでも無効にすることができます。

ONTAP 9.12.1以降からONTAP 9.12.0以前にリバートする場合は、リバート前にインバンド認証を無効にする必要があります。DH-HMAC-CHAPを使用するインバンド認証が無効になっていない場合、リバートは失敗します。

手順

1. ホストをサブシステムから削除してDH-HMAC-CHAP認証を無効にします。

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. DH-HMAC-CHAP認証プロトコルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

3. 認証を使用せずにホストをサブシステムに再度追加します。

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

NVMe/TCP用の**TLS**セキュアチャネルのセットアップ

ONTAP 9 .16.1以降では、NVMe/TCP接続用にTLSセキュアチャネルを設定できます。System ManagerまたはONTAP CLIを使用して、TLSが有効になっている新しいNVMeサブシステムを追加するか、既存のNVMeサブシステムに対してTLSを有効にすることができます。

System Manager

NVMe.16.1以降では、サブシステムの作成または更新、ネームスペースの作成またはクローニング、新しいONTAP 9ネームスペースを使用した整合性グループの追加時に、System Managerを使用してNVMe/TCP接続用のTLSを設定できます。

手順

1. System Managerで、**[ホスト]>[NVMeサブシステム]***をクリックし、[追加]*をクリックします。
2. NVMeサブシステム名を追加し、Storage VMとホストオペレーティングシステムを選択します。
3. ホストのNQNを入力します。
4. [Host NQN]の横にある*[Require Transport Layer Security（TLS）]*を選択します。
5. 事前共有キー（PSK）を指定します。
6. [保存（ Save ）] をクリックします。
7. TLSセキュアチャネルが有効になっていることを確認するには、*[システムマネージャ]>[ホスト]>[NVMeサブシステム]>[グリッド]>[ピークビュー]*を選択します。

CLI

手順

1. TLSセキュアチャネルをサポートするNVMeサブシステムホストを追加します。事前共有キー（PSK）は、 `tls-configured-psk`口論：

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. NVMeサブシステムホストがTLSセキュアチャネル用に設定されていることを確認します。オプションで引数を使用すると、そのキータイプを使用しているホストのみを表示でき `tls-key-type`ます。

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. NVMeサブシステムのホストコントローラがTLSセキュアチャネル用に設定されていることを確認します。必要に応じて、 `tls-identity`、、または `tls-cipher`引数を使用して、それらのTLS属性を持つコントローラのみを表示でき `tls-key-type`ます。

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

関連情報

- "SVM NVMeサブシステム"

NVMe/TCPのTLSセキュアチャネルを無効にする

ONTAP 9 .16.1以降では、NVMe/TCP接続用にTLSセキュアチャネルを設定できます。NVMe/TCP接続用にTLSセキュアチャネルを設定している場合は、いつでも無効にすることができます。

手順

1. サブシステムからホストを削除してTLSセキュアチャネルを無効にします。

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. TLSセキュアチャネルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

3. TLSセキュアチャネルがないサブシステムにホストを再度追加します。

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

関連情報

- "Vserver NVMeサブシステムホスト"

NVMeホスト優先度の変更

nvme .14.1以降では、ONTAP 9サブシステムを設定して、特定のホストに対するリソース割り当ての優先順位を設定できます。デフォルトでは、ホストがサブシステムに追加されると、通常の優先度が割り当てられます。高い優先度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。

ONTAPのコマンドラインインターフェイス（CLI）を使用して、デフォルト優先度を手動で標準から高に変更できます。ホストに割り当てられている優先度を変更するには、サブシステムからホストを削除してから再度追加する必要があります。

手順

1. ホストプライオリティがRegularに設定されていることを確認します。

```
vserver nvme show-host-priority
```

の詳細については `vserver nvme show-host-priority`、を"ONTAPコマンド リファレンス"参照してください。

2. サブシステムからホストを削除します。

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

の詳細については `vserver nvme subsystem host remove`、を"ONTAPコマンド リファレンス"参照してください。

3. ホストがサブシステムから削除されたことを確認します。

```
vserver nvme subsystem host show
```

の詳細については `vserver nvme subsystem host show`、を"ONTAPコマンド リファレンス"参照してください。

4. 優先度が高いサブシステムにホストを再度追加します。

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

の詳細については `vserver nvme subsystem host add`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPでの**NVMe/TCP**コントローラのホスト自動検出を管理します。

ONTAP 9.14.1以降では、IPベースのファブリックでNVMe/TCPプロトコルを使用するコントローラのホスト検出がデフォルトで自動化されます。

NVMe / TCPコントローラのホスト検出を自動化

以前に自動ホスト検出を無効にしていたが、ニーズが変わった場合は、再度有効にすることができます。

手順

1. advanced権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を有効にします。

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. NVMe/TCPコントローラの自動検出が有効になっていることを確認します。

```
vserver nvme show -fields mdns-service-discovery-enabled
```

NVMe / TCPコントローラのホストの自動検出を無効にする

NVMe / TCPコントローラをホストで自動的に検出する必要がなく、ネットワークで不要なマルチキャストトラフィックが検出された場合は、この機能を無効にする必要があります。

手順

1. advanced権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を無効にします。

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. NVMe/TCPコントローラの自動検出が無効になっていることを確認します。

```
vserver nvme show -fields mdns-service-discovery-enabled
```

ONTAPでNVMeホスト仮想マシン識別子を無効にする

ONTAP 9.14.1以降では、デフォルトで、ONTAPでNVMe/FCホストが一意の識別子で仮想マシンを識別し、NVMe/FCホストが仮想マシンのリソース利用率を監視する機能がサポートされます。これにより、ホスト側のレポート作成とトラブルシューティングが強化されます。

この機能は、bootargを使用して無効にできます。参照"NetAppナレッジベース: ONTAPで NVMe ホスト仮想マシン識別子を無効にする方法"。

FCアダプタを搭載したシステムを管理する

FCアダプタを搭載したシステムを管理する

オンボードFCアダプタとFCアダプタカードを管理するためのコマンドを使用できます。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージ システムには、イニシエータまたはターゲットとして設定できるオンボードFCアダプ

タが搭載されています。また、イニシエータまたはターゲットとして設定されたFCアダプタ カードを使用することもできます。イニシエーターはバックエンドのディスク シェルフに接続し、場合によっては外部ストレージ アレイにも接続します。ターゲットはFCスイッチのみに接続します。FCターゲットのHBAポートとスイッチ ポートの速度は、両方とも同じ値に設定し、autoには設定しないでください。

関連情報

"SAN構成"

FCアダプタの管理用コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、 FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、 FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。FCイニシエータアダプタのコマンドを使用する前に、コマンドを使用する必要があります `run -node node_name`。

FC ターゲットアダプタの管理用コマンド

状況	使用するコマンド
ノードの FC アダプタ情報を表示する	`network fcp adapter show`
FC ターゲットアダプタのパラメータを変更する	`network fcp adapter modify`
FC プロトコルトラフィック情報を表示します	`run -node node_name sysstat -f`
FC プロトコルの実行時間を表示します	`run -node node_name uptime`
アダプタの設定とステータスを表示します	`run -node node_name sysconfig -v adapter`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node node_name sysconfig -ac`
コマンドのマニュアルページを表示します	`man <command_name>`

FC イニシエータアダプタの管理用コマンド

状況	使用するコマンド
ノードのすべてのイニシエータおよびそのアダプタの情報を表示する	`run -node node_name storage show adapter`
アダプタの設定とステータスを表示します	`run -node node_name sysconfig -v adapter`

状況	使用するコマンド
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node node_name sysconfig -ac`

オンボード **FC** アダプタの管理用コマンド

状況	使用するコマンド
オンボード FC ポートのステータスを表示します	`run -node node_name system hardware unified-connect show`

関連情報

- "ネットワークFCPアダプタ"

FCアダプタの設定

オンボードのFCポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。特定のFCアダプタのポートは、オンボードのFCポートと同様に、ターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストについては、を参照"NetApp Hardware Universe"してください。

ターゲット モードは、ポートをFCイニシエータに接続するために使用します。イニシエータモードは、ポートをテープドライブ、テープライブラリ、またはForeign LUN Import（FLI）対応のサードパーティ製ストレージに接続するために使用されます。FC

FCアダプタを設定する手順は、FCプロトコルとFC-NVMeプロトコルで同じです。ただし、FC-NVMeをサポートするFCアダプタは一部のみです。FC-NVMeプロトコルをサポートするアダプタのリストについては、を参照してください"NetApp Hardware Universe"。

FCアダプタのターゲットモード設定

手順

1. アダプタをオフラインにします。

   `node run -node node_name storage disable adapter adapter_name`

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

   `system hardware unified-connect modify -t target -node node_name adapter adapter_name`

3. 変更したアダプタをホストしているノードをリブートします。
4. ターゲットポートの設定が正しいことを確認します。

```
network fcp adapter show -node node_name
```

の詳細については `network fcp adapter show`、を"ONTAPコマンド リファレンス"参照してください。

5. アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

FCアダプタのイニシエータモード設定

開始する前に

- アダプタのLIFを、メンバーになっているすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更対象の物理ポートを使用するすべてのStorage Virtual Machine（SVM）のすべてのLIFを移行または破棄する必要があります。

NVMe/FCではイニシエータモードがサポートされます。

手順

1. アダプタからすべてのLIFを削除します。

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

の詳細については `network interface delete`、を"ONTAPコマンド リファレンス"参照してください。

2. アダプタをオフラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

```
system hardware unified-connect modify -t initiator adapter_port
```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対してFCポートが正しい状態で設定されていることを確認します。

```
system hardware unified-connect show
```

6. アダプタをオンラインに戻します。

```
node run -node node_name storage enable adapter adapter_port
```

アダプタ設定の表示

特定のコマンドを使用して、FC / UTAアダプタに関する情報を表示できます。

FCターゲットアダプタ

ステップ

1. アダプタ情報を表示するには、コマンドを使用し `network fcp adapter show`ます。 `network fcp adapter show -instance -node node1 -adapter 0a`

   出力には、使用されている各スロットのシステム設定情報およびアダプタ情報が表示されます。

   の詳細については `network fcp adapter show`、を"ONTAPコマンド リファレンス"参照してください。

ユニファイドターゲットアダプタ（UTA）X1143A-R6

手順

1. ケーブルを接続していない状態でコントローラをブートします。
2. コマンドを実行し `system hardware unified-connect show`て、ポートの設定とモジュールを確認します。
3. CNAとポートを設定する前に、ポート情報を確認してください。

UTA2ポートのCNAモードからFCモードへの変更

FCイニシエータモードとFCターゲットモードをサポートするには、UTA2ポートをConverged Network Adapter（CNA；統合ネットワークアダプタ）モードからFibre Channel（FC；ファイバチャネル）モードに変更する必要があります。ポートをネットワークに接続する物理メディアを変更する必要がある場合は、パーソナリティを CNA モードから FC モードに変更します。

手順

1. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_name -status-admin down
   ```

2. ポートのモードを変更します。

   ```
   ucadmin modify -node node_name -adapter adapter_name -mode fcp
   ```

3. ノードをリブートし、アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_name -status-admin up
   ```

4. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。

   - ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ ifgrp ）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。

i. LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。

ii. コマンドを実行して、ポートを手動で削除し `network port delete`ます。

コマンドが失敗した場合は `network port delete`、エラーに対処してからもう一度コマンドを実行する必要があります。

の詳細については `network port delete`、を"ONTAPコマンド リファレンス"参照してください。

- ポートが LIF のホームポートとして使用されていない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。

VIFマネージャでポートが削除されない場合は、管理者がリブート後にコマンドを使用して手動で削除する必要があります `network port delete`。

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                                 Speed(Mbps)
Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0
```

```
    net-f8040-34::> network interface show -fields home-port, curr-
port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

5. 適切な SFP+ が取り付けられていることを確認します。

   `network fcp adapter show -instance -node -adapter`

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、ノードで構成を変更する前に、 8Gb SFP または 16Gb SFP を使用します。

   の詳細については `network fcp adapter show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "ネットワークインターフェイス"

CNA / UTA2ターゲットアダプタの光モジュールの変更

ユニファイドターゲットアダプタ（CNA / UTA2）用に選択したパーソナリティモードをサポートするように、ユニファイドターゲットアダプタ（CNA / UTA2）の光モジュールを変更する必要があります。

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
2. X1143A-R6アダプタから現在の光モジュールを取り外します。
3. 使用するパーソナリティモード（FCまたはCNA）光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   サポートされている SFP+ モジュールと Cisco ブランドの銅線（ Twinax ）ケーブルについては、 Hardware Universe を参照してください。

関連情報

- "NetApp Hardware Universe"
- "network fcp adapter show"

X1143A-R6アダプタでサポートされるポート構成

FCターゲットモードは、X1143A-R6アダプタポートのデフォルト設定です。ただし、このアダプタのポートは、10GbイーサネットポートおよびFCoEポート、または16Gb FCポートとして設定できます。

イーサネットおよびFCoE用に設定した場合、X1143A-R6アダプタは、同じ10-GBEポート上でNICおよびFCoEターゲットトラフィックを同時にサポートします。FC用に設定した場合、同じASICを共有する2ポートの各ペアをFCターゲットモードまたはFCイニシエータモード用に個別に設定できます。つまり、1つのX1143A-R6アダプタで、1つの2ポートペアでFCターゲットモードをサポートし、もう1つの2ポートペアでFCイニシエータモードをサポートできます。

関連情報

"NetApp Hardware Universe"

"SAN構成"

ポートの設定

ユニファイドターゲットアダプタ（ X1143A-R6 ）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

手順

1. コマンドを使用して、必要に応じてFibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定し `system node hardware unified-connect

modify`ます。

2. FC または 10Gb イーサネットに適したケーブルを接続します。
3. 適切な SFP+ が取り付けられていることを確認します。

   `network fcp adapter show -instance -node -adapter`

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、接続先の FC ファブリックに応じて 8Gb SFP または 16Gb SFP を使用します。

   の詳細については `network fcp adapter show`、を"ONTAPコマンド リファレンス"参照してください。

X1133A-R6アダプタ使用時の接続の切断を防止

別のX1133A-R6 HBAへの冗長パスをシステムに設定することで、ポート障害時に接続が失われないようにすることができます。

X1133A-R6 HBA は、 4 ポート 16Gb の FC アダプタで、 2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1 、ポート 3 とポート 4 は ASIC 2 ）。単一のASIC上の両方のポートは、ターゲットモードまたはイニシエータモードのいずれかで同じモードで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、 HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

すべての**SAN**プロトコルの**LIF**を管理します。

すべての**SAN**プロトコルの**LIF**を管理します。

SAN環境でクラスタのフェイルオーバー機能を利用するには、イニシエータでMultipath I/O（MPIO；マルチパスI/O）とAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）を使用する必要があります。ノードで障害が発生しても、LIFは障害が発生したパートナーノードのIPアドレスを引き継ぎません。代わりに、MPIOソフトウェアが、ホストのALUAを使用して、LIF経由でLUNにアクセスするための適切なパスを選択します。

HAペアの各ノードから1つ以上のiSCSIパスを作成し、HAペアで処理されるLUNに論理インターフェイス（LIF）を使用してアクセスできるようにする必要があります。SANをサポートするStorage Virtual Machine（SVM）ごとに管理LIFを1つ設定する必要があります。

直接接続またはイーサネットスイッチを使用した接続がサポートされています。両方のタイプの接続用にLIFを作成する必要があります。

- SANをサポートするStorage Virtual Machine（SVM）ごとに管理LIFを1つ設定する必要があります。ノードごとに2つのLIFを設定できます。LIFはFCで使用するファブリックごとに1つ、iSCSI用のイーサネットネットワークを分離します。

作成したLIFは、ポートセットから削除したり、Storage Virtual Machine（SVM）内の別のノードに移動したり、LIFを削除したりできます。

関連情報

- "LIFの設定の概要"
- "LIFの作成"

ONTAPでの**NVMe LIF**の設定

NVMe LIFを設定するときは、一定の要件を満たす必要があります。

開始する前に

LIFを作成するFCアダプタでNVMeがサポートされている必要があります。サポートされているアダプタをに示し "Hardware Universe"ます。

タスクの内容

ONTAP 9.12.1以降では、ノードごとに最大12ノードのNVMe LIFを2つ設定できます。ONTAP 9.11.1以前では、ノードあたり2つのNVMe LIFを、最大2つのノードで設定できます。

NVMe LIFを作成するときは、次のルールが適用されます。

- データLIFで使用できるデータプロトコルはNVMeだけです。
- SANをサポートするSVMごとに管理LIFを1つ設定する必要があります。
- ONTAP 9 .5以降の場合は、ネームスペースを含むノードとそのHAパートナーにNVMe LIFを設定する必要があります。
- ONTAP 9 .4の場合のみ：
  - NVMe LIFとネームスペースは同じノードでホストされている必要があります。
  - 設定できる NVMe データ LIF は SVM ごとに 1 つだけです。

手順

1. LIFを作成します。

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

NVMe/TCPはONTAP 9 10.1以降で使用できます。

2. LIFが作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

作成後、NVMe/TCP LIFはポート8009で検出をリスンします。

関連情報

- "ネットワークインターフェイス"

SAN LIFを移動する際の注意事項

クラスタへのノードの追加やクラスタからのノードの削除など、クラスタの内容を変更する場合にのみ、LIFを移動する必要があります。LIFを移動する場合は、FCファブリックを再ゾーニングしたり、クラスタに接続されたホストと新しいターゲットインターフェイスの間に新しいiSCSIセッションを作成したりする必要はありません。

コマンドを使用してSAN LIFを移動することはできません `network interface move`。SAN LIFを移動するには、対象のLIFをオフラインにし、別のホームノードまたはポートに移動してから、移動先の新しい場所でLIFをオンラインに戻します。ONTAP SANソリューションでは、Asymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）によってパスの冗長化と自動選択が実現します。そのため、移動時にLIFがオフラインになっても、I/Oの中断はありません。ホストは再試行してから別のLIFにI/Oを移動するだけです。

LIFの移動を使用すると、システムを停止することなく次の処理を実行できます。

- クラスタの1つのHAペアを、LUNデータにアクセスするホストに対して透過的な方法で、アップグレードされたHAペアに置き換える
- ターゲットインターフェイスカードのアップグレード
- Storage Virtual Machine（SVM）のリソースをクラスタ内のノードセットから別のノードセットに移行する

ポートセットから**SAN LIF**を削除する

削除または移動するLIFがポートセットに含まれている場合、LIFを削除または移動する前に、そのLIFをポートセットから削除する必要があります。

タスクの内容

次の手順1は、1つのLIFがポートセットにある場合にのみ実行する必要があります。ポートセットがイニシエータグループにバインドされている場合、ポートセット内の最後のLIFを削除することはできません。複数のLIFがポートセットにある場合は、手順2から始めることができます。

手順

1. ポートセットにLIFが1つしかない場合は、コマンドを使用し `lun igroup unbind`てイニシエータグループからポートセットのバインドを解除します。

   > イニシエータグループとポートセットのバインドを解除すると、イニシエータグループ内のすべてのイニシエータが、すべてのネットワークインターフェイス上のそのイニシエータグループにマッピングされているすべてのターゲットLUNにアクセスできるようになります。

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

   の詳細については `lun igroup unbind`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用し `lun portset remove`て、ポートセットからLIFを削除します。

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

の詳細については `lun portset remove`、を"ONTAPコマンド リファレンス"参照してください。

SAN LIFを移動する

ノードをオフラインにする必要がある場合、 SAN LIF を移動して WWPN などの設定情報を保持しておけば、スイッチファブリックの再ゾーニングを行わずに済みます。SAN LIF は移動前にオフラインにする必要があるため、ホストトラフィックについては、ホストマルチパスソフトウェアを使用して、 LUN への無停止アクセスを確保する必要があります。SAN LIF はクラスタ内の任意のノードに移動できますが、 SAN LIF を別の Storage Virtual Machine （ SVM ）に移動することはできません。

開始する前に

LIF がポートセットのメンバーである場合、 LIF を別のノードに移動する前に、その LIF をポートセットから削除しておく必要があります。

タスクの内容

移動する LIF のデスティネーションノードおよび物理ポートは、同じ FC ファブリック上またはイーサネットネットワーク上に存在する必要があります。適切にゾーニングされていない別のファブリック上に LIF を移動したり、 iSCSI イニシエータとターゲットを接続していないイーサネットネットワーク上に LIF を移動したりすると、その LIF をオンラインに戻しても接続できなくなります。

手順

1. LIFの管理ステータスと動作ステータスを表示します。

   ```
   network interface show -vserver vserver_name
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. LIFのステータスを（オフライン）に変更し `down`ます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin
   down
   ```

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

3. LIFを新しいノードとポートに割り当てます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   node_name -home-port port_name
   ```

4. LIFのステータスを（オンライン）に変更し `up`ます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin up
   ```

   の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。

5. 変更内容を確認します。

```
network interface show -vserver vserver_name
```

SAN環境で**LIF**を削除する

LIFを削除する前に、LIFに接続されているホストが別のパスを介してLUNにアクセスできることを確認する必要があります。

開始する前に

削除するLIFがポートセットのメンバーである場合、LIFを削除する前にポートセットからLIFを削除する必要があります。

System Manager

ONTAP System Manager（9.7以降）でLIFを削除する。

手順

1. System Managerで、* Network > Overview をクリックし、 Network Interfaces *を選択します。
2. LIFを削除するStorage VMを選択します。
3. をクリック ⋮ し、*[削除]*を選択します。

CLI

ONTAP CLIを使用してLIFを削除する。

手順

1. 削除するLIFの名前と現在のポートを確認します。

   ```
   network interface show -vserver vserver_name
   ```

2. LIFを削除します。

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

   の詳細については `network interface delete`、を"ONTAPコマンド リファレンス"参照してください。

3. LIFが削除されたことを確認します。

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                       Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

クラスタにノードを追加する際の**SAN LIF**の要件

クラスタにノードを追加する場合は、一定の考慮事項について理解しておく必要があります。

- 新しいノードにLUNを作成する前に、必要に応じて新しいノードにLIFを作成する必要があります。
- これらのLIFは、ホストスタックとプロトコルの指示に従って、ホストから検出する必要があります。
- クラスタインターコネクトネットワークを使用せずにLUNやボリュームを移動できるように、新しいノードにLIFを作成する必要があります。

ホストによる**iSCSI SendTargets**検出処理に対して**FQDN**を返すように**iSCSI LIF**を設定

ONTAP 9以降では、ホストOSから送信されたiSCSI SendTargets検出処理で完全修飾ドメイン名（FQDN）を返すようにiSCSI LIFを設定できます。FQDNを返すと、ホストOSとストレージサービスの間にネットワークアドレス変換（NAT）デバイスがある場合に便利です。

タスクの内容

IPアドレスはNATデバイスの片側では意味がありませんが、FQDNであれば両側で意味があります。

FQDN値の互換性の上限は、すべてのホストOSで128文字です。

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. FQDNを返すようにiSCSI LIFを設定します。

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   次の例では、FQDNとしてstoragehost-005.example.comを返すようにiSCSI LIFを設定しています。

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. SendTargetsがFQDNになっていることを確認します。

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   この例では、sendtargets-fqdn出力フィールドにstoragehost-005.example.comが表示されています。

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif        sendtargets-fqdn
------- ---------- --------------------------
vs1     vs1_iscsi1 storagehost-005.example.com
vs1     vs1_iscsi2 storagehost-006.example.com
```

関連情報

"ONTAPコマンド リファレンス"

SANプロトコルのONTAPスペース割り当てを有効にする

ONTAPのスペース割り当ては、LUNまたはNVMeネームスペースがスペース不足になった場合にオフラインになるのを防ぎ、SANホストでスペースを再生できるようにします。

ONTAPでスペースが割り当てられるかどうかは、使用しているSANプロトコルとONTAPのバージョンによって異なります。ONTAP 9.16.1以降では、iSCSI、FC、NVMeの各プロトコルについて、新規に作成したLUNおよびすべてのネームスペースに対してスペース割り当てがデフォルトで有効になります。

ONTAPのバージョン	プロトコル	スペース割り当て
9.16.1以降	• iSCSI • FC • NVMe	新規作成されたLUNおよびすべてのネームスペースに対してデフォルトで有効
9.15.1	• iSCSI • FC	新規作成されたLUNに対してデフォルトで有効
	NVMe	サポート対象外
9.14.1以前	• iSCSI • FC	新規作成されたLUNではデフォルトで無効
	NVMe	サポート対象外

スペース割り当てが有効な場合：

- LUNまたはネームスペースのスペースが不足すると、ONTAPはホストに書き込み処理に使用できる空きスペースがないことを通知します。そのため、LUNまたはネームスペースはオンラインのままで、読み取り処理は継続されます。ホストの設定に応じて、成功するか、ホストのファイルシステムがオフラインになるまで、ホストは書き込み処理を再試行します。LUNまたはネームスペースで使用可能な空きスペースが増えると、書き込み処理が再開されます。

  スペース割り当てが有効になっていない場合、LUNまたはネームスペースのスペースが不足すると、すべてのI/O処理が失敗し、LUNまたはネームスペースがオフラインになります。通常の処理を再開するには、スペースの問題を解決する必要があります。パスとデバイスを動作状態にリストアするには、ホスト

でLUNデバイスの再スキャンが必要になる場合もあります。

- ホストはSCSIまたはNVMe（とも呼ばれる `TRIM`）処理を実行できます `UNMAP`。マッピング解除処理を使用すると、有効なデータがなくなったために不要になったデータブロックをホストが特定できます。識別は通常、ファイルの削除後に行われます。その後、ストレージシステムはこれらのデータブロックの割り当てを解除して、スペースを他の場所で消費できるようにします。このように割り当てを解除することで、特にデータの書き替え率が高いファイルシステムでは、全体的なストレージ効率が大幅に向上します。

開始する前に

スペース割り当てを有効にするには、書き込みを完了できない場合にスペース割り当てエラーを正しく処理できるホスト構成が必要です。SCSIまたはNVMeを活用 `UNMAP`するには、SCSI SBC-3標準で定義されている論理ブロックプロビジョニングを使用できる構成が必要です。

現在、スペース割り当てを有効にした場合にシンプロビジョニングをサポートしているホストは次のとおりです。

- Citrix XenServer 6.5以降
- VMware ESXi 5.0以降
- Oracle Linux 6.2 UEKカーネル以降
- Red Hat Enterprise Linux 6.2以降
- SUSE Linux Enterprise Server 11以降
- Solaris 11.1以降
- ウィンドウ

タスクの内容

クラスタをONTAP 9 .15.1以降にアップグレードした場合、ソフトウェアのアップグレード前に作成されたすべてのLUNのスペース割り当て設定は、ホストタイプに関係なく、アップグレード後も変更されません。たとえば、スペース割り当てが無効になっているVMwareホスト用にONTAP 9 .13.1でLUNが作成された場合、ONTAP 9 .15.1にアップグレードしても、そのLUNでのスペース割り当ては無効なままになります。

手順

1. スペース割り当てを有効にします。

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. スペース割り当てが有効になっていることを確認します。

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. ホストOSでスペース割り当てが有効になっていることを確認します。

VMware ESXiの一部のバージョンなど、一部のホスト構成では、設定の変更が自動的に認識されるため、ユーザの操作は必要ありません。その他の設定では、デバイスの再スキャンが必要になる場合があります。一部のファイルシステムやボリュームマネージャでは、を使用したスペース再生を有効にするために、追加の設定が必要になる場合があります `SCSI UNMAP`。ファイルシステムの再マウントまたはOSの完全なリブートが必要になる場合があります。詳細については、ご使用のホストのドキュメントを参照してください。

VMware ESXi 8.x以降の**NVMe**ホスト用のホストの設定

NVMeプロトコルを使用してESXi 8.x以降を実行しているVMwareホストでは、ONTAPでスペース割り当てを有効にしたあとに、ホストで次の手順を実行する必要があります。

手順

1. ESXiホストで、DSMが無効になっていることを確認します。

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   想定される値は0です。

2. NVMe DSMを有効にします。

   ```
   esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
   ```

3. DSMが有効になっていることを確認します。

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   想定される値は1です。

関連リンク

詳細については、をご覧ください "ESXi 8.x（ONTAP）向けのNVMe-oFホストの設定"。

推奨されるボリュームとファイルまたは**LUN**の設定の組み合わせ

推奨されるボリュームとファイルまたは**LUN**の設定の組み合わせの概要

使用可能な FlexVol の設定とファイルまたは LUN の設定の組み合わせは、使用するアプリケーションと管理要件によって異なります。これらの組み合わせのメリットとデメリットを理解しておくと、環境に適したボリュームと LUN の設定の組み合わせを決定する際に役立ちます。

推奨されるボリュームと LUN の設定の組み合わせは次のとおりです。

- スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング
- スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリュームプロビジョニング
- スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

これらのいずれかの設定の組み合わせとともに、 LUN で SCSI シンプロビジョニングを使用できます。

スペースリザーブファイルまたはスペースリザーブ **LUN** とシックボリュームプロビジョニング

- 利点 :*
- スペースリザーブファイルでのすべての書き込み処理が保証されます。スペース不足のために失敗することはありません。
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- コストと制限： *
- シックプロビジョニングボリュームをサポートするための十分なスペースをアグリゲートから事前に確保しておく必要があります。
- LUN 作成時に、 LUN の 2 倍のサイズのスペースがボリュームから割り当てられます。

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンボリュームプロビジョニング

- 利点 :*
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- スペースは使用時に初めて割り当てられます。
- 費用および制限 :*
- 書き込み処理は保証されず、ボリュームの空きスペースが不足すると失敗する場合があります。
- アグリゲートの空きスペースを効果的に管理して、空きスペースが不足しないようにする必要があります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニング

- 利点 :*

事前に確保されるスペースがシックボリュームプロビジョニングの場合よりも少なく、ベストエフォートの書き込み保証も提供されます。

- 費用および制限 :*
- このオプションを指定すると、書き込み処理が失敗することがあります。

  このリスクは、ボリュームの空きスペースとデータの揮発性の適切なバランスを維持することで軽減できます。

- Snapshot、FlexCloneファイル、LUNなどのデータ保護オブジェクトは保持されません。
- 重複排除、圧縮、 ODX / コピーオフロードなど、自動で削除できない ONTAP のブロック共有ストレージ効率化機能は使用できません。

環境に適したボリュームと**LUN**の設定の組み合わせの決定

環境に関するいくつかの基本的な質問に答えることで、環境に最適なFlexVol volumeとLUNの設定を決定できます。

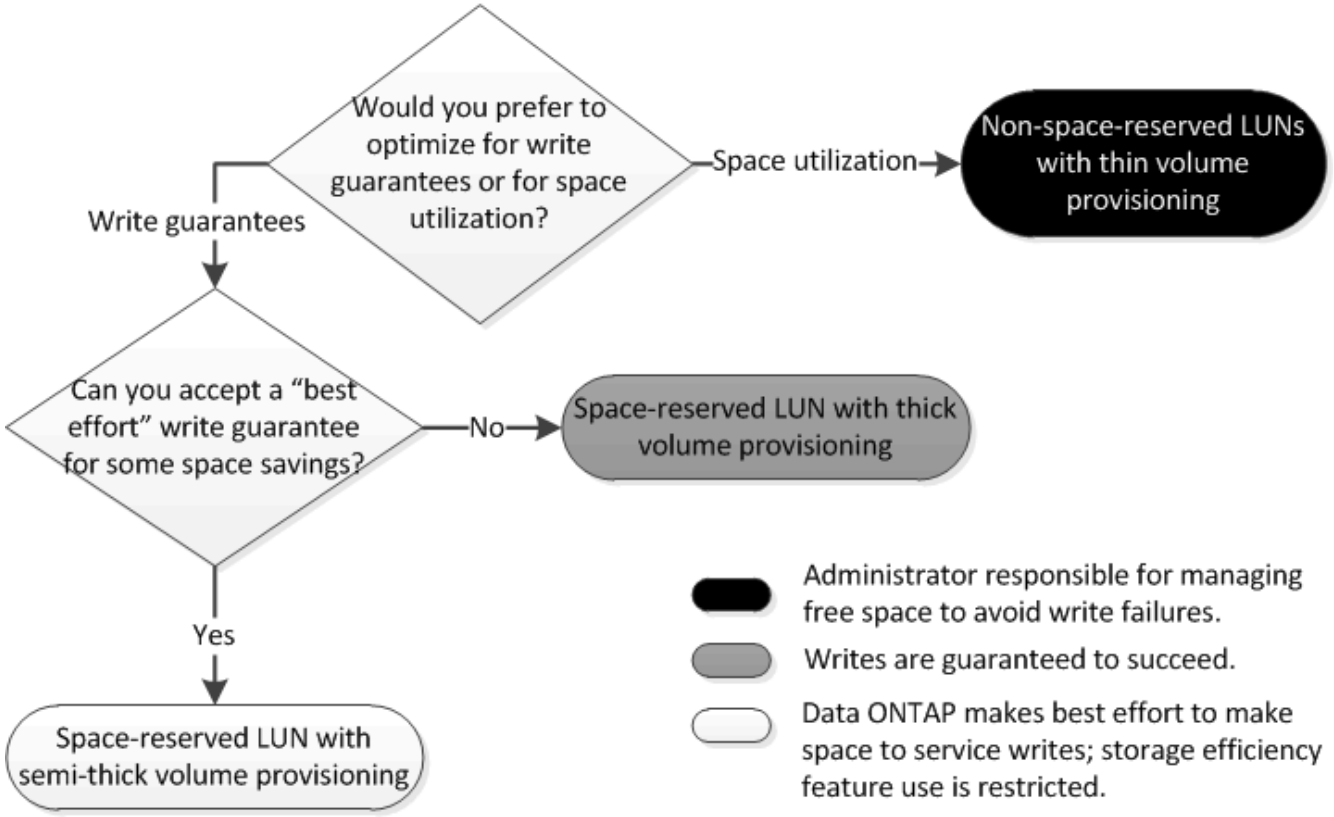
タスクの内容

LUNおよびボリュームの設定を最適化して、ストレージ利用率を最大限に高めたり、書き込みを保証したりすることができます。ストレージ利用要件、および空きスペースを監視して迅速に補充できるかどうかに基づいて、ご使用の環境に適したFlexVol volumeボリュームとLUNボリュームを決定する必要があります。

LUNごとに個別のボリュームを作成する必要はありません。

ステップ

1. 次のデシジョンツリーを使用して、環境に最適なボリュームとLUNの設定の組み合わせを決定してください。



LUNのデータ増加率の計算

スペースリザーブ LUN とスペースリザーブなしの LUN のどちらが適切かを判断するには、時間の経過に伴う LUN データの増加率を把握する必要があります。

タスクの内容

データの増加率が一貫して高い場合は、スペースリザーブLUNの方が適しています。データの増加率が低い場合は、スペースリザーブなしのLUNを検討してください。

OnCommand Insightなどのツールを使用してデータの増加率を計算することも、手動で計算することもできます。手動で計算する手順は次のとおりです。

手順

1. スペースリザーブLUNをセットアップします。
2. 一定期間（1週間など）、LUN上のデータを監視します。

定期的に発生するデータ増加の代表的なサンプルを形成するのに十分な監視期間があることを確認してください。たとえば、各月末に一貫して大量のデータが増加しているとします。

3. 毎日、増大するデータの量をGB単位で記録します。
4. 監視期間の終了時に、各日の合計を合計し、監視期間の日数で除算します。

   この計算により、平均成長率が算出されます。

例

この例では、200GBのLUNが必要です。LUNを1週間監視し、次の日次データの変更を記録します。

- 日曜日： 20GB
- 月曜日： 18GB
- 火曜日： 17GB
- 水曜日： 20GB
- 木曜日： 20GB
- 金曜日： 23GB
- 土曜日： 22GB

この例では、増加率は（ 20+18+17+20+20+23+22 ） / 7 で求めることができ、 1 日あたり 20GB となります。

スペースリザーブファイルまたはスペースリザーブ**LUN**とシックプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、 Storage Efficiency テクノロジを使用できます。また、事前に十分なスペースが割り当てられるため、空きスペースを能動的に監視する必要がありません。

シックプロビジョニングを使用するボリュームでスペースリザーブファイルまたはスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	値
保証	ボリューム
フラクショナルリザーブ	100
Snapshotリザーブ	任意
Snapshotの自動削除	オプション
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは **LUN** の設定	値
スペースリザベーション	有効

スペースリザーブなしのファイルまたはスペースリザーブなしの**LUN**とシンプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、事前に割り当てられるストレージの量が最小になりますが、スペース不足によるエラーを回避するために空きスペースを能動的に管理する必要があります。

シンプロビジョニングボリュームでスペースリザーブなしのファイルまたはスペースリザーブなしの LUN を設定するには、次の設定が必要です。

音量設定	値
保証	なし
フラクショナルリザーブ	0
Snapshotリザーブ	任意
Snapshotの自動削除	オプション
自動拡張	オプション

ファイルまたは **LUN** の設定	値
スペースリザベーション	無効にする

その他の考慮事項

ボリュームまたはアグリゲートのスペースが不足すると、ファイルまたは LUN への書き込み処理が失敗する場合があります。

ボリュームとアグリゲートの両方の空きスペースを能動的に監視しない場合は、ボリュームの自動拡張を有効にして、ボリュームの最大サイズをアグリゲートのサイズに設定してください。この設定では、アグリゲートの空きスペースを能動的に監視する必要がありますが、ボリュームの空きスペースを監視する必要はありません。

スペースリザーブファイルまたはスペースリザーブ**LUN**とセミシックボリュームプロビジョニングを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、フルプロビジョニングとの組み合わせに比べて事前に割り当てるストレージが少なくて済みますが、ボリュームに使用できる効率化テクノロジが制限されます。この設定の組み合わせでは、上書きがベストエフォートベースで行われます。

セミシックプロビジョニングを使用するボリュームでスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	値
保証	ボリューム
フラクショナルリザーブ	0
Snapshotリザーブ	0
Snapshotの自動削除	オン。この場合、コミットメントレベルを destroy に設定し、削除リストにすべてのオブジェクトを追加し、トリガーを volume に設定し、すべての FlexClone LUN と FlexClone ファイルの自動削除を有効にします。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは **LUN** の設定	値
スペースリザベーション	有効

テクノロジの制限事項

この設定の組み合わせでは、次のボリュームの Storage Efficiency テクノロジを使用できません。

- 圧縮
- 重複排除
- ODX コピーオフロードと FlexClone コピーオフロード
- 自動削除の対象としてマークされていない FlexClone LUN と FlexClone ファイル（アクティブクローン）
- FlexClone サブファイル
- ODX / コピーオフロード

その他の考慮事項

この設定の組み合わせを使用する場合は、次の点を考慮する必要があります。

- そのLUNをサポートするボリュームのスペースが不足すると、保護データ（FlexClone LUN、ファイル、Snapshot）が破棄されます。
- ボリュームの空きスペースが不足すると、書き込み処理がタイムアウトして失敗することがあります。

AFF プラットフォームではデフォルトで圧縮が有効になります。AFF プラットフォームのセミシックプロビジョニングを使用するボリュームに対しては、明示的に圧縮を無効にする必要があります。

SANのデータ保護

SAN環境向けのONTAPデータ保護方法

データを保護するには、データのコピーを作成して、偶発的な削除、アプリケーションのクラッシュ、データの破損、災害が発生した場合にデータをリストアできるようにします。ONTAPは、データ保護とバックアップのニーズに応じて、データを保護するためのさまざまな方法を提供します。

SnapMirrorアクティブ同期

ONTAP 9 .9.1の一般提供開始以降では、目標復旧時間ゼロ（ゼロRTO）または透過的アプリケーションフェイルオーバー（TAF）が提供され、SAN環境でビジネスクリティカルなアプリケーションを自動的にフェイルオーバーできます。SnapMirrorアクティブな同期を実行するには、2つのAFFクラスタまたは2つのオールフラッシュSANアレイ（ASA）クラスタを使用する構成にONTAPメディエーター1.2がインストールされている必要があります。

"SnapMirrorアクティブ同期"

Snapshot

LUNの複数のバックアップを手動または自動で作成、スケジュール、および保守できます。Snapshotは、最小限の追加ボリュームスペースのみを使用し、パフォーマンスコストは発生しません。LUNデータを誤って変更または削除してしまった場合でも、最新のSnapshotからデータを簡単かつ迅速にリストアできます。

FlexClone LUN（**FlexClone**のライセンスが必要）

アクティブボリュームまたはSnapshot内にある別のLUNの書き込み可能なポイントインタイムコピーを提供します。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

SnapRestore（ライセンスが必要）

ボリューム全体のSnapshotから、スペース効率に優れた高速データリカバリを必要に応じて実行できます。SnapRestoreを使用すると、ストレージシステムをリブートしなくても、LUNを以前保存した状態にリストアできます。

データ保護ミラー コピー（**SnapMirror**のライセンスが必要）

非同期のディザスタリカバリを提供します。これにより、ボリューム上のデータのSnapshotを定期的に作成し、それらのSnapshotをローカルまたはワイドエリアネットワーク経由でパートナーボリューム（通常は別のクラスタ上）にコピーして保持できます。ソースボリューム上のデータが破損した場合や失われた場合には、パートナーボリューム上のミラーコピーを使用して、最後のSnapshotの時点のデータをすぐに使用およびリストアできます。

SnapVaultバックアップ（**SnapMirror**のライセンスが必要）

ストレージ効率に優れた、長期間保持できるバックアップを提供します。SnapVault関係を使用すると、ボリュームの選択したSnapshotをデスティネーションボリュームにバックアップし、保持することができます。

テープ バックアップおよびアーカイブ処理を行っている場合は、SnapVaultセカンダリ ボリュームにすでにバックアップされているデータに対してそれらの処理を実行できます。

SnapDrive for Windowsまたは**SnapDrive for UNIX**（**SnapDrive**のライセンスが必要）

LUNへのアクセスを構成し、LUNを管理し、WindowsホストまたはUNIXホストからストレージシステムのスナップショットを直接管理します。

ネイティブ テープ バックアップ / リカバリ

ONTAPはほとんどの既存のテープ ドライブに対応しており、テープ ベンダーが新しいデバイスのサポートを動的に追加するための方策も用意されています。ONTAPはRemote Magnetic Tape（RMT）プロトコルもサポートしているため、RMT対応システムへのバックアップやリカバリも可能です。

関連情報

"NetAppのマニュアル：「SnapDrive for UNIX」" "NetAppのマニュアル：「SnapDrive for Windows（現在のリリース）」" "テープバックアップを使用したデータ保護"

ONTAPスナップショットから単一のLUNをリストアする

ボリューム全体をリストアすることなく、Snapshotから単一のLUNをリストアすることができます。LUN は、元の場所またはボリューム内の新しいパスにリストアできます。この処理では、ボリューム内の他のファイルまたは LUN に影響を与えることなく、単一の LUN だけがリストアされます。ファイルは、ストリームを使用してリストアすることもできます。

開始する前に

- リストア処理を完了するには、ボリュームに十分なスペースが必要です。
  - フラクショナルリザーブが0%のスペースリザーブLUNをリストアする場合は、リストアするLUNの1倍のサイズが必要です。
  - フラクショナルリザーブが100%のスペースリザーブLUNをリストアする場合は、リストアするLUNの2倍のサイズが必要です。
  - スペースリザーブなしのLUNをリストアする場合は、リストアするLUNで実際に使用されているスペースのみが必要です。
- デスティネーションLUNのSnapshotを作成しておく必要があります。

  リストア処理が失敗すると、デスティネーション LUN が切り捨てられる可能性があります。このような場合は、Snapshotを使用してデータの損失を防ぐことができます。

- ソースLUNのスナップショットを作成しておく必要があります。

  まれに、 LUN のリストアに失敗したときに、ソース LUN が使用不能になることがあります。この場合は、Snapshotを使用して、リストアを試みる直前の状態にLUNを戻すことができます。

- デスティネーション LUN とソース LUN の OS タイプが同じである必要があります。

  デスティネーション LUN の OS タイプがソース LUN の OS タイプと異なる場合は、リストア処理後、ホストからデスティネーション LUN へのデータアクセスが失われる可能性があります。

手順

1. ホストから、 LUN へのホストアクセスをすべて停止します。

2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUNのマッピングを解除します。

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. LUNのリストア先となるSnapshotを決定します。

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. LUNをリストアする前に、LUNのSnapshotを作成します。

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. ボリューム内の指定した LUN をリストアします。

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. 画面の手順に従います。
8. 必要に応じて、LUNをオンラインにします。

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. 必要に応じて、LUNを再マッピングします。

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. ホストから、 LUN を再マウントします。
11. ホストから、 LUN へのアクセスを再開します。

ONTAP Snapshotからのボリューム内のすべてのLUNのリストア

コマンドを使用すると、指定したボリューム内のすべてのLUNをSnapshotからリストアできます `volume snapshot restore`。

手順

1. ホストから、LUNへのホストアクセスをすべて停止します。

   ボリューム内のLUNへのホストアクセスをすべて停止せずにSnapRestoreを使用すると、データの破損やシステムエラーが発生する可能性があります。

2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUNのマッピングを解除します。

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. ボリュームのリストア先となるSnapshotを決定します。

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. 権限の設定をadvancedに変更します。

```
set -privilege advanced
```

6. データをリストアします。

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

7. 画面の指示に従います。
8. LUNを再マッピングします。

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. LUNがオンラインであることを確認します。

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. LUNがオンラインになっていない場合は、オンラインにします。

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. 権限の設定をadminに変更します。

```
set -privilege admin
```

12. ホストから、 LUN を再マウントします。
13. ホストから、 LUN へのアクセスを再開します。

ONTAP FlexClone LUNでデータを保護

FlexClone LUNは、アクティブボリュームまたはSnapshot内にある別のLUNの書き込み可能なポイントインタイムコピーです。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

FlexClone LUNを使用すると、LUNの読み取り/書き込みコピーを複数作成できます。

FlexClone LUNを作成する理由

- テスト用にLUNの一時的なコピーを作成する必要があります。
- 本番環境のデータへのアクセスを許可せずに、追加のユーザが利用できるデータのコピーを作成する必要があります。
- 操作や投影のためにデータベースのクローンを作成し、元のデータを変更せずに保持したいと考えています。
- LUNのデータの特定のサブセット（ボリュームグループ内の特定の論理ボリュームまたはファイルシステム、またはファイルシステム内の特定のファイルまたはファイルセット）にアクセスし、元のLUNの残りのデータをリストアすることなく、そのサブセットを元のLUNにコピーする。これは、LUNとLUNのクローンを同時にマウントできるオペレーティングシステムで機能します。SnapDrive for UNIXでは、コマンドを使用してこれをサポートしてい `snap connect`ます。
- オペレーティングシステムが同じ複数のSANブートホストが必要な場合。

FlexClone LUNは、最初は親LUNとスペースを共有します。デフォルトでは、FlexClone LUNは親LUNのスペースリザーブ属性を継承します。たとえば、親LUNがスペースリザーブなしの場合、FlexClone LUNもデフォルトでスペースリザーブなしになります。ただし、スペースリザーブLUNである親からスペースリザーブなしのFlexClone LUNを作成することはできます。

LUNクローンを作成するとバックグラウンドでブロック共有が行われ、ブロック共有が完了するまでボリュームSnapshotを作成できません。

コマンドを使用して、ボリュームでFlexClone LUNの自動削除機能を有効にする必要があります `volume snapshot autodelete modify`。そうしないと、FlexClone LUNを自動的に削除するように設定されていても、ボリュームでFlexCloneの自動削除が設定されていない場合、FlexClone LUNは削除されません。

FlexClone LUNを作成すると、FlexClone LUNの自動削除機能はデフォルトで無効になります。FlexClone LUNを自動的に削除するには、FlexClone LUNごとに手動で有効にする必要があります。ボリュームのセミシックプロビジョニングを使用している場合に、このオプションが提供する「ベストエフォート」の書き込み保証が必要な場合は、 _ALL_FlexClone LUN を自動削除できるようにする必要があります。

SnapshotからFlexClone LUNを作成すると、スペース効率に優れたバックグラウンドプロセスを使用して、Snapshotから自動的にLUNがスプリットされます。これにより、LUNがSnapshotに依存したり、追加のスペースを消費したりすることがなくなります。このバックグラウンドスプリットが完了しておらず、Snapshotが自動的に削除された場合、そのFlexClone LUNのFlexClone自動削除機能が無効になっていても、そのFlexClone LUNは削除されます。バックグラウンドスプリットの完了後は、Snapshotが削除されても、FlexClone LUNは削除されません。

関連情報

- "FlexClone LUNを作成する"
- "FlexClone LUNを自動的に削除するようにFlexVol volumeを設定する"
- "FlexClone LUNが自動的に削除されないようにする"

SAN環境でのSnapVaultバックアップの設定と使用

SAN環境でのONTAP SnapVaultバックアップの詳細

SAN環境でのSnapVaultの設定および使用方法は、NAS環境での設定および使用方法と非常によく似ていますが、SAN環境でLUNをリストアするには、いくつか特別な手順が必要になります。

SnapVaultバックアップには、ソースボリュームの読み取り専用コピーのセットが含まれています。SAN環境では、必ず個 々 のLUNではなく、ボリューム全体をSnapVaultセカンダリボリュームにバックアップします。

LUNを含むプライマリボリュームとSnapVaultバックアップとして機能するセカンダリボリューム間のSnapVault関係を作成および初期化する手順は、ファイルプロトコルに使用するFlexVolボリュームで使用する手順と同じです。この手順の詳細については、を"データ保護"参照してください。

Snapshotを作成してSnapVaultセカンダリボリュームにコピーする前に、バックアップ対象のLUNが整合性のある状態であることを確認することが重要です。SnapCenterを使用してSnapshotの作成を自動化すると、バックアップされたLUNが完全に作成され、元のアプリケーションで使用できるようになります。

SnapVaultセカンダリボリュームからLUNをリストアする場合、次の3つの基本的な選択肢があります。

- SnapVaultセカンダリボリュームからLUNを直接マッピングし、ホストをLUNに接続してLUNの内容にアクセスできます。

  LUNは読み取り専用で、SnapVaultバックアップ内の最新のSnapshotからのみマッピングできます。永続的予約およびその他のLUNメタデータは失われます。必要に応じて、元のLUNに引き続きアクセスできる場合は、ホスト上でコピープログラムを使用してLUNの内容をコピーし、元のLUNに戻すことができます。

  LUNのシリアル番号はソースLUNとは異なります。

- SnapVaultセカンダリボリューム内のSnapshotを新しい読み書き可能ボリュームにクローニングできます。

  その後、ボリューム内の任意のLUNをマッピングし、ホストをLUNに接続してLUNの内容にアクセスできます。必要に応じて、元のLUNに引き続きアクセスできる場合は、ホスト上でコピープログラムを使用してLUNの内容をコピーし、元のLUNに戻すことができます。

- SnapVaultセカンダリボリューム内の任意のSnapshotから、LUNを含むボリューム全体をリストアできます。

  ボリューム全体をリストアすると、ボリューム内のすべてのLUNとすべてのファイルが置き換えられます。Snapshotの作成後に作成された新しいLUNはすべて失われます。

  LUNでは、マッピング、シリアル番号、UUID、および永続的予約が保持されます。

ONTAP SnapVaultバックアップから読み取り専用LUNコピーにアクセスする

LUNの読み取り専用コピーには、SnapVaultバックアップ内の最新のSnapshotからアクセスできます。LUN の ID 、パス、およびシリアル番号はソース LUN のものとは異なり、あらかじめマッピングしておく必要があります。永続的予約、 LUN マッピング、および igroup は、 SnapVault セカンダリボリュームにレプリケートされません。

開始する前に

- SnapVault関係を初期化し、SnapVaultセカンダリボリュームの最新のSnapshotに目的のLUNが含まれている必要があります。
- SnapVaultバックアップがあるStorage Virtual Machine（SVM）に、適切なSANプロトコル対応のLIFが1つ以上あり、LUNコピーへのアクセスに使用するホストからアクセスできる必要があります。
- SnapVaultセカンダリボリュームからLUNコピーに直接アクセスする場合は、事前にSnapVault SVMにigroupを作成しておく必要があります。

  LUN には SnapVault セカンダリボリュームから直接アクセスできます。 LUN を含むボリュームのリストアやクローニングを行う必要はありません。

タスクの内容

以前のSnapshotからLUNがマッピングされているときに、新しいSnapshotがSnapVaultセカンダリボリュームに追加されると、マッピングされたLUNの内容が変更されます。LUNは引き続き同じ識別子でマッピングされますが、データは新しいSnapshotから取得されます。LUN のサイズが変更された場合、一部のホストはサイズの変更を自動的に検出します。 Windows ホストでは、サイズ変更を検知するためにディスクの再スキャンが必要です。

手順

1. SnapVaultセカンダリボリューム内の使用可能なLUNを表示します。

   ```
   lun show
   ```

   この例では、プライマリボリューム srcvolA 内の元の LUN と、 SnapVault セカンダリボリューム dstvolB 内のコピーされた LUN の両方が表示されています。

```
cluster::> lun show

Vserver   Path                  State   Mapped   Type          Size
--------  ------------------    ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

の詳細については `lun show`、を"ONTAPコマンド リファレンス"参照してください。

2. 目的のホストのigroupが、SnapVaultセカンダリボリュームがあるSVM内にまだ存在していない場合は、igroupを作成します。

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

このコマンドでは、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成します。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. 目的のLUNコピーをigroupにマッピングします。

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

の詳細については `lun mapping create`、を"ONTAPコマンド リファレンス"参照してください。

4. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

ONTAP SnapVaultバックアップから単一の**LUN**をリストア

単一の LUN を新しい場所または元の場所にリストアできます。SnapVaultセカンダリボリューム内の任意のSnapshotからリストアできます。LUN を元の場所にリストアするには、まず新しい場所にリストアしてから、元の場所にコピーします。

開始する前に

- SnapVault関係が初期化されていて、SnapVaultセカンダリボリュームにリストアする適切なSnapshotが含まれている必要があります。
- SnapVault セカンダリボリュームがある Storage Virtual Machine （ SVM ）に、適切な SAN プロトコル対応の LIF が 1 個以上あり、 LUN コピーへのアクセスに使用するホストからこの LIF にアクセスできることが必要です。
- igroup が SnapVault SVM 上にすでに存在している必要があります。

タスクの内容

このプロセスでは、SnapVaultセカンダリボリューム内のSnapshotから読み書き可能なボリュームクローンを作成します。このクローン内の LUN を直接使用することも、必要に応じて LUN の内容を元の LUN の場所にコピーすることもできます。

クローン内の LUN のパスとシリアル番号は、元の LUN のものとは異なります。永続的予約は維持されません。

手順

1. SnapVaultバックアップが含まれているセカンダリボリュームを確認します。

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                         Snapmirrored
                                 Idle       -         true    -
```

2. LUNのリストア元となるSnapshotを特定します。

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. 目的のSnapshotから読み書き可能クローンを作成

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

ボリュームクローンは、 SnapVault バックアップと同じアグリゲート内に作成されます。アグリゲート内に、クローンを格納できるだけの十分なスペースが必要です。

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. ボリュームクローン内のLUNを一覧表示します。

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

の詳細については `lun show`、を"ONTAPコマンド リファレンス"参照してください。

5. 目的のホストのigroupが、SnapVaultバックアップがあるSVM内にまだ存在していない場合は、igroupを作

成します。

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

この例では、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成しています。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. 目的のLUNコピーをigroupにマッピングします。

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

の詳細については `lun mapping create`、を"ONTAPコマンド リファレンス"参照してください。

7. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

   この LUN は読み書き可能であり、元の LUN の代わりに使用できます。LUN のシリアル番号が異なるため、ホストはこの LUN が元の LUN とは別の LUN であると解釈します。

8. ホスト上でコピープログラムを使用して、 LUN の内容を元の LUN にコピーします。

関連情報

- "snapmirror show"

ボリューム内のすべての**LUN**を**ONTAP SnapVault**バックアップからリストア

ボリューム内の1つ以上のLUNをSnapVaultバックアップからリストアする必要がある場合は、ボリューム全体をリストアできます。ボリュームをリストアする場合は、ボリューム内のすべての LUN が対象になります。

開始する前に

SnapVault関係が初期化されていて、SnapVaultセカンダリボリュームにリストアする適切なSnapshotが含まれている必要があります。

タスクの内容

ボリューム全体をリストアすると、ボリュームの状態はSnapshotが作成された時点の状態に戻ります。Snapshotの作成後にボリュームにLUNが追加された場合、そのLUNはリストアプロセス中に削除されま

す。

ボリュームのリストア後も、 LUN と igroup とのマッピングはリストアの直前と同じ状態が維持されます。LUNマッピングは、Snapshot作成時点のマッピングとは異なる場合があります。ホストクラスタによる LUN の永続的予約は維持されます。

手順

1. ボリューム内のすべての LUN に対する I/O を停止します。
2. SnapVaultセカンダリボリュームが含まれているセカンダリボリュームを確認します。

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

3. リストア元のSnapshotを特定します。

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. 使用するSnapshotを指定します。

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

リストア先として指定するのは、リストア先の元のボリュームです。

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. ホストクラスタ間で LUN を共有している場合は、影響を受けるホストから LUN に対する永続的予約をリストアします。

SnapVault バックアップからのボリュームのリストア

次の例では、Snapshotの作成後にlun_Dという名前のLUNがボリュームに追加されています。Snapshotからボリューム全体をリストアすると、lun_Dは表示されなくなります。

コマンド出力では `lun show`、プライマリボリュームsrcvolA内のLUNと、SnapVaultセカンダリボリュームdstvolB内のこれらのLUNの読み取り専用コピーを確認できます。SnapVault バックアップに lun_D のコピーはありません。

```
cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than snapshot hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

ボリュームが SnapVault セカンダリボリュームからリストアされると、ソースボリュームには lun_D が存在しなくなりますリストア後もソースボリューム内の LUN のマッピングは維持されるため、再マッピングする必要はありません。

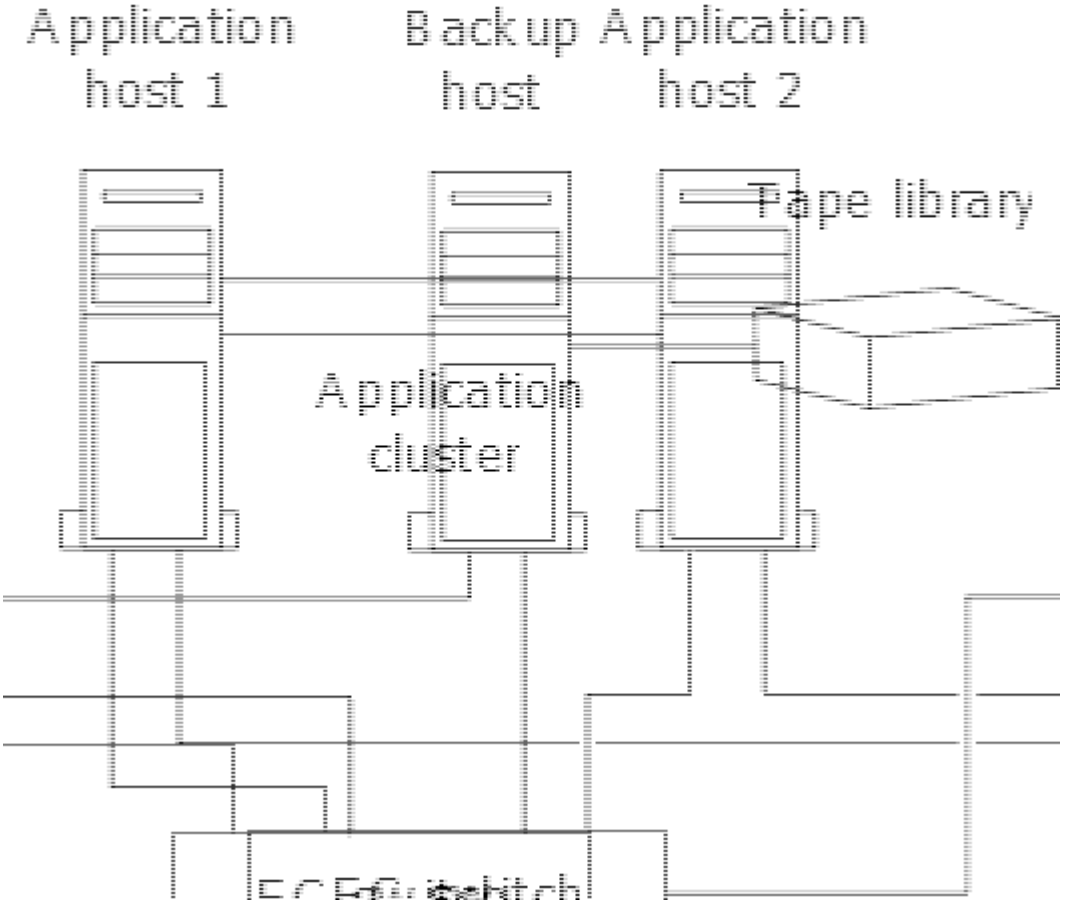
関連情報

- "スナップミラー復元"
- "snapmirror show"

ホストバックアップシステムを**ONTAP**に接続するための推奨構成

別のバックアップホストを使用してSANシステムをテープにバックアップすると、アプリケーションホストのパフォーマンス低下を回避できます。

バックアップのためには、SANデータとNASデータを分離しておくことが不可欠です。次の図は、プライマリストレージシステムに対するホストバックアップシステムの推奨される物理構成を示しています。ボリュームはSAN専用として設定する必要があります。LUNは単一のボリュームに限定することも、複数のボリュームまたはストレージシステムに分散させることもできます。



ホスト上のボリュームは、ストレージシステムからマッピングされた単一のLUN、またはボリュームマネージャを使用する複数のLUN（HP-UXシステムのVxVMなど）で構成できます。

ホストバックアップシステムを使用して**ONTAP**ストレージシステム上の**LUN**を保護する

ホストバックアップシステムのソースデータとして、Snapshotからクローニングされたを使用できます。

開始する前に

本番用LUNが存在し、アプリケーションサーバのWWPNまたはイニシエータノード名を含むigroupにマッピングされている必要があります。また、LUNがフォーマットされていて、ホストからアクセスできる必要があります。

手順

1. ホストファイルシステムバッファの内容をディスクに保存します。

   ホストオペレーティングシステムのコマンドを使用するか、SnapDrive（Windows）またはSnapDrive（UNIX）を使用できます。この手順をSANバックアップの前処理スクリプトに含めることもできます。

2. 本番LUNのスナップショットを作成します。

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. 本番用LUNのクローンを作成します。

```
volume file clone create -vserver <SMV_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. バックアップサーバのWWPNを含むigroupを作成します。

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
<protocol> -ostype <os_type> -initiator <initiator>
```

5. 手順3で作成したLUNクローンをバックアップホストにマッピングします。

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup>
```

   この手順をSANバックアップアプリケーションのポストプロセススクリプトに含めることもできます。

6. ホストから、新しいLUNを検出し、ファイルシステムをホストで使用できるようにします。

   この手順をSANバックアップアプリケーションのポストプロセススクリプトに含めることもできます。

7. SANバックアップアプリケーションを使用して、バックアップホストのLUNクローン内のデータをテープにバックアップします。
8. LUNクローンをオフラインにします。

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. LUNクローンを削除します。

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. スナップショットを削除します。

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN構成のリファレンス

ONTAP SAN構成の詳細

Storage Area Network（SAN；ストレージエリアネットワーク）は、iSCSIやFCなどのSAN転送プロトコルを使用してホストに接続されるストレージソリューションで構成されます。ストレージソリューションが1つ以上のスイッチを介してホストに接続されるようにSANを設定できます。iSCSIを使用している場合は、スイッチを使用せずにストレージソリューションをホストに直接接続するようにSANを設定することもできます。

SANでは、Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストが、ストレージソリューションに同時にアクセスできます。および"ポートセット"を使用すると、ホストとストレージの間のデータアクセスを制限できます"選択的LUNマッピング"。

iSCSIの場合、ストレージソリューションとホスト間のネットワークトポロジをネットワークと呼びます。FC、FC / NVMe、FCoEの場合、ストレージソリューションとホストの間のネットワークトポロジをファブリックと呼びます。冗長性を確保してデータアクセスの中断からデータを保護するには、マルチネットワークまたはマルチファブリック構成のHAペアを使用してSANをセットアップする必要があります。シングルノードまたはシングルネットワーク/ファブリックを使用する構成は完全な冗長性がないため、推奨されません。

SANの設定が完了したら"iSCSIまたはFC用のストレージのプロビジョニング"、またはを実行できます"FC / NVMe用のストレージのプロビジョニング"。その後、ホストに接続してデータの提供を開始できます。

SANプロトコルのサポートは、ONTAPのバージョン、プラットフォーム、構成によって異なります。特定の設定の詳細については、を参照して"NetApp Interoperability Matrix Tool"ください。

関連情報

- "SANの管理の概要"
- "NVMeの構成、サポート、制限事項"

iSCSIコウセイ

ONTAPシステムでのiSCSIネットワークの設定

iSCSI構成は、iSCSI SANホストに直接接続されたハイアベイラビリティ（HA）ペアか、1つ以上のIPスイッチを介してホストと接続されたHAペアでセットアップします。

"HAペア"ホストがLUNへのアクセスに使用するアクティブ/最適化パスとアクティブ/非最適パスのレポートノードとして定義されます。Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから同時にストレージにアクセスできます。ホストには、ALUAをサポートするサポート対象のマルチパスソリューションがインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、で確認できます"NetApp Interoperability Matrix Tool"。

マルチネットワーク構成では、ホストをストレージシステムに接続するスイッチが複数あります。完全な冗長性を備えたマルチネットワーク構成を推奨します。シングルネットワーク構成では、1台のスイッチでホストをストレージシステムに接続します。シングルネットワーク構成では完全な冗長性は確保されません。

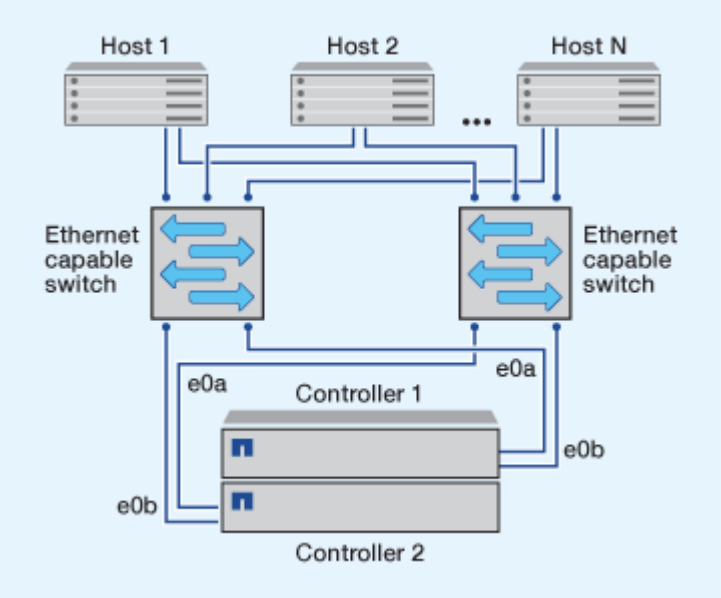
"シングルノードコウセイ"は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- HAペアが所有するLUNへのアクセスに使用するパスを制限する方法について説明します。"選択的LUNマッピング（SLM）"
- 詳細はこちらをご覧ください "SAN LIF"。
- については、を参照して"iSCSIにおけるVLANの利点"ください。

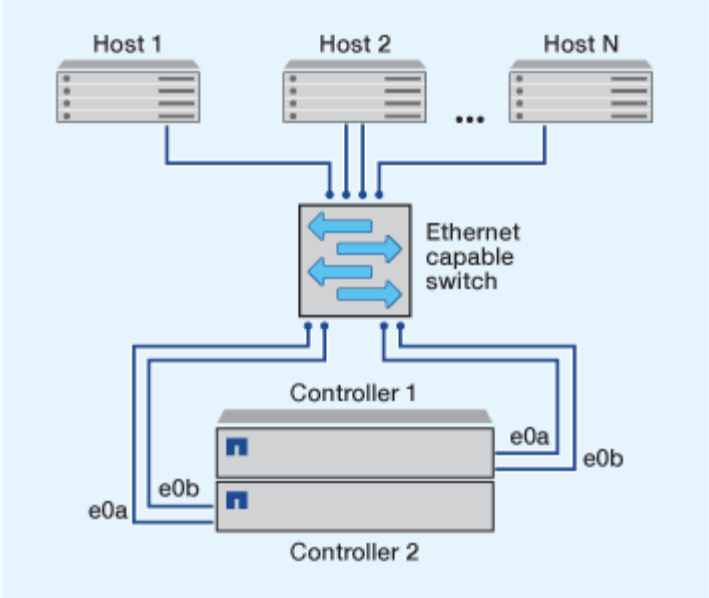
マルチネツトワアク**iSCSI**コウセイ

マルチネットワークのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。スイッチが複数あるため、この構成では完全な冗長性が確保されます。



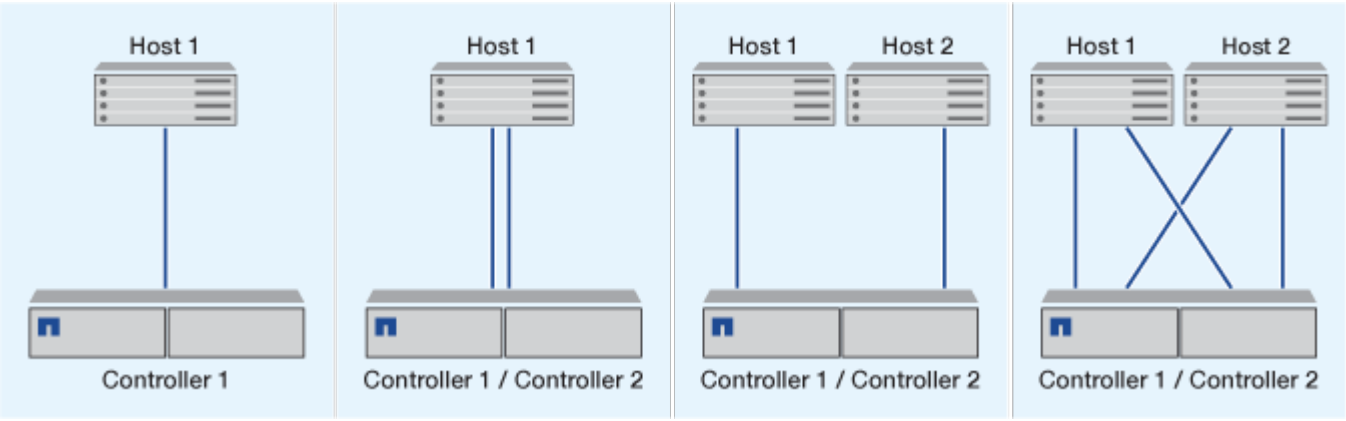
タンイチネツトワアクノ**iSCSI**コウセイ

単一ネットワークのHAペア構成では、HAペアを1つのスイッチで1つ以上のホストに接続します。スイッチが1台しかないため、この構成では完全な冗長性は確保されません。



直接接続型**iSCSI**構成

直接接続型の構成では、1つ以上のホストをコントローラに直接接続します。



iSCSI構成で**ONTAP**システムで**VLAN**を使用する利点

VLANは、ブロードキャストドメインにグループ化されたスイッチポートのグループで構成されます。VLANは、単一のスイッチ上に配置することも、複数のスイッチシャーシにまたがって配置することもできます。静的VLANと動的VLANを使用すると、IPネットワークインフラ内のセキュリティを強化し、問題を切り分け、使用可能なパスを制限できます。

大規模なIPネットワークインフラにVLANを実装すると、次のような利点が得られます。

- セキュリティの強化：

  VLANを使用すると、イーサネットネットワークまたはIP SANの異なるノード間のアクセスが制限されるため、既存のインフラを活用しながらセキュリティを強化できます。

- 問題を切り分けることで、イーサネットネットワークとIP SANの信頼性が向上します。

- 問題領域を制限することで、問題解決時間を短縮
- 特定のiSCSIターゲットポートへの使用可能なパスの数が削減されます。
- ホストで使用されるパスの最大数が削減されます。

  パスが多すぎると、再接続時間が遅くなります。ホストにマルチパスソリューションがない場合は、VLANを使用してパスを1つだけ許可できます。

動的な**VLAN**

ダイナミックVLANはMACアドレスベースです。VLANを定義するには、含めるメンバーのMACアドレスを指定します。

動的VLANは柔軟性を提供し、デバイスがスイッチに物理的に接続されている物理ポートへのマッピングを必要としません。VLANを再設定することなく、1つのポートから別のポートにケーブルを移動できます。

セイテキナ**VLAN**

静的なVLANはポートベースです。スイッチとスイッチポートは、VLANとそのメンバーを定義するために使用されます。

スタティックVLANは、メディアアクセス制御（MAC）スプーフィングを使用してVLANを侵害できないため、セキュリティが向上します。ただし、誰かがスイッチに物理的にアクセスできる場合は、ケーブルを交換してネットワークアドレスを再設定するとアクセスが許可されます。

環境によっては、動的なVLANよりも静的なVLANを作成および管理する方が簡単です。これは、スタティックVLANでは、48ビットのMACアドレスではなく、スイッチとポートの識別子だけを指定する必要があるためです。さらに、VLAN IDを使用してスイッチポート範囲にラベルを付けることもできます。

FCコウセイ

ONTAPシステムでの**FC**ファブリックまたは**FC-NVMe**ファブリックの設定

FCおよびFC-NVMe SANホストは、HAペアと、少なくとも2つのスイッチを使用して構成することを推奨します。これにより、ファブリック レイヤとストレージ システム レイヤで冗長性が確保され、フォールト トレランスとノンストップ オペレーションがサポートされます。FCまたはFC-NVMe SANホストをスイッチを使用せずにHAペアに直接接続することはできません。

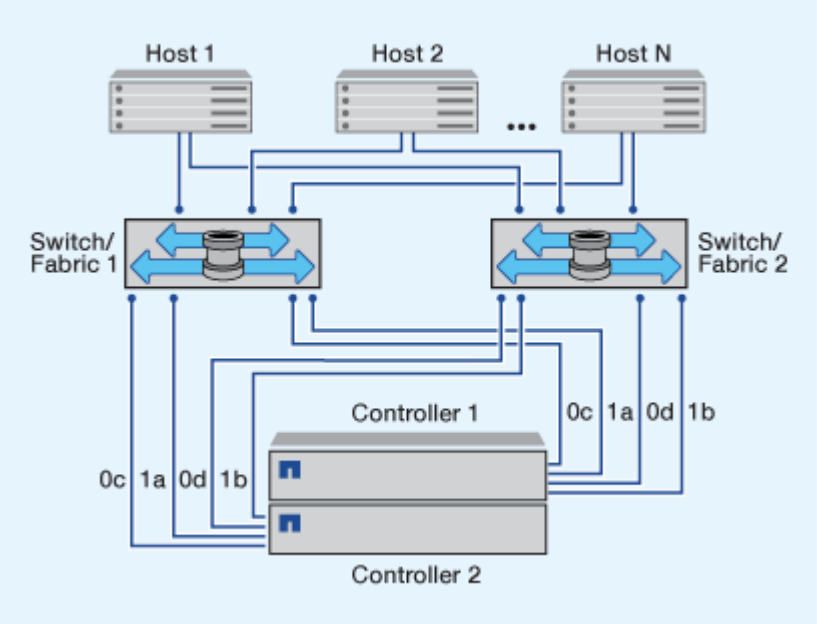
カスケード ファブリック、部分メッシュ ファブリック、フルメッシュ ファブリック、コアエッジ ファブリック、およびディレクタ ファブリックは、FCスイッチをファブリックに接続する業界標準の方法であり、いずれもサポートされます。異機種混在のFCスイッチ ファブリックの使用は、組み込みのブレード スイッチ以外はサポートされません。特定の例外については、を"Interoperability Matrix Tool"参照してください。ファブリックは1つまたは複数のスイッチで構成でき、ストレージコントローラは複数のスイッチに接続できます。

Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから、ストレージコントローラに同時にアクセスできます。ホストには、サポートされているマルチパスソリューションがインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、Interoperability Matrix Toolで確認できます。

マルチファブリックノ**FC**コウセイオヨビ**FC-NVMe**コウセイ

マルチファブリックのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。次の図は、マルチファブリックのHAペアを示しています。わかりやすいように、この図ではファブリックが2つだけになっていますが、マルチファブリック構成は2つ以上の任意の数のファブリックで構成できます。

次の図のFCターゲット ポート番号（0c、0d、1a、1b）は一例です。実際のポート番号は、使用しているストレージ ノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

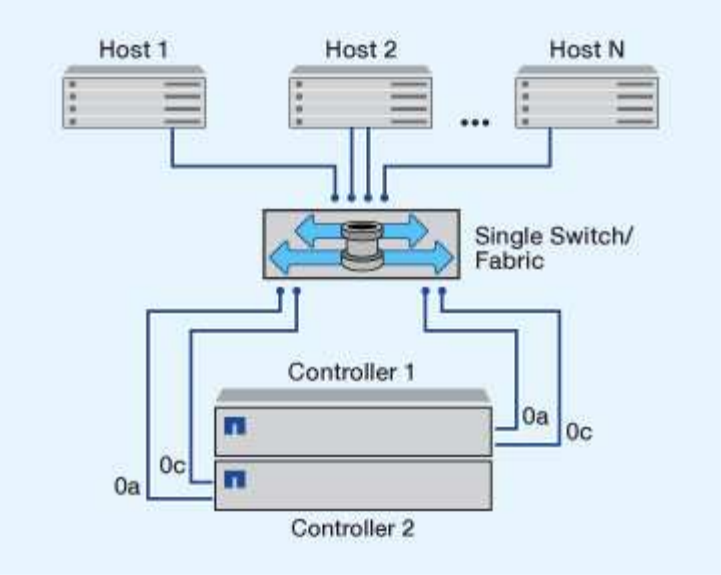


タンイツファブリックノ**FC**コウセイオヨビ**FC-NVMe**コウセイ

単一ファブリックのHAペア構成では、HAペアの両方のコントローラを1つのファブリックで1つ以上のホストに接続します。ホストとコントローラは単一のスイッチを介して接続されるため、単一ファブリックのHAペア構成では完全な冗長性は確保されません。

次の図のFCターゲットポート番号（0a、0c）は一例です。実際のポート番号は、ストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

単一ファブリックのHAペア構成は、FC構成をサポートするすべてのプラットフォームでサポートされます。



"シングルノードコウセイ"は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- HAペアが所有するLUNへのアクセスに使用するパスを制限する方法について説明します。"選択的LUNマッピング（SLM）"
- 詳細はこちらをご覧ください "SAN LIF"。

ONTAPシステムで**FC**スイッチを設定する際のベストプラクティス

FCスイッチを設定する際には、パフォーマンスを最大限に高めるために一定のベストプラクティスを考慮する必要があります。

FCスイッチの構成では、リンク速度を固定に設定することを推奨します。これは、ファブリックのリビルド時に最適なパフォーマンスが得られるため、時間を大幅に節約できるため、大規模なファブリックに特に適しています。自動ネゴシエーションは柔軟性に優れていますが、FCスイッチの構成が必ずしも期待どおりのパフォーマンスを発揮するとは限らず、ファブリック全体の構築時間が長くなります。

ファブリックに接続されているすべてのスイッチでN_Port ID Virtualization（NPIV）がサポートされ、NPIVが有効になっている必要があります。ONTAPは、NPIVを使用してFCターゲットをファブリックに提示します。

サポートされる環境の詳細については、を参照してください "NetApp Interoperability Matrix Tool"。

FCとiSCSIのベストプラクティスについては、を参照してください "NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"。

ONTAPシステムの推奨される**FC**ターゲットポート構成と速度

FC-NVMeプロトコル用のFCターゲットポートは、FCプロトコル用の設定および使用とまったく同じ方法で設定および使用できます。FC-NVMeプロトコルがサポートされるかどうかは、プラットフォームとONTAPのバージョンによって異なります。NetApp Hardware Universeを使用してサポートを確認します。

最適なパフォーマンスと可用性を実現するには、使用するプラットフォームに対応したに記載されている推奨されるターゲットポート構成を使用する必要があります "NetApp Hardware Universe"。

共有ASICを使用するFCターゲットポートの設定

次のプラットフォームには、ASIC（特定用途向け共有集積回路）を使用したポートペアがあります。これらのプラットフォームで拡張アダプタを使用する場合は、接続に同じASICが使用されないようにFCポートを設定する必要があります。

コントローラ	ASIC を共有するポートペア	ターゲットポートの数：推奨ポート
• FAS8200 • AFF A300用	0g+0h	1：0g 2：0g、0h
• FAS2720 • FAS2750 • AFF A220用	0c+0d 0e+0f	1：0c 2：0c、0e 3：0c、0e、0d 4：0c、0e、0d、0f

サポートされるFCターゲットポートの速度

FCターゲットポートは、さまざまな速度で実行するように設定できます。特定のホストで使用されるすべてのターゲットポートを同じ速度に設定する必要があります。ターゲットポートの速度は、接続先デバイスの速度と同じに設定する必要があります。ポート速度に自動ネゴシエーションを使用しないでください。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

オンボードポートと拡張アダプタは、次の速度で実行するように設定できます。コントローラと拡張アダプタのポートは、必要に応じて、さまざまな速度で実行するように個別に構成することができます。

4Gb ポート	8Gb ポート	16Gb ポート	32Gb ポート
• 4 Gb • 2Gb • 1Gb	• 8Gb • 4 Gb • 2Gb	• 16Gb • 8Gb • 4 Gb	• 32Gb • 16Gb • 8Gb

サポートされているアダプタとサポートされている速度の一覧については、を参照してください "NetApp Hardware Universe"。

ONTAP FCアダプタポートの設定

オンボードFCアダプタと一部のFC拡張アダプタカードは、イニシエータポートまたはターゲットポートとして個別に構成できます。その他のFC拡張アダプタは、工場出荷時にイニシエータまたはターゲットとして構成されており、変更することはできません。FC SFP+アダプタで構成されたサポート対象のUTA2カードから、FCポートを追加することもできます。

イニシエータポートを使用してバックエンドディスクシェルフに直接接続でき、場合によっては外部ストレー

ジアレイに接続できます。ターゲットポートはFCスイッチへの接続にのみ使用できます。

FC用に設定されたオンボードポートとCNA / UTA2ポートの数は、コントローラのモデルによって異なります。サポートされるターゲット拡張アダプタも、コントローラのモデルによって異なります。オンボードのFCポートと、コントローラモデルでサポートされるターゲット拡張アダプタの一覧については、を参照してください"NetApp Hardware Universe"。

FCアダプタのイニシエータモード設定

イニシエータモードは、ポートをテープドライブ、テープライブラリ、またはForeign LUN Import（FLI）対応のサードパーティ製ストレージに接続するために使用されます。FC

開始する前に

- アダプタのLIFを、メンバーになっているすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更対象の物理ポートを使用するすべてのStorage Virtual Machine（SVM）のすべてのLIFを移行または破棄する必要があります。

NVMe/FCではイニシエータモードがサポートされます。

手順

1. アダプタからすべてのLIFを削除します。

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. アダプタをオフラインにします。

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対してFCポートが正しい状態で設定されていることを確認します。

```
system hardware unified-connect show
```

6. アダプタをオンラインに戻します。

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

FCアダプタのターゲットモード設定

ターゲットモードは、ポートをFCイニシエータに接続するために使用されます。

FCアダプタを設定する手順は、FCプロトコルとFC-NVMeプロトコルについても同じです。ただし、FC-NVMeをサポートするFCアダプタは一部のみです。FC-NVMeプロトコルをサポートするアダプタのリストについては、を参照してください"NetApp Hardware Universe"。

手順

1. アダプタをオフラインにします。

   ```
   node run -node _node_name_ storage disable adapter _adapter_name_
   ```

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

   ```
   system node hardware unified-connect modify -t target -node _node_name_
   adapter _adapter_name_
   ```

3. 変更したアダプタをホストしているノードをリブートします。
4. ターゲットポートの設定が正しいことを確認します。

   ```
   network fcp adapter show -node _node_name_
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node _node_name_ -adapter _adapter_port_
   -state up
   ```

FCアダプタ速度の設定

自動ネゴシエーションを使用する代わりに、アダプタのターゲットポートの速度を接続先デバイスの速度と同じに設定する必要があります。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

タスクの内容

この処理ではクラスタ内のすべてのStorage Virtual Machine（SVM）とLIFが対象となるため、パラメータと`-home-lif`パラメータを使用して処理範囲を制限する必要があります `-home-port`。これらのパラメー

タを使用しないと、処理環境によってクラスタ内のすべての LIF が処理によって使用されなくなる可能性があります。

開始する前に

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

手順

1. アダプタのすべての LIF をオフラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. アダプタをオフラインにします。

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

3. ポートアダプタの最大速度を確認します。

```
fcp adapter show -instance
```

アダプタ速度を最大速度よりも速くすることはできません。

4. アダプタ速度を変更します。

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. アダプタをオンラインにします。

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. アダプタのすべての LIF をオンラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

FCアダプタの管理用**ONTAP**コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、 FC イニ

シエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、 FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。FCイニシエータアダプタのコマンドを使用する前に、コマンドを使用する必要があります `run -node node_name`。

FC ターゲットアダプタの管理用コマンド

状況	使用するコマンド
ノードの FC アダプタ情報を表示する	`network fcp adapter show`
FC ターゲットアダプタのパラメータを変更する	`network fcp adapter modify`
FC プロトコルトラフィック情報を表示します	`run -node node_name sysstat -f`
FC プロトコルの実行時間を表示します	`run -node node_name uptime`
アダプタの設定とステータスを表示します	`run -node node_name sysconfig -v adapter`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node node_name sysconfig -ac`
コマンドのマニュアルページを表示します	`man command_name`

FC イニシエータアダプタの管理用コマンド

状況	使用するコマンド
ノードのすべてのイニシエータおよびそのアダプタの情報を表示する	`run -node node_name storage show adapter`
アダプタの設定とステータスを表示します	`run -node node_name sysconfig -v adapter`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node node_name sysconfig -ac`

オンボード **FC** アダプタの管理用コマンド

状況	使用するコマンド
オンボード FC ポートのステータスを表示します	`system node hardware unified-connect show`

関連情報

- "ネットワークFCPアダプタ"

X1133A-R6アダプタを使用した**ONTAP**システムへの接続の切断を回避する

別のX1133A-R6 HBAへの冗長パスをシステムに設定することで、ポート障害時に接続が失われないようにすることができます。

X1133A-R6 HBA は、 4 ポート 16Gb の FC アダプタで、 2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1 、ポート 3 とポート 4 は ASIC 2 ）。単一のASIC上の両方のポートは、ターゲットモードまたはイニシエータモードのいずれかで同じモードで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、 HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

FCoEコウセイ

ONTAPシステムでの**FCoE**ファブリックの設定

FCoEは、FCoEスイッチを使用してさまざまな方法で設定できます。直接接続型の構成はFCoEではサポートされません。

FCoE構成はすべてデュアルファブリックで、完全に冗長化されており、ホスト側のマルチパスソフトウェアが必要です。いずれのFCoE構成でも、イニシエータとターゲット間のパスには、最大ホップ数の範囲内でFCoEスイッチとFCスイッチを複数配置できます。スイッチを相互に接続するには、イーサネットISLに対応したバージョンのファームウェアがスイッチで実行されている必要があります。FCoE構成の各ホストでオペレーティングシステムが異なることがあります。

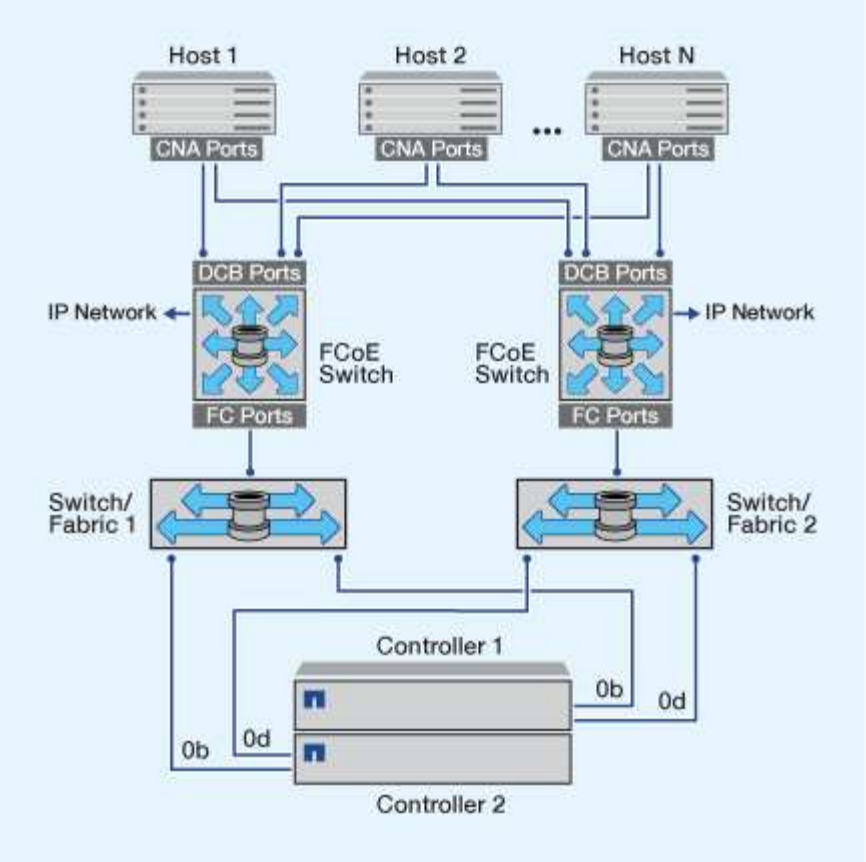
FCoE構成には、FCoEの機能を明示的にサポートするイーサネットスイッチが必要です。FCoE構成は、FCスイッチと同じ相互運用性と品質管理のプロセスで検証されます。サポートされる構成の一覧については、Interoperability Matrixを参照してください。サポートされる構成に含まれるパラメータには、スイッチモデル、単一ファブリックに導入できるスイッチの数、サポートされるスイッチファームウェアのバージョンなどがあります。

次の図のFCターゲット拡張アダプタのポート番号は一例です。実際のポート番号は、FCoEターゲット拡張アダプタがインストールされている拡張スロットによって変わる場合があります。

FCoEイニシエータから**FC**ターゲット

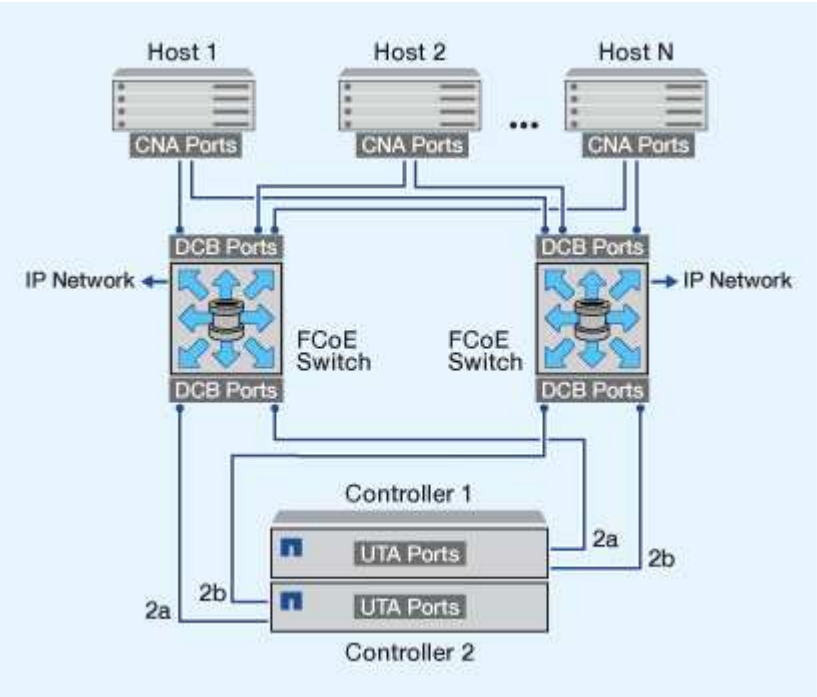
FCoEイニシエータ（CNA）を使用すると、FCoEスイッチからFCターゲットポートに接続して、ホストをHAペアの両方のコントローラに接続できます。FCoEスイッチにはFCポートも必要です。ホストのFCoEイニシエータは常にFCoEスイッチに接続されます。FCoEスイッチは、FCターゲットに直接接続することも、FCスイッチを介してFCターゲットに接続することもできます。

次の図では、ホストのCNAをFCoEスイッチに接続し、FCスイッチをHAペアに接続しています。



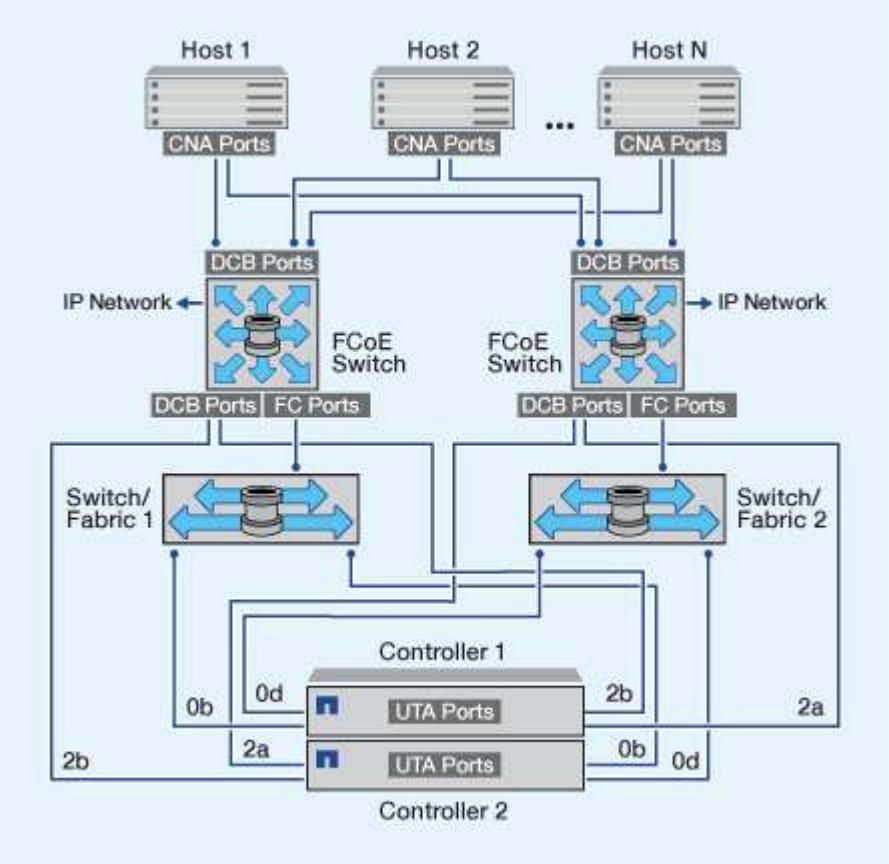
FCoEイニシエータから**FCoE**ターゲット

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。



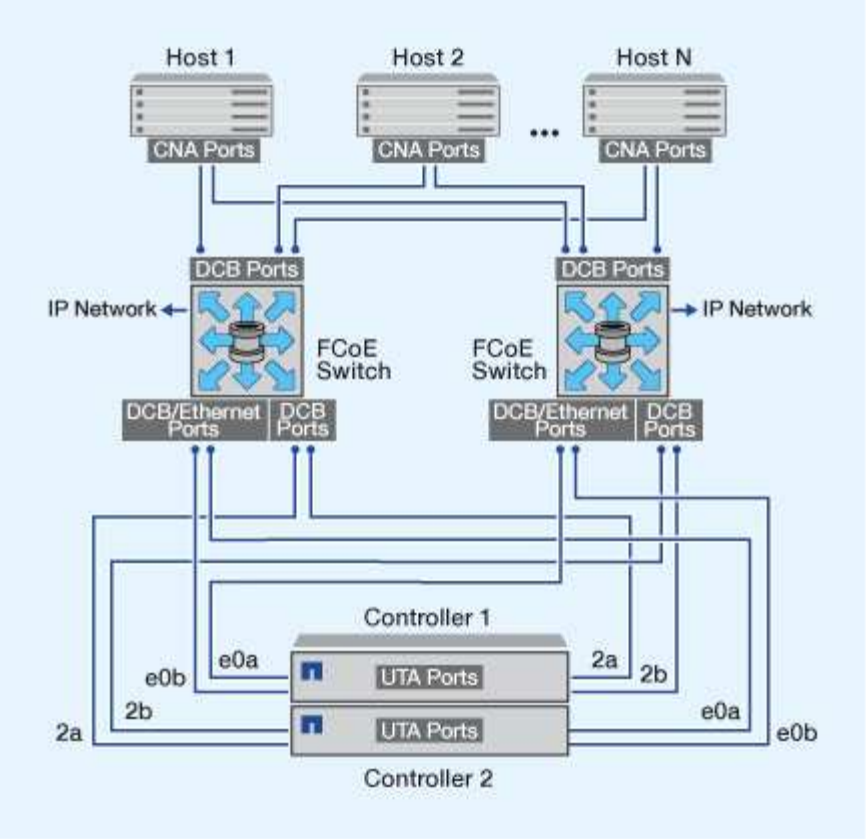
FCoEイニシエータから**FCoE**および**FC**ターゲット

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEおよびFCターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。



FCoEと**IP**ストレージプロトコルの混在

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。FCoEポートは、単一のスイッチへの従来のリンクアグリゲーションを使用できません。Ciscoスイッチでは、FCoEをサポートする特殊なタイプのリンクアグリゲーション（仮想ポートチャネル）がサポートされます。仮想ポートチャネルは、2つのスイッチへの個 々 のリンクを集約します。仮想ポートチャネルは、他のイーサネットトラフィックにも使用できます。NFS、SMB、iSCSI、およびその他のイーサネットトラフィックなど、FCoE以外のトラフィックに使用されるポートでは、FCoEスイッチの通常のイーサネットポートを使用できます。



ONTAPでサポートされる**FCoE**イニシエータとターゲットポートの組み合わせ

FCoEと従来のFCのイニシエータとターゲットの特定の組み合わせがサポートされます。

FCoEイニシエータ

ホストコンピュータのFCoEイニシエータは、ストレージコントローラのFCoEターゲットと従来のFCターゲットの両方で使用できます。ホストのFCoEイニシエータはFCoE DCB（Data Center Bridging）スイッチに接続する必要があります。ターゲットに直接接続することはできません。

次の表に、サポートされる組み合わせを示します。

イニシエータ	ターゲット	サポートの有無
FC	FC	○
FC	FCoE	○
FCoE	FC	○
FCoE	FCoE	○

FCoEターゲット

ストレージコントローラでFCoEターゲットポートと4Gb、8Gb、または16GbのFCポートを混在させることができます。FCポートがアドインのターゲットアダプタであるかオンボードのポートであるかは関係ありません。FCoEとFCの両方のターゲットアダプタを同じストレージコントローラに搭載できます。

FCのオンボードポートと拡張ポートの組み合わせルールも適用されます。

FCオヨビFCoEソオニンク

ONTAPシステムを使用したFCおよびFCoEのゾーニングについて

FC ゾーン、 FC-NVMe ゾーン、または FCoE ゾーンは、ファブリック内の 1 つ以上のポートを論理的にグループ化したものです。デバイスがお互いを認識し、接続し、相互にセッションを作成し、通信できるようにするには、両方のポートが同じゾーンのメンバーである必要があります。

ゾーンを共有するエンドポイントへのアクセスと接続を制限することで、セキュリティを強化します。同じゾーンにないポートは相互に通信できません。これにより、イニシエータHBA間の_クロストーク_が削減または排除されます。接続の問題が発生した場合にゾーニングを使用すると、問題を特定のポートセットに切り分けて解決までの時間を短縮できます。

特定のポートへの使用可能なパスの数と、ホストとストレージシステムの間のパスの数を削減します。たとえば、一部のホスト OS のマルチパスソリューションには、管理できるパスの数に制限があります。ゾーニングを使用すると、ホストに認識されるパスの数を減らして、ホストへのパスがホストOSで許可されている最大数を超えないようにすることができます。

World Wide Nameに基づくゾーニング

World Wide Name（WWN）に基づくゾーニングでは、ゾーンに含めるメンバーのWWNを指定します。一部のスイッチベンダーではWorld Wide Node Name（WWNN；ワールドワイドノード名）ゾーニングを使用できますが、ONTAPでゾーニングを行う場合は、World Wide Port Name（WWPN；ワールドワイドポート名）ゾーニングを使用する必要があります。

特定のポートを適切に定義し、NPIVを効果的に使用するには、WWPNゾーニングが必要です。FCスイッチは、ノードの物理ポートのWWPNではなく、ターゲットの論理インターフェイス（LIF）のWWPNを使用してゾーニングする必要があります。物理ポートの WWPN は「 50 」で始まり、 LIF の WWPN は「 20 」で始まります。

WWPNゾーニングは柔軟性に優れており、デバイスがファブリックに物理的に接続されている場所によってアクセスが決まりません。ゾーンを再設定することなく、1つのポートから別のポートにケーブルを移動できます。

ONTAPシステムヨウノFCオヨヒFCoEソオニンクセツテイ

ホストにマルチパスソリューションがインストールされていない場合、SANにホストを4つ以上接続する場合、またはクラスタ内のノードに選択的LUNマッピングが実装されていない場合は、ゾーニング設定を作成する必要があります。

FCおよびFCoEの推奨されるゾーニング設定では、各ゾーンに1つのイニシエータポートと1つ以上のターゲットLIFが含まれます。この構成では、各ホストイニシエータは任意のノードにアクセスできますが、同じノー

ドにアクセスするホストはお互いのポートを認識できません。

Storage Virtual Machine（SVM）のすべてのLIFをホストイニシエータを含むゾーンに追加します。これにより、既存のゾーンを編集したり、新しいゾーンを作成したりせずに、ボリュームや LUN を移動できます。

dual-fabricゾーニング構成

単一コンポーネントの障害によるデータ損失から保護できるため、デュアルファブリックゾーニング構成を推奨します。デュアルファブリック構成では、各ホストイニシエータが異なるスイッチを使用してクラスタ内の各ノードに接続されます。一方のスイッチが使用できなくなっても、残りのスイッチを介してデータアクセスが維持されます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。

次の図では、ホストに2つのイニシエータがあり、マルチパスソフトウェアを実行しています。2つのゾーンがあります。"選択的LUNマッピング（SLM）"すべてのノードがレポートノードとみなされるように設定されています。

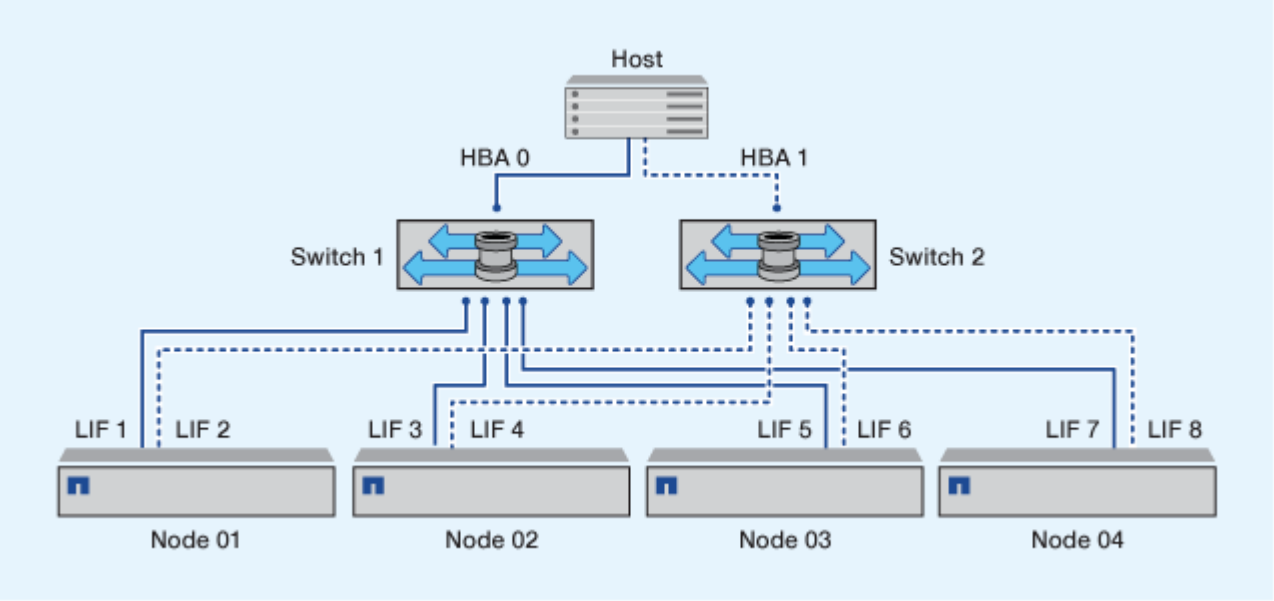
この図で使用されている命名規則は、ONTAPソリューションで使用できる一例です。

- ゾーン1：HBA 0、LIF_1、LIF_3、LIF_5、およびLIF_7
- ゾーン2：HBA 1、LIF_2、LIF_4、LIF_6、およびLIF_8

各ホストイニシエータは、異なるスイッチを使用してゾーニングされます。ゾーン1にはスイッチ1からアクセスします。ゾーン2にはスイッチ2からアクセスします。

各ホストは、すべてのノードのLIFにアクセスできます。これにより、ノードで障害が発生しても、ホストはLUNに引き続きアクセスできます。SVMは、SLMレポートノードの設定に基づいて、クラスタ内のすべてのノードのすべてのiSCSI LIFとFC LIFにアクセスできます。SLM、ポートセット、またはFCスイッチゾーニングを使用して、SVMからホストへのパスの数とSVMからLUNへのパスの数を減らすことができます。

構成に追加のノードが含まれている場合、追加のノードのLIFはこれらのゾーンに含まれます。



ホストオペレーティングシステムとマルチパスソフトウェアが、ノード上のLUNへのアクセスに使用される数のパスをサポートしている必要があります。

単一ファブリック構成では、1つのスイッチを使用して各ホストイニシエータを各ストレージノードに接続します。単一ファブリックゾーニング構成は、単一コンポーネントの障害によるデータ損失から保護されないため、推奨されません。単一ファブリックゾーニングを設定する場合は、ソリューションの耐障害性を確保するために、マルチパス用のイニシエータを各ホストに2つ用意する必要があります。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。

各ホストイニシエータには、イニシエータがアクセスできる各ノードのLIFが少なくとも1つ必要です。ホストイニシエータからクラスタ内のHAペアのノードへのパスが少なくとも1つあるようにゾーニングを設定して、LUN接続用のパスを提供する必要があります。つまり、ホスト上の各イニシエータには、そのゾーン構成内のノードごとにターゲットLIFが1つだけ割り当てられます。クラスタ内の同じノードまたは複数のノードへのパスが複数必要な場合は、ゾーン構成内の各ノードに複数のLIFが割り当てられます。これにより、ノードに障害が発生した場合や、LUNを含むボリュームが別のノードに移動された場合でも、ホストはLUNに引き続きアクセスできます。また、レポートノードを適切に設定する必要があります。

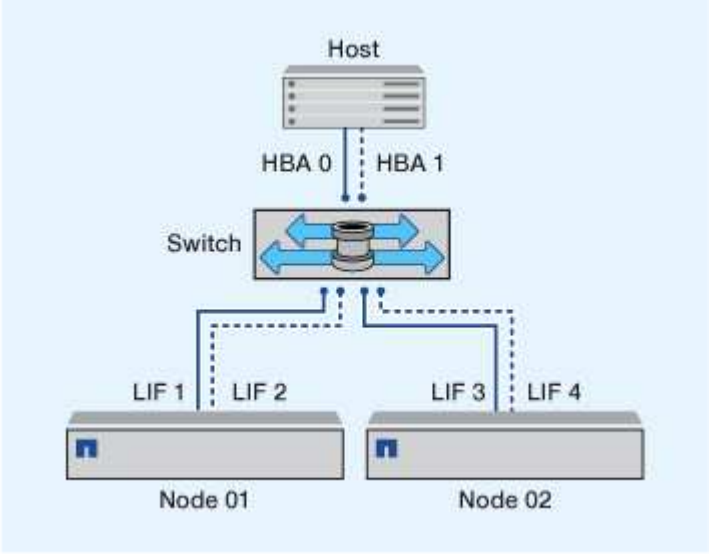
Cisco FC スイッチおよび FCoE スイッチを使用する場合、 1 つのファブリックゾーンに同じ物理ポートのターゲット LIF を複数含めることはできません。同じポートの LIF を同じゾーンに複数配置すると、接続が失われた場合に LIF ポートがリカバリできなくなる可能性があります。

次の図では、ホストに2つのイニシエータがあり、マルチパス ソフトウェアを実行しています。次の2つのゾーンがあります。

この図で使用されている命名規則は、ONTAPソリューションで使用できる一例です。

- ゾーン1：HBA 0、LIF_1、およびLIF_3
- ゾーン2：HBA 1、LIF_2、およびLIF_4

構成に追加のノードが含まれている場合、追加のノードのLIFはこれらのゾーンに含まれます。



この例では、各ゾーンに4つのLIFをすべて配置することもできます。その場合のゾーンは次のようになります。

- ゾーン1：HBA 0、LIF_1、LIF_2、LIF_3、およびLIF_4
- ゾーン2：HBA 1、LIF_1、LIF_2、LIF_3、およびLIF_4

ホストオペレーティングシステムとマルチパスソフトウェアが、ノード上のLUNへのアクセスに使用される数のパスをサポートしている必要があります。ノードのLUNへのアクセスに使用するパスの数については、SAN構成の制限に関するセクションを参照してください。

Cisco FCおよび**FCoE**スイッチのゾーニング制限

Cisco FCおよびFCoEスイッチを使用する場合、ゾーンでの物理ポートと論理インターフェイス（LIF）の使用には一定の制限が適用されます。

物理ポート

- FC-NVMeとFCで同じ32Gb物理ポートを共有可能
- FC-NVMeとFCoEは同じ物理ポートを共有できない
- FCとFCoEは同じ物理ポートを共有できますが、プロトコルLIFは別 々 のゾーンに配置する必要があります。

論理インターフェイス（**LIF**）

- ゾーンには、クラスタ内のすべてのターゲットポートのLIFを1つ含めることができます。

  ホストへのパスの最大数を超えないように、SLMの設定を確認します。

- 特定のポートの各LIFは、そのポートの他のLIFとは別のゾーンに配置する必要があります。
- 物理ポートが異なる LIF は、同じゾーンに配置することもできます。

ONTAPシステムと**NetApp**以外のシステムに接続された**SAN**ホストの要件

共有SAN構成とは、ONTAPストレージシステムと他社のストレージシステムの両方に接続されるホストのことです。ONTAPストレージシステムと他のベンダーのストレージシステムに単一のホストからアクセスする場合は、いくつかの要件を満たす必要があります。

すべてのホストオペレーティングシステムで、各ベンダーのストレージシステムへの接続には別 々 のアダプタを使用することを推奨します。別 々 のアダプタを使用すると、ドライバと設定が競合する可能性が低くなります。ONTAPストレージシステムに接続する場合は、NetApp Interoperability Matrix Toolにサポート対象として記載されているアダプタモデル、BIOS、ファームウェア、ドライバを使用する必要があります。

必須または推奨のタイムアウト値や、ホストのその他のストレージパラメータを設定する必要があります。NetAppソフトウェアをインストールするか、NetApp設定を最後に適用する必要があります。

- AIXの場合、構成に対応するAIX Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- ESXの場合、Virtual Storage Console for VMware vSphereを使用してホスト設定を適用します。
- HP-UXの場合は、HP-UXのデフォルトのストレージ設定を使用する必要があります。
- Linuxの場合、構成に対応するLinux Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- Solarisの場合、構成に対応するSolaris Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。

- Windowsの場合、構成に対応するWindows Host UtilitiesバージョンをInteroperability Matrix Toolで確認してインストールする必要があります。

関連情報

"NetApp Interoperability Matrix Tool"

MetroCluster環境でのSAN構成

ONTAP MetroCluster環境でサポートされるSAN構成

MetroCluster環境でSAN構成を使用する場合は、一定の考慮事項に注意する必要があります。

- MetroCluster 構成では ' フロントエンド FC ファブリックのルーテッド VSAN 構成はサポートされません
- ONTAP 9 .15.1以降では、NVMe/TCPで4ノードのMetroCluster IP構成がサポートされます。
- ONTAP 9.12.1以降では、NVMe / FCで4ノードのMetroCluster IP構成がサポートされます。MetroCluster構成は、ONTAP 9.12.1よりも前のフロントエンドNVMeネットワークではサポートされません。
- MetroCluster構成では、iSCSI、FC、FCoEなどのその他のSANプロトコルがサポートされます。
- SANクライアント構成を使用している場合は、（IMT）に記載されているメモにMetroCluster構成に関する特別な考慮事項がないかどうかを確認する必要があります"NetApp Interoperability Matrix Tool"。
- MetroClusterの自動計画外スイッチオーバーとTiebreakerまたはMediatorで開始されるスイッチオーバーをサポートするには、オペレーティングシステムとアプリケーションで120秒のI/O耐障害性を提供する必要があります。
- MetroCluster構成では、フロントエンドFCファブリックの両側で同じWWNNとWWPNが使用されます。

関連情報

- "MetroClusterのデータ保護とディザスタリカバリの概要"
- "NetAppナレッジベース: MetroCluster構成における AIX ホストのサポートに関する考慮事項は何ですか?"
- "NetAppナレッジベース: MetroCluster構成における Solaris ホストのサポートに関する考慮事項"

ONTAP MetroClusterのスイッチオーバーおよびスイッチバック時にポートの重複を回避

SAN環境では、古いポートがオフラインになって新しいポートがオンラインになったときに重複しないようにフロントエンドスイッチを設定できます。

スイッチオーバーの実行中、ディザスタサイトのFCポートがオフラインであることがファブリックで検出され、ネームサービスとディレクトリサービスからこのポートが削除される前に、サバイバーサイトのFCポートがファブリックにログインすることがあります。

災害時にFCポートをまだ削除していない場合、WWPNの重複が原因でサバイバーサイトのFCポートのファブリックログイン試行が拒否されることがあります。FCスイッチのこの動作は、既存のデバイスではなく以前のデバイスのログインを維持するように変更できます。この動作が他のファブリックデバイスに与える影響を確認する必要があります。詳細については、スイッチベンダーにお問い合わせください。

スイッチのタイプに応じて、正しい手順を選択します。

例 **22.** 手順

Ciscoスイッチ

1. スイッチに接続してログインします。
2. コンフィギュレーションモードを開始します。

```
switch# config t
switch(config)#
```

3. ネームサーバデータベースの最初のデバイスエントリを新しいデバイスで上書きします。

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.xを実行しているスイッチで、flogi quiesce timeoutがゼロに設定されていることを確認します。

   a. 休止時間を表示します。

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. 前の手順の出力でtimervalがゼロであることが示されていない場合は、ゼロに設定します。

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Brocadeスイッチ

1. スイッチに接続してログインします。
2. コマンドを入力します `switchDisable`。
3. コマンドを入力し `configure`、プロンプトでを押し `y`ます。

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. 設定1を選択：

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 残りのプロンプトに応答するか、 * Ctrl+D* を押します。
6. コマンドを入力します `switchEnable`。

関連情報

"テストまたはメンテナンスのためのスイッチオーバーの実行"

SANホストのマルチパスに対するONTAPのサポート

ONTAPは、FCホストとiSCSIホストの両方でのマルチパスにAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）ソフトウェアを使用します。

ONTAP 9.5以降では、Asynchronous Namespace Access（ANA）を使用するNVMeホストで、マルチパスハイアベイラビリティ（HA）ペアのフェイルオーバー/ギブバックがサポートされます。ONTAP 9.4では、NVMeでサポートされるホストからターゲットへのパスは1つだけであるため、アプリケーションホストでHAパートナーへのパスフェイルオーバーを管理する必要があります。

複数のパスを使用してLUNまたはNVMeネームスペースにアクセスできるSANホストには、マルチパスソフトウェアが必要です。LUNまたはNVMeネームスペースへのすべてのパスで単一のディスクをオペレーティングシステムに提供します。このパスがないと、オペレーティングシステムは各パスを個別のディスクとして扱い、データが破損する可能性があります。

次のいずれかに該当する場合、ソリューションには複数のパスがあるとみなされます。

- ホストの単一のイニシエータポートをSVMの複数のSAN LIFに接続している場合
- 複数のイニシエータポートをSVMの単一のSAN LIFに接続している場合
- 複数のイニシエータポートをSVMの複数のSAN LIFに接続している場合

HA構成では、マルチパスソフトウェア（マルチパスI/O）が推奨されます。マルチパスソフトウェアはMPIO（マルチパスI/O）ソフトウェアとも呼ばれます。選択的LUNマップに加えて、FCスイッチのゾーニングまたはポートセットを使用してLUNへのアクセスに使用するパスを制限することも推奨されます。

ALUAまたはANAをサポートする具体的なホスト構成については、ご使用のホストオペレーティングシステムに対応したおよび "ONTAP SANホスト構成"を参照して "NetApp Interoperability Matrix Tool"ください。

ホストからクラスタ内のノードへの推奨されるパス数

ホストからクラスタ内の各ノードへのパスは8個までにする必要があります。また、ホストOSおよびホストで使用されるマルチパスでサポートされるパスの総数を超えないようにしてください。

クラスタ内のStorage Virtual Machine（SVM）が使用する各レポートノードへのパスをLUNごとに少なくとも2つ確保します"選択的LUNマップ（SLM）"。これにより、単一点障害（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

クラスタにノードが4つ以上ある場合、またはいずれかのノードのSVMで5つ以上のターゲットポートを使用している場合は、次の方法でノード上のLUNへのアクセスに使用できるパスの数を制限して、推奨される最大数の8個を超えないようにすることができます。

- SLM

SLMを使用すると、ホストからLUNへのパスの数が、LUNを所有するノードとそのHAパートナーのパスだけになります。SLMはデフォルトで有効になっています。

- "iSCSIのポートセット"
- ホストのFC igroupマッピング
- FCスイッチゾーニング

構成の制限

ONTAPクラスタあたりのサポートされるノードと**SAN**ホストの最大数を確認する

クラスタでサポートされるノード数は、ONTAPのバージョン、コントローラモデル、およびクラスタノードのプロトコルによって異なります。クラスタに接続できるSANホストの最大数は、構成によっても異なります。

クラスタあたりのサポートされる最大ノード数の確認

FC、FC-NVMe、FCoE、またはiSCSIが設定されたノードがクラスタにある場合、そのクラスタにはSANノードの制限が適用されます。クラスタ内のコントローラに基づくノードの制限については、 _ Hardware Universe _ を参照してください。

手順

1. に進みます "NetApp Hardware Universe"。
2. 左上の*ホーム*の横にある*プラットフォーム*を選択し、プラットフォームタイプを選択します。
3. ONTAPのバージョンを選択します。

   プラットフォームを選択するための新しい列が表示されます。
4. ソリューションで使用するプラットフォームを選択します。
5. [Choose Your Specifications]*で、[Select All]*の選択を解除します。
6. [Max Nodes per Cluster（NAS/SAN）]*を選択します。
7. [結果を表示（ Show Results ）] をクリックする。

結果

選択したプラットフォームのクラスタあたりの最大ノード数が表示されます。

クラスタでサポートできる**FC**ホストが増えるかどうかを確認する

FC 構成および FC-NVMe 構成では、システムの Initiator-Target Nexus （ ITN ；イニシエータ - ターゲット接続）の数に基づいて、クラスタにホストを追加できるかどうかを判断します。

1 つの ITN は、ホストのイニシエータからストレージシステムのターゲットへの 1 つのパスに該当します。FC 構成および FC-NVMe 構成のノードあたりの最大 ITN 数は 2 、 048 です。ITNの数が上限を下回っている場合は、引き続きクラスタにホストを追加できます。

クラスタで使用されている ITN の数を確認するには、クラスタの各ノードで次の手順を実行します。

手順

1. ノードの LIF をすべて特定します。
2. ノードのすべてのLIFに対して次のコマンドを実行します。

```
fcp initiator show -fields wwpn, lif
```

   コマンド出力の一番下に表示されたエントリ数が、その LIF の ITN 数です。

3. それぞれの LIF について、表示された ITN 数を記録します。
4. クラスタのすべてのノードの各 LIF の ITN 数を合計します。

   この値がクラスタの ITN の総数になります。

クラスタでサポートできる**iSCSI**ホストが増えるかどうかを確認する

ノードに直接または 1 つ以上のスイッチを介して接続できるホストの数は、使用可能なイーサネットポートの数で決まります。使用可能なイーサネットポートの数は、コントローラのモデル、およびコントローラにインストールされているアダプタの数とタイプによって決まります。コントローラおよびアダプタでサポートされるイーサネットポートの数は、 _ Hardware Universe _ で確認できます。

マルチノードクラスタ構成の場合は、ノードあたりの iSCSI セッションの数に基づいて、クラスタにホストを追加できるかどうかを判断する必要があります。ノードあたりの iSCSI セッションの最大数をクラスタが下回っている場合は、引き続きクラスタにホストを追加できます。ノードあたりの iSCSI セッションの最大数は、クラスタ内のコントローラのタイプによって異なります。

手順

1. ノードのターゲットポータルグループをすべて特定します。
2. ノードのすべてのターゲットポータルグループについて、それぞれ iSCSI セッションの数を確認します。

```
iscsi session show -tpgroup _tpgroup_
```

   コマンド出力の一番下に表示されたエントリ数が、そのターゲットポータルグループの iSCSI セッション数です。

3. 各ターゲットポータルグループについて、表示された iSCSI セッション数を記録します。
4. ノードの各ターゲットポータルグループの iSCSI セッション数を追加します。

   この値がノードの iSCSI セッションの総数になります。

オールフラッシュ**SAN**アレイ構成の制限とサポート

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

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

これらの制限は ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "ASA R2システムのストレージ制限" 。

SANプロトコルとサポートされるクラスタあたりのノード数

サポートされるSANプロトコルとクラスタあたりの最大ノード数は、MetroCluster以外の構成とMetroCluster構成のどちらを使用しているかによって異なります。

MetroCluster以外の構成

次の表は、MetroCluster以外の構成での、ASAでサポートされるSANプロトコルとクラスタあたりのノード数をまとめたものです。

ONTAPバージョン	プロトコルのサポート	クラスタあたりの最大ノード数
9.11.1	• NVMe / TCP • NVMe/FC	12
9.10.1	• NVMe / TCP	2
9.9.1	• NVMe/FC	2
	• FC • iSCSI	12
9.7	• FC • iSCSI	2

MetroCluster IP構成

次の表は、MetroCluster IP構成での、ASAでサポートされるSANプロトコルとクラスタあたりのノード数をまとめたものです。

ONTAPバージョン	プロトコルのサポート	クラスタあたりの最大ノード数
9.15.1	• NVMe / TCP	4ノードMetroCluster IP構成ではクラスタあたり2ノード
9.12.1	• NVMe/FC	4ノードMetroCluster IP構成ではクラスタあたり2ノード
9.9.1	• FC • iSCSI	8ノードMetroCluster IP構成ではクラスタあたり4ノード
9.7	• FC • iSCSI	4ノードMetroCluster IP構成ではクラスタあたり2ノード

永続ポートのサポート

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

永続ポートは、ハイアベイラビリティ（HA）パートナーの対応する物理ポートにシャドウLIFを作成することで、テイクオーバーの影響を軽減します。ノードがテイクオーバーされると、パートナー ノードのシャドウLIFにWWPNなどの元のLIFの識別情報が引き継がれます。テイクオーバーされたノードへのパスのステータスが「障害」に変更される前に、シャドウLIFがホストのMPIOスタックへのアクティブな最適パスとして表示され、I/Oが移行されます。これにより、ストレージ フェイルオーバー処理の実行中も含めてホストが認識するターゲットへのパス数は変わらないため、I/Oの中断が軽減されます。

永続ポートについては、FCPポートの次の特性がHAペア間で同じでなければなりません。

- FCPポートの数
- FCPポートの名前
- FCPポートの速度
- FCP LIFのWWPNベースのゾーニング

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

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

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

ONTAPシステムで使用するFCスイッチの構成の制限

ファイバチャネルスイッチには、ポート、ポートグループ、ブレード、およびスイッチごとにサポートされるログイン数など、最大構成制限があります。サポートされる制限については、スイッチベンダーのドキュメントを参照してください。

各FC論理インターフェイス（LIF）がFCスイッチポートにログインします。ノード上の1つのターゲットからのログインの総数は、LIFの数に、基盤となる物理ポートへのログイン数1を足した数です。スイッチベンダーが設定しているログインやその他の設定値の制限を超えないようにしてください。これは、NPIVが有効な仮想環境でホスト側で使用されているイニシエータにも当てはまります。ソリューションで使用しているターゲットまたはイニシエータのログインに関して、スイッチベンダーが設定している制限を超えないようにしてください。

Brocadeスイッチの最大数

Brocade スイッチの最大構成数は、 _Brocade 拡張性ガイドライン _ で確認できます。

Ciscoシステムのスイッチ制限

Ciscoスイッチの構成の制限については、使用しているバージョンのCiscoスイッチソフトウェアのガイドを参照して "Cisco設定の制限"ください。

ONTAPでサポートされるFCおよびFCoEの最大ホップ数

ホップ数は、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチの数として定義されます。ホストとストレージシステムの間でサポートされるFCの最大ホップ数は、スイッチベンダーによって異なります。

Cisco Systems のマニュアルでは、この値のことを「 SAN fabric_ の直径」とも呼んでいます。

FCoEでは、FCoEスイッチをFCスイッチに接続できます。エンドツーエンドのFCoE接続では、イーサネットInter-Switch Link（ISL；スイッチ間リンク）に対応するバージョンのファームウェアがFCoEスイッチで実行されている必要があります。

スイッチベンダー	サポートされるホップ数
Brocade	• FCの場合は7 • FCoEの場合は5
Cisco	• FCの場合は7 • 最大3つのスイッチをFCoEスイッチにすることができます。

ONTAP FCホストのキュー深度の計算

ノードおよびFCポートのファンインあたりのITN数を最大にするために、ホストのFCキュー深度の調整が必要になる場合があります。LUNの最大数と1つのFCポートに接続できるHBAの数は、FCターゲット ポートで使用可能なキューの深度によって制限されます。

タスクの内容

キュー深度は、ストレージコントローラで一度にキューに格納できるI/O要求（SCSIコマンド）の数です。ホストのイニシエータHBAからストレージコントローラのターゲットアダプタへのI/O要求ごとに、キューエントリが1つ作成されます。通常、キュー深度が大きいほどパフォーマンスは向上します。ただし、ストレージコントローラの最大キュー深度に達すると、ストレージコントローラはQFULL応答を返して受信コマンドを拒否します。QFULL状態が発生するとシステムパフォーマンスが大幅に低下し、一部のシステムでエラーが発生する可能性があるため、1台のストレージコントローラに多数のホストがアクセスしている場合は、QFULLが発生しないように慎重に計画する必要があります。

複数のイニシエータ（ホスト）を含む構成では、すべてのホストでキュー深度を同程度に設定する必要があります。同じターゲットポートを介してストレージコントローラに接続されているホスト間でキュー深度が異なるため、キュー深度が小さいホストは、キュー深度が大きいホストからリソースにアクセスできなくなります。

キュー深度を「チューニング」する場合は、次の一般的な推奨事項を考慮してください。

- 小規模から中規模のシステムでは、HBAキュー深度を32にします。
- 大規模なシステムでは、HBAキュー深度を128にします。
- 例外的なケースやパフォーマンステストでは、キュー深度を256にして、キューの問題の可能性を回避します。

- すべてのホストに均等にアクセスできるようにするには、すべてのホストのキュー深度を同じ値に設定する必要があります。
- パフォーマンスの低下やエラーを回避するために、ストレージコントローラのターゲットFCポートのキュー深度を超えないようにする必要があります。

手順

1. 1つのFCターゲットポートに接続しているすべてのホストのFCイニシエータの総数を数えます。
2. 128を掛けます。
   - 2 、 048 より小さい場合は、すべてのイニシエータのキュー深度を 128 に設定します。15台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。15 × 128 = 1 、 920 。これは合計最大キュー深度の 2 、 048 より少ないため、すべてのイニシエータのキュー深度を 128 に設定できます。
   - この値が 2 、 048 よりも大きい場合は、手順 3 に進みます。30台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。30 × 128 = 3 、 840 。これは合計最大キュー深度の 2 、 048 より大きいため、手順 3 に記載されているいずれかのオプションを実行して調整します。
3. 次のいずれかのオプションを選択して、ストレージコントローラにホストを追加します。
   - オプション1：
     i. FCターゲットポートを追加します。
     ii. FCイニシエータを再配置します。
     iii. 手順1と2を繰り返します。+ 必要なキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。これを解決するには、各コントローラに2ポートのFCターゲットアダプタを追加し、30台のホストのうち15台を1つのポートセットに接続し、残りの15台を2つ目のポートセットに接続するようにFCスイッチをゾーニングし直します。これで、ポートあたりのキュー深度は 15 × 128 = 1 、 920 となります。
   - オプション2：
     i. 各ホストを「ラージ」または「モール」として指定します。これは、予想される I/O ニーズに基づいています。
     ii. 大規模イニシエータの数に128を掛けます。
     iii. 小規模イニシエータの数に32を掛けます。
     iv. 2つの結果を足し合わせます。
     v. 2 、 048 より小さい場合は、大規模ホストのキュー深度を 128 に、小規模ホストのキュー深度を 32 に設定します。
     vi. 2 、 048 よりも大きい場合は、合計キュー深度が 2 、 048 以下になるまで各イニシエータのキュー深度を下げます。

> ⓘ 特定の1秒あたりのI/Oスループットを達成するために必要なキュー深度を見積もるには、次の式を使用します。
>
> 必要なキュー深度=（1秒あたりのI/O数）×（応答時間）
>
> たとえば、応答時間 3 ミリ秒で 40 、 000 IOPS のスループットに必要なキュー深度は、 40 、 000 × （ .003 ） = 120 です。

基本的な推奨構成に従ってキュー深度を32に制限した場合、ターゲットポートに接続できるホストの最大数は64です。ただし、キュー深度を128にすると、1つのターゲットポートに接続できるホストの最大数は16になります。キュー深度が大きいほど、1つのターゲットポートでサポートできるホストの数が少なくなります。キュー深度を妥協できないような要件の場合は、追加のターゲットポートを用意する必要があります。

必要とされるキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。ストレージ I/O のニーズが高い「大規模」ホストが 10 台あり、 I/O のニーズが低い「モール」ホストが 20 台あります。大規模ホストのイニシエータのキュー深度を128に、小規模ホストのイニシエータのキュー深度を32に設定します。

その結果、合計キュー深度は（ 10 × 128 ） + （ 20 × 32 ） = 1 、 920 になります。

使用可能なキュー深度を、各イニシエータに均等に分配できます。

そのため、イニシエータあたりのキュー深度は 2 、 048 ÷ 30 = 68 となります。

ONTAP SANホストのキュー深度を変更する

ノードあたりおよびFCポートのファンインあたりのITN数を最大にするために、ホストのキュー深度の変更が必要になる場合があります。環境に応じて変更できます。"最適なキュー深度の計算"

AIX ホスト

AIXホストのキュー深度は、コマンドを使用して変更できます `chdev`。コマンドを使用して行った変更 `chdev`はリブート後も維持されます。

例：

- hdisk7デバイスのキュー深度を変更するには、次のコマンドを使用します。

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- fcs0 HBAのキュー深度を変更するには、次のコマンドを使用します。

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  のデフォルト値 `num_cmd_elems`は200です。最大値は2、048です。

  > ⓘ 場合によっては、コマンドと `makdev -l fcs0 -P`コマンドを使用してHBAをオフラインにして変更後にオンラインに戻し `rmdev -l fcs0 -R`なければならないことがあり `num_cmd_elems`ます。

HP-UX ホスト

HP-UXホストのLUNまたはデバイスのキュー深度は、kernelパラメータを使用して変更できます `scsi_max_qdepth`。HBAのキュー深度は、カーネルパラメータを使用して変更できます `max_fcp_reqs`。

- のデフォルト値 `scsi_max_qdepth`は8です。最大値は255です。

  `scsi_max_qdepth`コマンドのオプションを `kmtune`使用すると、実行中のシステムで動的に変更で

きます `-u`。この変更は、システム上のすべてのデバイスに有効になります。たとえば、LUNのキュー深度を64に増やすには、次のコマンドを使用します。

```
kmtune -u -s scsi_max_qdepth=64
```

コマンドを使用すると、個 々 のデバイスファイルのキュー深度を変更でき `scsictl`ます。コマンドを使用した変更 `scsictl`は、システムのリブート後は維持されません。特定のデバイスファイルのキュー深度を表示および変更するには、次のコマンドを実行します。

```
scsictl -a /dev/rdsk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
```

- のデフォルト値 `max_fcp_reqs`は512です。最大値は1024です。

  変更を有効にするには、カーネルを再構築し、システムを再起動する必要があり `max_fcp_reqs`ます。たとえば、HBAのキュー深度を256に変更するには、次のコマンドを使用します。

```
kmtune -u -s max_fcp_reqs=256
```

Solaris ホストの場合

SolarisホストのLUNおよびHBAのキュー深度を設定できます。

- LUN のキュー深度の場合：ホストで使用中の LUN の数に LUN あたりのスロットル（ lun-queue-depth ）をかけた値が、ホストの tgt-queue-depth の値以下になる必要があります。
- Sunスタックのキュー深度の場合：標準ドライバでは、LUN単位またはターゲット単位でHBAレベルを設定することはできません `max_throttle`。ネイティブドライバの値は、ファイルおよび `/kernel/drv/ssd.conf`ファイルのデバイスタイプ（`VID_PID`）単位で設定することを `/kernel/drv/sd.conf`推奨します `max_throttle`。ホストユーティリティでは、この値がMPxIO構成では64、Veritas DMP構成では8に設定されます。

手順

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. 検索対象 `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   デフォルト値はインストール時に32に設定されます。

4. 環境の構成に基づいて、必要な値を設定します。
5. ファイルを保存します。
6. コマンドを使用してホストをリブートし `sync; sync; sync; reboot -- -r`ます。

QLogicHBAヨウノVMwareホスト

HBAタイムアウト設定を変更するには、コマンドを使用し `esxcfg-module`ます。ファイルを手動で更新すること `esx.conf`は推奨されません。

手順

1. rootユーザとしてサービスコンソールにログオンします。
2. コマンドを使用し `#vmkload_mod -l`て、現在ロードされているQlogic HBAモジュールを確認します。
3. Qlogic HBAの単一インスタンスの場合は、次のコマンドを実行します。

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

この例では、qla2300_707モジュールを使用しています。の出力に基づいて、適切なモジュールを使用し `vmkload_mod -l`ます。

4. 次のコマンドを使用して変更を保存します。

```
#/usr/sbin/esxcfg-boot -b
```

5. 次のコマンドを使用してサーバをリブートします。

```
#reboot
```

6. 次のコマンドを使用して変更を確認します。
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Emulex HBAヨウノVMwareホスト

HBAタイムアウト設定を変更するには、コマンドを使用し `esxcfg-module`ます。ファイルを手動で更新すること `esx.conf`は推奨されません。

手順

1. rootユーザとしてサービスコンソールにログオンします。
2. コマンドを使用し `#vmkload_mod -l grep lpfc`て、どのEmulex HBAが現在ロードされているかを確認します。
3. Emulex HBAの単一インスタンスの場合は、次のコマンドを入力します。

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

HBAのモデルに応じて、モジュールはlpfcdd_7xxまたはlpfcdd_732のいずれかになります。上記のコマンドはlpfcdd_7xxモジュールを使用します。の結果に基づいて、適切なモジュールを使用する必要があります `vmkload_mod -l`。

このコマンドを実行すると、lpfc0で表されるHBAのLUNキュー深度が16に設定されます。

4. Emulex HBAの複数のインスタンスの場合は、次のコマンドを実行します。

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

lpfc0のLUNキュー深度とlpfc1のLUNキュー深度が16に設定されます。

5. 次のコマンドを入力します。

   ```
   #esxcfg-boot -b
   ```

6. を使用してリブートします `#reboot`

Emulex HBAヨウノWindowsホスト

Windowsホストでは、ユーティリティを使用してEmulex HBAのキュー深度を更新できます `LPUTILNT`。

手順

1. ディレクトリにあるユーティリティを `C:\WINNT\system32`実行し `LPUTILNT`ます。
2. 右側のメニューから * Drive Parameters * （ドライブパラメータ）を選択します。
3. スクロールダウンして、 [**QueueDepth**] をダブルクリックします。

> 150 より大きい * QueueDepth * を設定する場合は、次の Windows レジストリ値も適切に増やす必要があります。
>
> ```
> HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
> ```

Qlogic HBA用のWindowsホスト

Windowsホストでは、およびHBAマネージャユーティリティを使用してQlogic HBAのキュー深度を更新できます `SANsurfer`。

手順

1. HBAマネージャユーティリティを実行し `SANsurfer`ます。
2. [* HBA ポート > 設定] をクリックします。
3. リスト・ボックスの * HBA ポートの詳細設定 * をクリックします。
4. パラメータを更新し `Execution Throttle`ます。

Emulex HBAヨウノLinuxホスト

Linux ホストでは Emulex HBA のキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。

手順

1. 変更するキュー深度パラメータを特定します。

   ```
   modinfo lpfc|grep queue_depth
   ```

   キュー深度パラメータとその概要のリストが表示されます。使用しているオペレーティングシステムのバージョンに応じて、次のキュー深度パラメータを 1 つ以上変更できます。

   - `lpfc_lun_queue_depth`：特定のLUNのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_hba_queue_depth`：lpfc HBAのキューに格納できるFCコマンドの最大数（uint）

- `lpfc_tgt_queue_depth`：特定のターゲットポートのキューに格納できるFCコマンドの最大数（uint）

> `lpfc_tgt_queue_depth`パラメータは、`Red Hat Enterprise Linux 7.x`システム、`SUSE Linux Enterprise Server 11 SP4`システム、および`12.x`システムにのみ適用されます。

2. キュー深度を更新するには、Red Hat Enterprise Linux 5.xシステムの場合はファイル、Red Hat Enterprise Linux 6.x / 7.xシステム、またはSUSE Linux Enterprise Server 11.x / 12.xシステムの場合はファイルに、`/etc/modprobe.d/scsi.conf`キュー深度パラメータを追加します `/etc/modprobe.conf`。

   使用しているオペレーティングシステムのバージョンに応じて、次のコマンドを 1 つ以上追加できます。

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

   詳細については、使用しているLinuxオペレーティングシステムのバージョンに対応したを参照してください"システム管理"。

4. 変更したキュー深度パラメータの値が更新されていることを確認します。

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
      30
```

   キュー深度の現在の値が表示されます。

QLogicHBAヨウノLinuxホスト

Linux ホストでは QLogic ドライバのデバイスキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。QLogic HBA のキュー深度を変更するには、 QLogic HBA の管理 GUI またはコマンドラインインターフェイス（ CLI ）を使用します。

このタスクでは、 QLogic HBA の CLI を使用して QLogic HBA のキュー深度を変更する方法を示します

手順

1. 変更するデバイスキュー深度パラメータを特定します。

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

   変更できるのはキュー深度パラメータのみ `ql2xmaxqdepth`です。このパラメータは、LUNごとに設定できる最大キュー深度を示します。RHEL 7.5以降のデフォルト値は64です。RHEL 7.4以前のデフォルト値は32です。

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. デバイスのキュー深度の値を更新します。

   - 永続的に変更する場合は、次の手順を実行します。

     i. キュー深度を更新するには、Red Hat Enterprise Linux 5.xシステムの場合はファイルに、`/etc/modprobe.d/scsi.conf`Red Hat Enterprise Linux 6.x / 7.xシステムまたはSUSE Linux Enterprise Server 11.x / 12.xシステムの場合はファイルに、キュー深度パラメータを追加し `/etc/modprobe.conf`ます。 `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

     詳細については、使用しているLinuxオペレーティングシステムのバージョンに対応したを参照してください"システム管理"。

   - 現在のセッションだけでパラメータを変更する場合は、次のコマンドを実行します。

     `echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

     次の例では、キュー深度を 128 に設定します。

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. キュー深度の値が更新されたことを確認します。

   `cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

   キュー深度の現在の値が表示されます。

4. QLogic HBA BIOSからファームウェアパラメータを更新して、QLogic HBAのキュー深度を変更します `Execution Throttle`。

   a. QLogic HBA管理CLIにログインします。

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. メインメニューからオプションを選択します `Adapter Configuration`。

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

c. アダプタ設定パラメータのリストから、オプションを選択し `HBA Parameters`ます。

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. HBA ポートのリストから、必要な HBA ポートを選択します。

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

HBA ポートの詳細が表示されます。

e. [HBA Parameters]メニューで、オプションの現在の値を表示するオプションを `Execution Throttle`選択します `Display HBA Parameters。

このオプションのデフォルト値 `Execution Throttle`は65535です。

```
HBA Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
--------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```
--------------------------------------------------------------------------------
Connection Options              : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                       : Auto
Frame Size                      : 2048
Hard Loop ID                    : 0
Loop Reset Delay (seconds)      : 5
Enable Host HBA BIOS            : Enabled
Enable Hard Loop ID             : Disabled
Enable FC Tape Support          : Enabled
Operation Mode                  : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)   : 0
**Execution Throttle              : 65535**
Login Retry Count               : 8
Port Down Retry Count           : 30
Enable LIP Full Login           : Enabled
Link Down Timeout (seconds)     : 30
Enable Target Reset             : Enabled
LUNs Per Target                 : 128
Out Of Order Frame Assembly     : Disabled
Enable LR Ext. Credits          : Disabled
Enable Fabric Assigned WWN      : N/A

Press <Enter> to continue:
```

a. Enter * を押して続行します。

b. [HBA Parameters]メニューから、HBAパラメータを変更するオプションを選択します `Configure HBA Parameters`。

c. [Configure Parameters]メニューからオプションを選択し `Execute Throttle`、このパラメータの値を更新します。

```
Configure Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Enter * を押して続行します。

e. [Configure Parameters]メニューから、変更を保存するオプションを選択し `Commit Changes`ます。

f. メニューを終了します。

S3オブジェクトストレージの管理

ONTAP 9でのS3サポートの詳細

ONTAP S3設定の詳細

ONTAP 9 .8以降では、ONTAPクラスタでONTAP Simple Storage Service（S3）オブジェクトストレージサーバを有効にすることができます。ONTAP System Managerなどの使い慣れた管理ツールを使用して、ONTAPの開発と運用用にハイパフォーマンスなオブジェクトストレージを迅速にプロビジョニングし、ONTAPのStorage Efficiencyとセキュリティを活用できます。

2024年7月以降、これまでPDFとして公開されていたテクニカルレポートの内容がONTAPの製品ドキュメントに統合されました。ONTAP S3のドキュメントに、ONTAPのベストプラクティス_の_TR-4814：S3のコンテンツが追加されました。

System ManagerおよびONTAP CLIを使用したS3の設定

ONTAP S3は、System ManagerおよびONTAP CLIを使用して設定および管理できます。System Managerを使用してS3を有効にしてバケットを作成すると、ONTAPでは設定を簡易化するためにベストプラクティスのデフォルトが選択されます。設定パラメータを指定する必要がある場合は、ONTAP CLIを使用できます。CLIからS3サーバとバケットを設定した場合でも、必要に応じてSystem Managerで管理できます。その逆も可能です。

System Managerを使用してS3バケットを作成すると、ONTAPによってデフォルトのパフォーマンスサービスレベルがシステムで使用可能な最も高いレベルに設定されます。たとえば、 AFF システムでは、デフォルト設定は * Extreme * になります。パフォーマンスサービスレベルは、事前に定義されたアダプティブQoSポリシーグループです。デフォルトのいずれかのサービスレベルの代わりに、カスタムのQoSポリシーグループを指定することも、ポリシーグループを指定しないこともできます。

事前定義されたアダプティブQoSポリシーグループは次のとおりです。

- * Extreme * ：最高レベルのレイテンシと最高レベルのパフォーマンスを求められるアプリケーションに使用されます。
- * パフォーマンス * ：適度なパフォーマンスとレイテンシが求められるアプリケーションに使用します。
- * Value * ：スループットと容量がレイテンシよりも重視されるアプリケーションに使用します。
- * カスタム * ：カスタムの QoS ポリシーを指定するか、 QoS ポリシーなしで指定します。

[階層化に使用する *] を選択した場合、パフォーマンスサービスレベルは選択されず、階層化データに最適なパフォーマンスを備えた低コストのメディアを選択しようとします。

も参照してください"アダプティブQoSポリシーグループを使用する"。

ONTAPは、選択したサービスレベルを満たす最も適切なディスクを使用するローカル階層にこのバケットをプロビジョニングしようとします。ただし、バケットに含めるディスクを指定する必要がある場合は、CLIからローカル階層（アグリゲート）を指定してS3オブジェクトストレージを設定することを検討してください。CLIからS3サーバを設定した場合も、必要に応じてSystem Managerで管理できます。

バケットに使用するアグリゲートを指定できるようにするには、CLIを使用する必要があります。

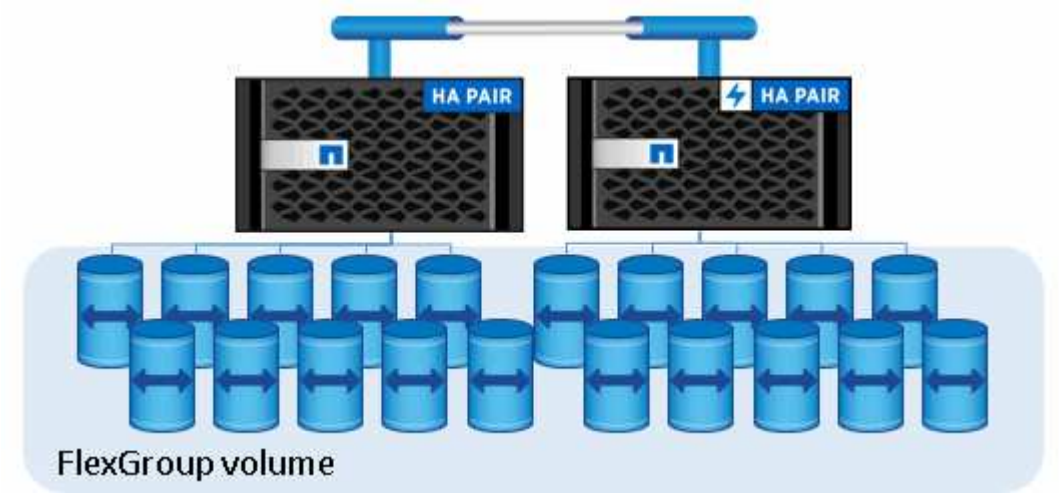
Cloud Volumes ONTAPでのS3バケットの設定

Cloud Volumes ONTAPからバケットを提供する場合は、使用するアグリゲートが1つのノードだけになるように、基盤となるアグリゲートを手動で選択することを強く推奨します。両方のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を与える可能性があります。そのため、Cloud Volumes ONTAP環境ではを推奨しCLIからS3バケットを設定するます。

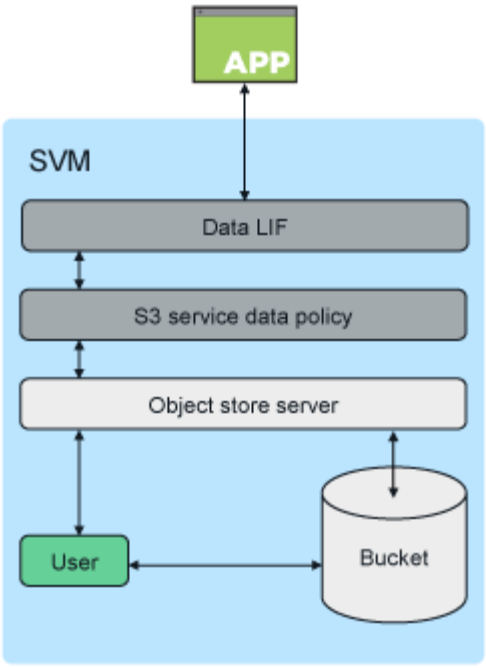
それ以外の場合、Cloud Volumes ONTAP上のS3サーバは、Cloud Volumes ONTAPでオンプレミス環境と同じように設定および維持されます。

FlexGroupボリュームを使用したONTAP S3アーキテクチャ

ONTAPのバケットの基盤となるアーキテクチャはです。は、複数のコンスティチュエントメンバーボリュームで構成される "FlexGroupボリューム"単一のネームスペースですが、単一のボリュームとして管理されます。



バケットへのアクセスは、許可されたユーザとクライアントアプリケーションを通じて提供されます。



バケットがFabricPoolエンドポイントなどのS3アプリケーション専用に使用されている場合、基盤となるFlexGroupボリュームではS3プロトコルのみがサポートされます。

ONTAP 9.12.1以降では、NASプロトコルを使用するように事前設定されたでS3プロトコルを有効にすることもできます"マルチプロトコルNASボリューム"。マルチプロトコルNASボリュームでS3プロトコルが有効になっている場合、クライアントアプリケーションはNFS、SMB、およびS3を使用してデータの読み取りと書き込みを行うことができます。

バケット制限

最小バケットサイズは95GBです。+最大バケットサイズは、FlexGroupの最大サイズである60PBに制限されています。

FlexGroupボリュームあたり1、000バケット、またはクラスタあたり12、000バケット（12個のFlexGroupボリュームを使用）の制限があります。

ONTAP 9.14.1以降での**FlexGroup**の自動サイジング

ONTAP 9.14.1以降では、デフォルトのFlexGroupサイズは格納されるバケットのサイズに基づいて決まります。FlexGroupボリュームは、バケットが追加または削除されると自動的に拡張または縮小されます。

たとえば、初期のBucket_Aが100GBにプロビジョニングされている場合、FlexGroupは100GBにシンプロビジョニングされます。Bucket_B（300GB）とBucket_C（500GB）の2つのバケットを追加で作成すると、FlexGroupボリュームは900GBに拡張されます。

（100GBのBucket_A、300GBのBucket_B、500GBのBucket_C = 900GB）

Bucket_Aを削除すると、基盤となるFlexGroupボリュームは800GBに縮小されます。

ONTAP 9.13.1以前で修正されたデフォルトの**FlexGroup**サイズ

バケットの拡張用の容量を確保するには、FlexGroupボリュームのすべてのバケットの合計使用済み容量が、クラスタ上の使用可能なストレージアグリゲートに基づくFlexGroupの最大容量の33%未満である必要があります。この要件を満たすことができない場合、作成される新しいバケットは、自動的に作成される新しいFlexGroupボリュームにプロビジョニングされます。

ONTAP 9.14.1より前のバージョンでは、FlexGroupサイズは環境に基づいてデフォルトサイズに固定されていました。

- 1.6PB（ONTAP）
- ONTAP Selectで100TB

FlexGroupボリュームをデフォルトサイズでプロビジョニングするための十分な容量がクラスタにない場合、ONTAPは既存の環境でプロビジョニングできるようになるまでデフォルトサイズを半分に縮小します。

たとえば、300TBの環境では、200TBのFlexGroupボリュームが自動的にプロビジョニングされます（1.6PB、800TB、400TBのFlexGroupボリュームは、環境にしては大きすぎます）。

ONTAP S3の主なユースケース

ONTAP S3サービスへのクライアントアクセスの主なユースケースは次のとおりです。

- FabricPoolを使用してアクセス頻度の低いデータをONTAPのバケットに階層化することで、ONTAPからONTAPへの階層化が可能になります。内のバケットへの階層化、または上のバケットへの階層化 "ローカルクラスタ"の "リモートクラスタ"両方がサポートされます。ONTAP S3への階層化により、使用頻度の低いデータに低コストのONTAPシステムを使用し、新しいフラッシュ容量にかかるコストを削減できます。追加のFabricPoolライセンスや新しいテクノロジを管理する必要はありません。
- ONTAP 9.12.1以降では、NASプロトコルを使用するように事前設定されたでS3プロトコルを有効にすることもできます"マルチプロトコルNASボリューム"。マルチプロトコルNASボリュームでS3プロトコルを有効にすると、クライアントアプリケーションはS3、NFS、およびSMBを使用してデータの読み取りと書き込みを行うことができるため、さまざまなユースケースが開かれます。最も一般的なユースケースの1つは、NASクライアントがボリュームにデータを書き込み、S3クライアントが同じデータを読み取り、分析、ビジネスインテリジェンス、機械学習、光学式文字認識などの特殊なタスクを実行することです。

> ONTAP S3は、既存のONTAPクラスタで追加のハードウェアや管理作業を行わずにS3機能を有効にする場合に適しています。NetApp StorageGRIDは、NetAppのオブジェクトストレージ向け主力ソリューションです。StorageGRIDは、S3のあらゆる操作、高度なILM機能、またはONTAPベースのシステムでは達成できない容量を活用する必要があるネイティブのS3アプリケーションに推奨されます。詳細については、を参照して"StorageGRID のドキュメント"ください。

関連情報

"FlexGroupホリユウムノカンリ"

計画

ONTAPのバージョンとプラットフォームでS3オブジェクトストレージをサポート

S3オブジェクトストレージは、ONTAP 9.8以降を使用するすべてのAFF、FAS、ONTAP Selectプラットフォームでサポートされます。

FC、iSCSI、NFS、NVMe_oF、SMBなどの他のプロトコルと同様に、 S3をONTAPで使用するには、ライセンスをインストールする必要があります。S3ライセンスはゼロコストライセンスですが、ONTAP 9.8にアップグレードするシステムにインストールする必要があります。S3ライセンスは、NetAppサポートサイトのからダウンロードできます "マスターライセンスキーページ" 。

新しいONTAP 9.8以降のシステムにはS3ライセンスがプリインストールされています。

Cloud Volumes ONTAP

ONTAP S3は、Cloud Volumes ONTAPでオンプレミス環境と同じように設定および機能しますが、例外が1つあります。

- Cloud Volumes ONTAPでバケットを作成する場合は、CLIの手順を使用して、基盤となるFlexGroupボリュームが単一ノードのアグリゲートのみを使用するようにしてください。複数のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響します。

クラウドプロバイダ	ONTAPバージョン
Google Cloud	ONTAP 9.12.1以降
AWS	ONTAP 9.11.0以降
Azure	ONTAP 9.9.1以降

NetApp ONTAP 対応の Amazon FSX

S3オブジェクトストレージは、ONTAP 9.11以降を使用するAmazon FSx for NetAppサービスでサポートされます。

MetroClusterによるS3のサポート

ONTAP 9 .14.1以降では、MetroCluster IP構成およびFC構成で、ミラーされたアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にすることができます。

ONTAP 9 12.1以降では、MetroCluster IP構成のミラーされていないアグリゲートにあるSVMでS3オブジェクトストレージサーバを有効にできます。MetroCluster IP構成でのミラーされていないアグリゲートの制限事項の詳細については、を参照してください"ミラーされていないアグリゲートに関する考慮事項"。

SnapMirror S3はMetroCluster構成ではサポートされません。

ONTAP 9 .7でのS3のパブリックプレビュー

ONTAP 9.7では、S3オブジェクトストレージがパブリックプレビューとして導入されました。このバージョンは本番環境向けではなく、ONTAP 9.8以降では更新されません。本番環境でS3オブジェクトストレージをサポートするのは、ONTAP 9.8以降のリリースのみです。

9.7のパブリックプレビューで作成されたS3バケットは、ONTAP 9 .8以降で使用できますが、強化された機能

は利用できません。9.7のパブリックプレビューで作成したバケットがある場合は、機能サポート、セキュリティ、パフォーマンスを強化するために、バケットの内容を9.8のバケットに移行する必要があります。

ONTAP S3でサポートされる操作

ONTAP S3の操作は、以下に示す以外は標準のS3 REST APIでサポートされます。詳細については、を参照して"Amazon S3 APIリファレンス』を参照してください"ください。

> これらのS3アクションは、特にONTAPでネイティブのS3バケットを使用する場合にサポートされます。バージョン管理、オブジェクトロック、その他の機能に関連付けられたアクションなど、これらのアクションの一部は、を使用している場合はサポートされません"S3 NASバケット（マルチプロトコルNASボリューム内のS3）"。

特定の操作について明記されていない限り、 ONTAP 9.8 以降では次の共通要求ヘッダーがサポートされます。

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

バケットの処理

AWS S3 APIを使用するONTAPでサポートされる処理は次のとおりです。

バケットの処理	**ONTAP**でのサポート開始
CreateBucket ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `x-amz-bucket-object-lock-enabled`	ONTAP 9 .11.1
DeleteBucket ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .11.1

バケットの処理	**ONTAP**でのサポート開始
DeleteBucketCors ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
DeleteBucketLifecycle ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
DeleteBucketPolicy ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 12.1
GetBucketAcl ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
GetBucketCors ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
GetBucketLifecycleConfiguration ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .13.1 *有効期限アクションのみがサポートされています
GetBucketLocation ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 10.1
GetBucketPolicy ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 12.1
GetBucketVersioning ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .11.1
HeadBucket ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
ListAllMyBuckets ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
ListBuckets ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
ListBucketVersions ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .11.1
PutBucket	• ONTAP 9 .11.1 • ONTAP 9.8 - ONTAP REST APIのみでサポート

バケットの処理	**ONTAP**でのサポート開始
PutBucketCors ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
PutBucketLifecycleConfiguration ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.13.1 * 有効期限アクションのみがサポートされています
PutBucketPolicy ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 12.1
PutBucketVersioning ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .11.1

オブジェクトの処理

ONTAP 9.9.1以降では、ONTAP S3でオブジェクト メタデータとタグ付けがサポートされます。

- PutObjectとCreateMultipartUploadには、 `x-amz-meta-<key>`.

  例： `x-amz-meta-project: ontap_s3`。

- GetObjectとHeadObjectは、ユーザ定義のメタデータを返します。
- メタデータと違って、タグは次の処理でオブジェクトとは別に読み取ることができます。
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

ONTAP 9 .11.1以降では、ONTAP S3でオブジェクトのバージョン管理と次のONTAP APIによる関連操作がサポートされます。

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

特定の操作について明記されていない限り、次の URI クエリ パラメータがサポートされます。

- `versionId`（ ONTAP 9.12.1以降のオブジェクト操作に必要なため）

オブジェクトの処理	**ONTAP**でのサポート開始
AbortMultipartUpload ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI クエリ パラメータをサポートしています。 `uploadId`	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
CompleteMultipartUpload ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI クエリ パラメータをサポートしています。 `uploadId`	ONTAP 9.8
CopyObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-metadata-directive` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-tagging` • `x-amz-tagging-directive` • `x-amz-meta-<metadata-name>`	ONTAP 9 12.1

オブジェクトの処理	**ONTAP**でのサポート開始
CreateMultipartUpload ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
deleteObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `x-amz-bypass-governance-retention`	ONTAP 9.8
DeleteObjects ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています: * `x-amz-bypass-governance-retention`	ONTAP 9 .11.1
DeleteObjectTagging ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .9.1

オブジェクトの処理	**ONTAP**でのサポート開始
GetObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI クエリ パラメータをサポートしています。 • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` そして、この追加のリクエスト ヘッダー: • 範囲	ONTAP 9.8
GetObjectAcl ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
オブジェクト属性の取得 ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .14.1
GetObjectTagging ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .9.1
HeadObject ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
ListMultipartUpload ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています。 • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9.8
ListObjects ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています。 • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9.8
ListObjectsV2 ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています。 • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
ListObjectVersions ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています。 • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9 .11.1
ListParts ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています。 • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9.8
PutObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
PutObjectLockConfiguration ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .14.1
PutObjectRetention ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています。 • `x-amz-bypass-governance-retention`	ONTAP 9 .14.1
PutObjectTagging ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9 .9.1
パーツのアップロード	ONTAP 9.8
パーツコピーをアップロード ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています。 • `partNumber` • `uploadId` さらに次の追加のリクエスト ヘッダーがあります。 • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9 12.1

グループポリシー

これらの処理はS3に固有の処理ではなく、一般にIdentity and Management（IAM）プロセスに関連しています。ONTAPはこれらのコマンドをサポートしていますが、IAM REST APIは使用しません。

- ポリシーの作成
- AttachGroupポリシー

ユーザ管理

以下の処理はS3に固有のものではなく、IAMプロセスに関連する一般的なものです。

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

リリース別の**S3**操作

ONTAP 9 .14.1

ONTAP 9 .14.1では、S3オブジェクトロックのサポートが追加されました。

リーガルホールド処理（保持期間が定義されていないロック）はサポートされません。

- GetObjectLockConfigurationの略
- GetObjectRetention
- PutObjectLockConfiguration
- PutObjectRetention

ONTAP 9 .13.1

ONTAP 9 .13.1では、バケットライフサイクル管理のサポートが追加されています。

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9 12.1

ONTAP 9 .12.1では、バケットポリシーのサポートとオブジェクトのコピー機能が追加されています。

- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- パーツコピーをアップロード

ONTAP 9 .11.1

ONTAP 9 .11.1では、バージョン管理、事前定義されたURL、チャンクアップロードがサポートされるようになりました。また、S3 APIを使用したバケットの作成や削除など、一般的なS3操作もサポートされるようになりました。

- ONTAP S3は、次の方法でチャンクアップロード署名リクエストをサポートするようになりました。 `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3では、クライアントアプリケーションが事前定義されたURLを使用してオブジェクトを共有したり、他のユーザがユーザクレデンシャルを必要とせずにオブジェクトをアップロードしたりできるようになりました。
- CreateBucket

- DeleteBucket
- GetBucketVersioning
- ListBucketVersions
- PutBucket
- PutBucketVersioning
- オブジェクトの削除
- ListObjectVersions

> 基盤となるFlexGroupは最初のバケットがになるまで作成されないため、外部クライアントがCreateBucketを使用してバケットを作成する前に、ONTAPでバケットを作成する必要があります。

ONTAP 9 10.1

ONTAP 9 .10.1では、SnapMirror S3およびGetBucketLocationのサポートが追加されました。

- GetBucketLocation

ONTAP 9 .9.1

ONTAP 9 .9.1では、ONTAP S3にオブジェクトメタデータのサポートとタグ付けのサポートが追加されました。

- PutObjectとCreateMultipartUploadに、を使用したキーと値のペアが追加されました `x-amz-meta-<key>`。例： `x-amz-meta-project: ontap_s3`。
- GetObjectとHeadObjectがユーザ定義のメタデータを返すようになりました。

タグはバケットでも使用できます。メタデータとは異なり、タグは次のコマンドを使用してオブジェクトから独立して読み取ることができます。

- PutObjectTagging
- GetObjectTagging
- DeleteObjectTagging

ONTAP S3の相互運用性

ONTAP S3サーバは、次の表に記載されている場合を除き、ONTAPの他の機能と正常に連携します。

フィーチャー領域（ **Feature area** ）	サポート対象	サポート対象外
Cloud Volumes ONTAP	• ONTAP 9 .9.1以降のリリースのAzureクライアント • ONTAP 9.11.0以降のリリースのAWSクライアント • ONTAP 9.12.1以降のリリースのGoogle Cloudクライアント	• ONTAP 9.8以前のリリースのクライアントのCloud Volumes ONTAP

フィーチャー領域（ **Feature area** ）	サポート対象	サポート対象外
データ保護	• Cloud Sync • オブジェクトロック、ガバナンスとコンプライアンス（ONTAP 9.14.1以降） • "オブジェクトのバージョン管理"（ONTAP 9.11.1以降） • ミラーされていないMetroClusterアグリゲート（ONTAP 9.12.1以降） • ミラーされたMetroClusterアグリゲート（ONTAP 9.14.1以降） • "SnapMirror S3"（ONTAP 9.10.1以降） • SnapMirror（NASボリュームのみ、ONTAP 9.12.1以降） • SnapLock（NASボリュームのみ、ONTAP 9.14.1以降）	• イレイジャーコーディング • NDMP • SMTape • SnapMirror （同期および非同期） • SnapMirrorクラウド • SVMディザスタリカバリ • SyncMirror (SyncMirrorミラーアグリゲートは、 ONTAP 9.14.1 以降のMetroCluster構成でサポートされます。SyncMirrorはMetroCluster構成外ではサポートされません。)
暗号化	• NetAppアグリゲート暗号化（NAE） • NetAppボリューム暗号化（NVE） • NetAppストレージ暗号化（NSE） • TLS/SSL	• SLAG
MetroClusterカンキヨウ	-	SnapMirror S3
Storage Efficiency	• 重複排除 • 圧縮 • コンパクション	• アグリゲートレベルの効率（同じアグリゲート上に存在するメンバーはボリューム間の重複排除を利用できますが、異なるアグリゲート上に存在するメンバーは利用できません） • ONTAP S3バケットを含むFlexGroupボリュームのボリューム クローン
Quality of Service（QoS）	• QoSの最大値（上限） • QoSの最小値（下限）	-

フィーチャー領域（ **Feature area** ）	サポート対象	サポート対象外
その他の機能	• "S3イベントの監査" （ONTAP 9.10.1以降） • "バケットライフサイクル管理" （ONTAP 9.13.1以降） • FabricPoolクラウド層 (ネイティブ S3 のみ) • FabricPoolローカル層 (NAS ボリュームのみ)	• FlexCacheホリユウム • FPolicy • qtree • クォータ • FabricPoolクラウド層 (NAS ボリュームのみ) • FabricPoolローカル層 (ネイティブ S3 のみ)

ONTAP で S3 を使用する検証済みのサードパーティ ソリューション

S3 は普遍的な標準であり、これはサポートされているアプリケーションの包括的なリストではなく、各パートナーと協力して検証されたソリューションのリストのみです。探しているソリューションがリストにない場合は、NetApp アカウント担当者にお問い合わせください。

ネイティブ S3 バケットを使用して検証されたサードパーティ ソリューション

- Amazon SageMaker
- Apache Hadoop S3Aクライアント
- Apache Kafka
- アパッチスパーク
- Commvault（V11）
- コンフルエントカフカ
- NetBackup
- レッドハットキー
- Rubrik
- スノーフレーク
- トリノ
- Veeam（V12）

これらのソリューションは、ONTAPのネイティブS3バケットを使用する場合にのみ有効です。バージョン管理、オブジェクトロック、その他の機能に関連するソリューションなど、一部のソリューションは、ONTAPではサポートされません。 "S3 NASバケット（マルチプロトコルNASボリューム内のS3）" 。

設定

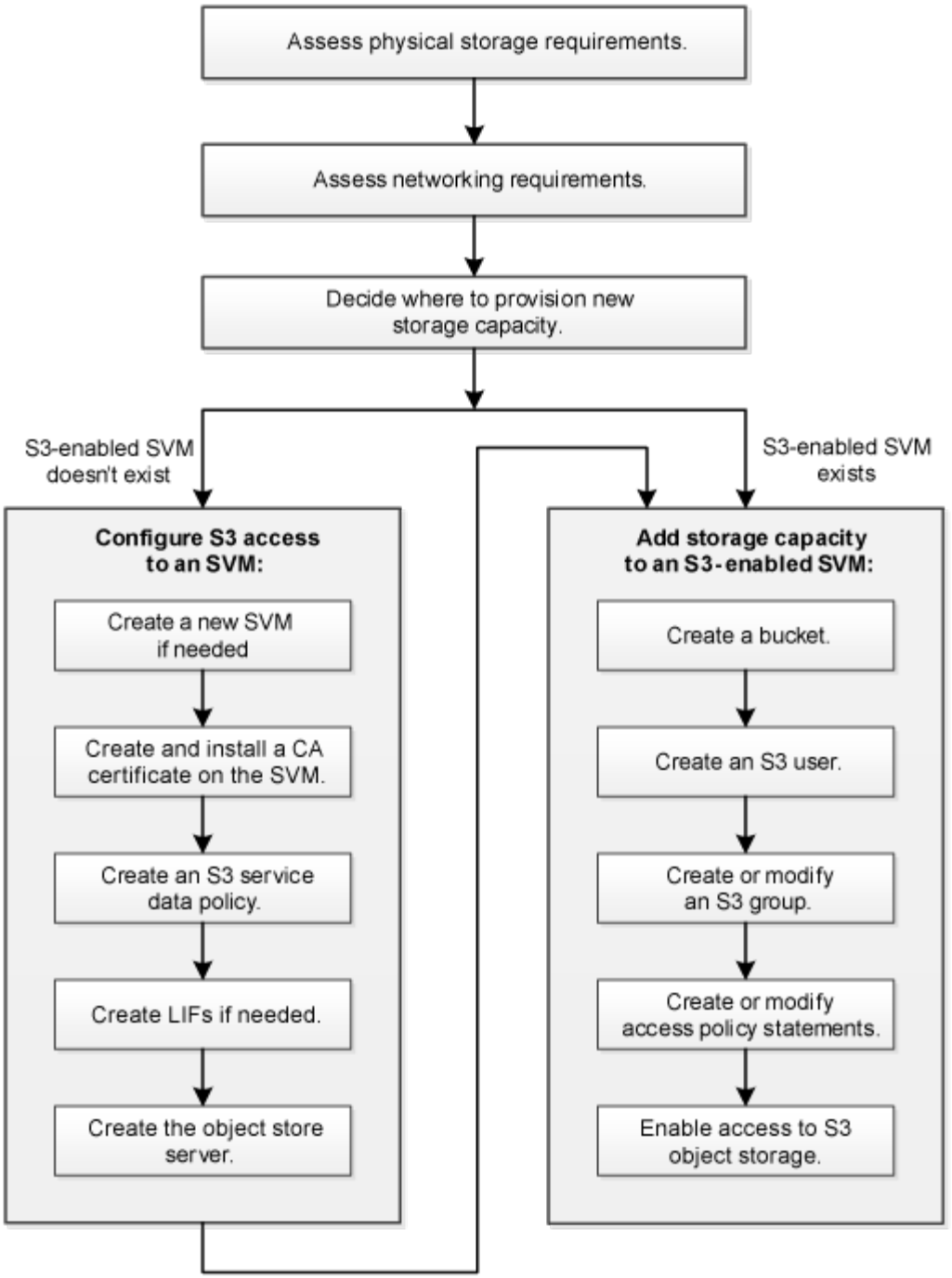
S3の設定プロセスの概要

ONTAP S3の設定ワークフロー

S3を設定するには、物理ストレージとネットワークの要件を評価し、目的に応じたワークフローを選択します。新規または既存のSVMへのS3アクセスを設定するか、すでにS3アクセスの設定が完了している既存のSVMにバケットとユーザを追加するかによってワークフローが異なります。

> クラスターとクライアント間で時間が同期されるようにするには、ネットワーク タイム プロトコル (NTP) 構成が必要です。多くの場合、クライアント アクセスには、 ONTAP S3 オブジェクト ストアとクライアント間の有効なタイムスタンプの差が 15 分以上必要です。"NTPの設定方法について学ぶ" 。

System Managerを使用して新しいStorage VMへのS3アクセスを設定すると、証明書とネットワーク情報を入力するように求められ、1回の処理でStorage VMとS3オブジェクトストレージサーバが作成されます。



ONTAP S3の物理ストレージ要件の評価

クライアントのS3ストレージをプロビジョニングする前に、既存のアグリゲート内に新しいオブジェクトストア用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプと場所で新しいアグリゲートを作成できます。

タスクの内容

S3対応SVMにS3バケットを作成する場合、そのバケットはFlexGroupボリューム "自動作成" でサポートされます。使用するアグリゲートとFlexGroupコンポーネントをONTAP Selectで自動的に選択することも（デフォルト）、使用するアグリゲートとFlexGroupコンポーネントを自分で選択することもできます。

基盤となるディスクのパフォーマンス要件がある場合など、アグリゲートとFlexGroupコンポーネントを指定する場合は、アグリゲートの構成がFlexGroupボリュームのプロビジョニングに関するベストプラクティスガイドラインに準拠していることを確認する必要があります。詳細：

- "FlexGroupホリユウムノカンリ"
- "ネットアップテクニカルレポート 4571-A ：『 NetApp ONTAP FlexGroup Volume Top Best Practices 』"

Cloud Volumes ONTAPからバケットを提供する場合は、使用するアグリゲートが1つのノードだけになるように、基盤となるアグリゲートを手動で選択することを強く推奨します。両方のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を与える可能性があります。詳細はこちらをご覧ください "Cloud Volumes ONTAP 用バケットの作成"。

ONTAP S3サーバを使用して、高パフォーマンス階層と同じクラスタにローカルのFabricPool大容量階層を作成できます。これは、 SSD ディスクが 1 つの HA ペアに接続されている状況で、別の HA ペアの HDD ディスクに階層化 _cold_data を設定する場合などに便利です。このユースケースでは、S3サーバとローカルの大容量階層を含むバケットを高パフォーマンス階層とは別のHAペアに配置する必要があります。ローカル階層化は、1ノードクラスタと2ノードクラスタではサポートされていません。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。

   ```
   storage aggregate show
   ```

   十分なスペースまたは必要なノードの場所を備えたアグリゲートがある場合は、その名前をS3構成用に記録します。

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 十分なスペースや必要なノードの場所を備えたアグリゲートがない場合は、コマンドを使用して既存のアグリゲートにディスクを追加する `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成 `storage aggregate create`します。

関連情報

- "storage aggregate add-disks"
- "storage aggregate create"

ONTAP S3のネットワーク要件の評価

クライアントにS3ストレージを提供する前に、ネットワークが正しく設定されてS3のプロビジョニング要件を満たしていることを確認する必要があります。

開始する前に

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）
- 外部ファイアウォール

タスクの内容

リモートのFabricPool容量（クラウド）階層とリモートS3クライアントの場合は、データSVMを使用し、データLIFを設定する必要があります。FabricPoolクラウド階層の場合は、クラスタ間LIFも設定する必要があります。クラスタピアリングは必要ありません。

ローカル FabricPool の大容量階層には、システム SVM （「 Cluster 」）を使用する必要がありますが、 LIF を設定する方法は 2 つあります。

- クラスタLIFを使用できます。

  このオプションでは、LIFをこれ以上設定する必要はありませんが、クラスタLIFのトラフィックが増加します。また、ローカル階層に他のクラスタからはアクセスできなくなります。

- データLIFとクラスタ間LIFを使用できます。

  このオプションでは、LIFをS3プロトコルに対して有効にするなどの追加の設定が必要ですが、リモートのFabricPoolクラウド階層として他のクラスタからもローカル階層にアクセスできるようになります。

手順

1. 使用可能な物理ポートと仮想ポートを表示します。

   ```
   network port show
   ```

   - 可能な場合は、データネットワークの速度が最も速いポートを使用してください。
   - 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。

2. サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、サブネットが存

在し、十分な数のアドレスが使用可能であることを確認します。

```
network subnet show
```

サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。

の詳細については `network subnet show`、を"ONTAPコマンド リファレンス"参照してください。

3. 使用可能なIPspaceを表示します。

```
network ipspace show
```

デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

4. IPv6アドレスを使用する場合は、IPv6がクラスタで有効になっていることを確認します。

```
network options ipv6 show
```

必要に応じて、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

関連情報

- "network port show"
- "ネットワークオプションIPv6"
- "network ipspace show"
- "ネットワークサブネットの作成"

新しい**ONTAP S3**ストレージ容量のプロビジョニング先を決定する

新しいS3バケットを作成する前に、そのバケットを新規と既存のどちらのSVMに配置するかを決定する必要があります。この決定によって、ワークフローが決まります。

選択肢

- 新しいSVMまたはS3が有効になっていないSVMにバケットをプロビジョニングする場合は、次のトピックの手順を実行します。

  "S3用のSVMの作成"

  "S3用のバケットを作成"

  S3はNFSやSMBを使用するSVMに共存できますが、次のいずれかに該当する場合は新しいSVMを作成します。

  - クラスタでS3を初めて有効にする場合。
  - クラスタ内の既存の SVM で S3 サポートを有効にするのが望ましくない場合。
  - クラスタ内に S3 対応 SVM が 1 つ以上あり、パフォーマンス特性が異なる別の S3 サーバが必要な場合。SVMでS3を有効にしたら、バケットのプロビジョニングに進みます。
- 既存のS3対応SVMに最初のバケットまたは追加のバケットをプロビジョニングする場合は、次のトピッ

クの手順を実行します。

"S3用のバケットを作成"

SVMへのS3アクセスの設定

ONTAP S3用のSVMの作成

S3はSVM内で他のプロトコルと共存できますが、ネームスペースやワークロードを分離するために新しいSVMを作成することもできます。

タスクの内容

SVMからS3オブジェクトストレージのみを提供する場合は、S3サーバにDNS設定は必要ありません。ただし、他のプロトコルを使用する場合は、SVMにDNSを設定することもできます。

System Managerを使用して新しいStorage VMへのS3アクセスを設定すると、証明書とネットワーク情報を入力するように求められ、1回の処理でStorage VMとS3オブジェクトストレージサーバが作成されます。

例 **23.** 手順

System Manager

クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。S3サーバのFQDNの1文字目をバケット名にすることはできません。

インターフェイスロールデータのIPアドレスを入力する準備をしておく必要があります。

外部CA署名証明書を使用している場合は、この手順の実行中に入力するように求められます。また、システムで生成された証明書を使用することもできます。

1. Storage VMでS3を有効にします。

   a. 新しいStorage VMを追加します。[* Storage（ストレージ）]>[Storage VMs]をクリックし、[* Add（追加）]をクリックします。

      既存のStorage VMがない新しいシステムの場合は、*ダッシュボード>プロトコルの設定*をクリックします。

   既存のStorage VMにS3サーバを追加する場合は、**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、 S3 *の下をクリックし ⚙ ます。

   a. Enable S3 * をクリックし、 S3 Server Name を入力します。

   b. 証明書のタイプを選択します。

      システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。

   c. ネットワークインターフェイスを入力します。

2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。

   - 今後シークレットキーは表示されません。
   - 証明書情報が再度必要な場合は、[*ストレージ]、[Storage VMs]の順にクリックし、Storage VMを選択して、[*設定]をクリックします。

CLI

1. クラスタでS3のライセンスが有効になっていることを確認します。

   ```
   system license show -package s3
   ```

   サポートされていない場合は、営業担当者にお問い合わせください。

2. SVMを作成します。

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- オプションにはUNIX設定を使用し `-rootvolume-security-style`ます。
- デフォルトのC.UTF-8オプションを使用し `-language`ます。
- この `ipspace`設定はオプションです。

3. 新しく作成したSVMの設定とステータスを確認します。

```
vserver show -vserver <svm_name>
```

`Vserver Operational State`フィールドには状態が表示されている必要があり `running`ます。状態が表示された場合は `initializing`、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

例

次のコマンドは、データアクセス用のSVMをIPspace ipspaceAに作成します。

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて状態になっていることを示しています running。ルートボリュームには、ルールが含まれていないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。デフォルトでは、vsadminユーザアカウントが作成され、状態がになってい `locked`ます。vsadminロールは、デフォルトのvsadminユーザアカウントに割り当てられます。

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP S3対応**SVM**に**CA**証明書を作成してインストールする

S3 クライアントには、S3 対応 SVM に HTTPS トラフィックを送信するための証明機関 (CA) 証明書が必要です。 CA 証明書は、クライアント アプリケーションとONTAPオブジェクト ストア サーバの間に信頼関係を作成します。 ONTAP をリモート クライアントからアクセス可能なオブジェクト ストアとして使用する前に、 ONTAPに CA 証明書をインストールする必要があります。

タスクの内容

HTTPのみを使用するようにS3サーバを設定したり、CA証明書を必要とせずにクライアントを設定したりすることも可能ですが、ONTAP S3サーバへのHTTPSトラフィックをCA証明書で保護することを推奨します。

IPトラフィックがクラスタLIFのみを経由するローカル階層化では、CA証明書は必要ありません。

この手順では、ONTAP自己署名証明書を作成してインストールします。ONTAPでは自己署名証明書を生成できますが、サードパーティの認証局からの署名済み証明書を使用することを推奨します。詳細については、管理者の認証に関するドキュメントを参照してください。

"カンリシヤニンシヨウトRBAC"

およびその他の設定オプションの詳細については、を"ONTAPコマンド リファレンス"参照して `security certificate`ください。

手順

1. 自己署名デジタル証明書を作成します。

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   オプションは `-type root-ca`、認証局（CA）として機能して他の証明書に署名するための自己署名デジタル証明書を作成してインストールします。

   オプションを使用 `-common-name`すると、SVMの認証局（CA）名が作成され、証明書の完全な名前を生成するときに使用されます。

   デフォルトの証明書サイズは2048ビットです。

   例

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   生成された証明書の名前が表示されたら、以降の手順で使用するために保存しておきます。

   の詳細については `security certificate create`、を"ONTAPコマンド リファレンス"参照してください。

2. 証明書署名要求を生成します。

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   `-common-name`署名要求のパラメータには、S3サーバ名（FQDN）を指定する必要があります。

   必要に応じて、SVMの場所やその他の詳細情報を指定できます。

   その `-dns-name`パラメータは、DNS 名のリストを提供するサブジェクト代替名拡張を指定するためにクライアントによって要求されることがよくあります。

   その `-ipaddr`パラメータは、IP アドレスのリストを提供するサブジェクト代替名拡張を指定するためにクライアントによって要求されることがよくあります。

   あとで参照できるように、証明書要求と秘密鍵のコピーを保管するように求められます。

の詳細については `security certificate generate-csr`、を"ONTAPコマンド リファレンス"参照してください。

3. SVM_CAを使用してCSRに署名し、S3サーバの証明書を生成します。

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   前の手順で使用したコマンドオプションを入力します。

   - `-ca`--ステップ1で入力したCAの共通名。
   - `-ca-serial`--ステップ1のCAシリアル番号。たとえば、CA証明書の名前がsvm1_ca_159D1587CE21E9D4_svm1_caの場合、シリアル番号は159D1587CE21E9D4です。

     デフォルトでは、署名済み証明書の有効期限は365日です。別の値を選択したり、他の署名の詳細を指定したりできます。

     プロンプトが表示されたら、手順2で保存した証明書要求文字列をコピーして入力します。

   署名済み証明書が表示されます。あとで使用できるように保存しておきます。

4. S3対応SVMに署名済み証明書をインストールします。

   `security certificate install -type server -vserver` *`svm_name`*

   プロンプトが表示されたら、証明書と秘密鍵を入力します。

   証明書チェーンが必要な場合は、中間証明書を入力できます。

   秘密鍵とCA署名デジタル証明書が表示されたら、あとで参照できるように保存します。

5. 公開鍵証明書を取得します。

   `security certificate show -vserver` *`svm_name`* `-common-name` *`ca_cert_name`* `-type root-ca -instance`

   クライアント側の設定用に公開鍵証明書を保存しておきます。

   例

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
          Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

関連情報

- "セキュリティ証明書のインストール"
- "security certificate show"
- "セキュリティ証明書の署名"

ONTAP S3サービスデータポリシーを作成

S3のデータサービスと管理サービスのサービスポリシーを作成できます。LIFでS3データトラフィックを有効にするには、S3サービスデータポリシーが必要です。

タスクの内容

データLIFとクラスタ間LIFを使用している場合は、S3サービスデータポリシーが必要です。ローカル階層化のユースケースにクラスタLIFを使用している場合は必要ありません。

LIFにサービスポリシーを指定すると、そのポリシーを使用してLIFのデフォルトロール、フェイルオーバーポリシー、およびデータプロトコルのリストが作成されます。

SVMとLIFには複数のプロトコルを設定できますが、オブジェクトデータの提供にはS3プロトコルのみを使用

することを推奨します。

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. サービスデータポリシーを作成します。

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   > `data-core`ONTAP S3を有効にするために必要なサービスはサービスと `data-s3-server`サービスだけですが、必要に応じて他のサービスも含めることができます。

   の詳細については `network interface service-policy create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP S3用のデータ**LIF**の作成

新しいSVMを作成した場合は、S3アクセス専用のLIFとしてデータLIFを作成する必要があります。

開始する前に

- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

  の詳細については `network subnet create`、を"ONTAPコマンド リファレンス"参照してください。

- LIFサービスポリシーがすでに存在している必要があります。
- ベストプラクティスとして、データアクセスに使用するLIF（data-s3-server）と管理処理に使用するLIF（management-https）を別 々 に配置することを推奨します。同じLIFで両方のサービスを有効にしないでください。
- DNSレコードには、data-s3-serverが関連付けられているLIFのIPアドレスだけを含める必要があります。他のLIFのIPアドレスがDNSレコードに指定されている場合、ONTAP S3要求が他のサーバから処理され、予期しない応答やデータの損失が発生する可能性があります。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。

および `network interface capacity details show`の詳細については `network interface capacity show`、を"ONTAPコマンド リファレンス"参照してください。

- リモートのFabricPool容量（クラウド）階層化を有効にする場合は、クラスタ間LIFも設定する必要があります。

手順

1. LIFを作成します。

```
network interface create -vserver svm_name -lif lif_name -service-policy
service_policy_names -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

   - `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

     の詳細については `network interface revert`、を"ONTAPコマンド リファレンス"参照してください。

     オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

   - `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
   - オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
   - サブネットを使用してIPアドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときに、ゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
   - IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内での静的ルートの作成に関する詳細については、を"ONTAPコマンド リファレンス"参照し `network route create`てください。
   - オプションには `-firewall-policy`、LIFのロールと同じデフォルトを使用し `data`ます。

     必要に応じて、あとからカスタムファイアウォールポリシーを作成して追加できます。

     ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

   - `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false`。
   - オプションは、 `-service-policy`作成したデータサービスポリシーと管理サービスポリシー、およびその他の必要なポリシーを指定します。

2. オプションでIPv6アドレスを割り当てる場合 `-address`は、次の手順を実行します。

   a. コマンドを使用して `network ndp prefix show`、さまざまなインターフェイスで学習されたRAプレフィックスのリストを表示します。

      コマンドは `network ndp prefix show`、advanced権限レベルで使用できます。

   b. 形式を使用し `prefix:id`て、IPv6アドレスを手動で作成します。

      `prefix`は、さまざまなインターフェイスで学習されたプレフィックスです。

   を生成するには `id`、ランダムな64ビット16進数を選択します。

3. コマンドを使用して、LIFが正常に作成されたことを確認します `network interface show`。
4. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドは、サービスポリシーが割り当てられたS3データLIFを作成する方法を示してい `my-S3-policy`ます。

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

関連情報

- "ネットワークping"
- "ネットワークインターフェイス"
- "network ndp prefix show"

ONTAP S3によるリモート**FabricPool**階層化用のクラスタ間**LIF**の作成

ONTAP S3を使用してリモートのFabricPool容量（クラウド）階層化を有効にする場合は、クラスタ間LIFを設定する必要があります。データネットワークと共有するポートにクラスタ間LIFを設定できます。これにより、クラスタ間ネットワークに必要なポート数

を減らすことができます。

開始する前に

- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。の詳細については `up`、を"ONTAPコマンド リファレンス"参照してください。
- LIFサービスポリシーがすでに存在している必要があります。

タスクの内容

クラスタ間LIFは、ローカルのファブリックプールの階層化や外部のS3アプリケーションへの提供には必要ありません。

手順

1. クラスタ内のポートの一覧を表示します。

   ```
   network port show
   ```

   次の例は、のネットワークポートを示してい`cluster01`ます。

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

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

2. システムSVMにクラスタ間LIFを作成します。

   ```
   network interface create -vserver Cluster -lif LIF_name -service-policy
   default-intercluster -home-node node -home-port port -address port_IP -netmask
   netmask
   ```

   次の例は、クラスタ間LIFと`cluster01_icl02`を作成し`cluster01_icl01`ます。

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

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

の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

3. クラスタ間LIFが作成されたことを確認します。

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

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. クラスタ間LIFが冗長構成になっていることを確認します。

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

   次の例は、インタークラスタLIFおよび `cluster01_icl02`ポート上の `e0c`ポートがそのポートにフェイルオーバーする `e0d`ことを示しています `cluster01_icl01`。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP S3オブジェクトストアサーバの作成

ONTAPオブジェクトストアサーバは、ONTAP NASサーバやSANサーバが提供するファイルストレージやブロックストレージとは対照的に、S3オブジェクトとしてデータを管理します。

開始する前に

クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。FQDNの1文字目をバケット名にすることはできません。仮想ホスト形式を使用してバケットにアクセスする場合は、サーバ名がとして使用されます `mydomain.com`。たとえば、 `bucketname.mydomain.com`です。

自己署名CA証明書（前の手順で作成）または外部CAベンダーによって署名された証明書が必要です。IPトラフィックがクラスタLIFのみを経由するローカル階層化では、CA証明書は必要ありません。

タスクの内容

オブジェクトストアサーバを作成すると、UIDが0のrootユーザが作成されます。このrootユーザに対してアクセスキーやシークレットキーは生成されません。ONTAP管理者は、このユーザのアクセスキーとシークレットキーを設定するコマンドを実行する必要があります `object-store-server users regenerate-keys`。

> NetAppのベストプラクティスとして、このrootユーザは使用しないでください。rootユーザのアクセスキーまたはシークレットキーを使用するクライアントアプリケーションには、オブジェクトストア内のすべてのバケットとオブジェクトへのフルアクセスが付与されます。

の詳細については `vserver object-store-server`、を"ONTAPコマンド リファレンス"参照してください。

例 **24.** 手順

System Manager

この手順は、既存のStorage VMにS3サーバを追加する場合に使用します。新しいStorage VMにS3サーバを追加する方法については、を参照してください"S3用のストレージSVMを作成します"。

インターフェイスロールデータのIPアドレスを入力する準備をしておく必要があります。

1. 既存のStorage VMでS3を有効にします。
   a. Storage VMを選択します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[S3]*の下をクリックします ⚙ 。
   b. Enable S3 * をクリックし、 S3 Server Name を入力します。
   c. 証明書のタイプを選択します。

      システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。

   d. ネットワークインターフェイスを入力します。
2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。
   - 今後シークレットキーは表示されません。
   - 証明書情報が再度必要な場合は、 [* ストレージ] 、 [Storage VMs] の順にクリックし、 Storage VM を選択して、 [* 設定] をクリックします。

CLI

1. S3サーバを作成します。

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   追加のオプションは、S3サーバの作成時または作成後いつでも指定できます。

   - ローカルの階層化を設定する場合は、SVM名にデータSVM名またはシステムSVM（クラスタ）名を指定できます。
   - 証明書名は、サーバCA証明書（中間またはルートCA証明書）ではなく、サーバ証明書（エンドユーザまたはリーフ証明書）の名前にする必要があります。
   - HTTPSはポート443ではデフォルトで有効になっています。ポート番号はオプションで変更できます `-secure-listener-port`。

     HTTPSを有効にすると、SSL/TLSと正しく統合するためにCA証明書が必要になります。ONTAP 9 .15.1以降では、S3オブジェクトストレージでTLS 1.3がサポートされます。

   - HTTPはデフォルトで無効になっています。有効にすると、サーバはポート80でリスンします。オプションを使用して有効にすることも、オプションを使用してポート番号を変更する `-listener-port`こともできます `-is-http-enabled`。

     HTTPが有効な場合、要求と応答はクリアテキストでネットワーク経由で送信されます。

2. S3が設定されていることを確認します。

```
vserver object-store-server show
```

例

このコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                 HTTP Enabled: false
                                HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

S3対応SVMにストレージ容量を追加する

ONTAP S3バケットを作成する

S3オブジェクトは_Buckets_に保持されます。他のディレクトリ内のディレクトリ内にファイルとしてネストされることはありません。

開始する前に

S3サーバを含むStorage VMがすでに存在している必要があります。

タスクの内容

- ONTAP 9 14.1以降では、S3 FlexGroupボリュームでバケットが作成されたときに、ボリュームの自動サイズ変更が有効になりました。これにより、既存および新規のFlexGroupボリュームでバケットを作成する際の過剰な容量割り当てが解消されます。FlexGroupボリュームのサイズは、次のガイドラインに基づいて、必要な最小サイズに変更されます。必要な最小サイズは、FlexGroupボリューム内のすべてのS3バケットの合計サイズです。
  - ONTAP 9 14.1以降では、新しいバケットの作成時にS3 FlexGroupボリュームが作成されると、必要な最小サイズでFlexGroupボリュームが作成されます。
  - S3 FlexGroupボリュームがONTAP 9 .14.1より前に作成された場合は、ONTAP 9のあとに最初に作成または削除されたバケットが表示されます。14.1では、FlexGroupボリュームのサイズが必要な最小サイズに変更されます。
  - S3 FlexGroupボリュームがONTAP 9 .14.1より前に作成されたボリュームで、必要な最小サイズがすでに設定されている場合は、ONTAP 9 .14.1以降のバケットの作成または削除によってS3 FlexGroupボリュームのサイズが維持されます。

- ストレージサービスレベルは、事前定義されたアダプティブ QoS ポリシーグループで、 *value*、*performion*、 _extreme デフォルトレベルがあります。デフォルトのストレージサービスレベルの代わりに、カスタムのQoSポリシーグループを定義してバケットに適用することもできます。ストレージサービス定義の詳細については、を参照してください"ストレージサービスの定義"。パフォーマンス管理の詳細については、を参照してください"パフォーマンス管理"。ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。
- ローカルの容量階層化を設定する場合は、S3サーバが配置されているシステムStorage VMではなく、データStorage VMにバケットとユーザを作成します。
- リモートクライアントアクセスの場合は、S3対応Storage VMにバケットを設定する必要があります。S3対応でないStorage VMにバケットを作成した場合、そのバケットはローカルの階層化にのみ使用できます。
- ONTAP 9 .14.1以降では、この機能を"MetroCluster構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットを作成する"使用できます。
- CLIでバケットを作成する場合は、次の2つのプロビジョニングオプションがあります。
  - ONTAP Selectを基盤となるアグリゲートとFlexGroupコンポーネントにする（デフォルト）
    - ONTAPでは、アグリゲートが自動的に選択されることで、最初のバケットのFlexGroupボリュームが作成および設定されます。プラットフォームで使用可能な最も高いサービスレベルが自動的に選択されます。または、ストレージサービスレベルを指定できます。あとでStorage VMに追加するバケットには、同じFlexGroupボリュームが使用されます。
    - バケットを階層化に使用するかどうかを指定することもできます。その場合、ONTAPは階層化されたデータに最適なパフォーマンスを備えた低コストのメディアを選択しようとします。
  - 使用するアグリゲートとFlexGroupコンポーネントを選択します（advanced権限のコマンドオプションが必要です）。バケットと包含FlexGroupボリュームを作成するアグリゲートを手動で選択し、各アグリゲートのコンスティチュエントの数を指定できます。バケットを追加する場合：
    - 新しいバケット用のアグリゲートとコンスティチュエントを指定すると、そのバケット用に新しいFlexGroupが作成されます。
    - 新しいバケット用のアグリゲートとコンスティチュエントを指定しない場合、新しいバケットは既存のFlexGroupに追加されます。詳細については、を参照してください FlexGroupホリユウムノカンリ 。

      バケットの作成時にアグリゲートとコンスティチュエントを指定した場合、デフォルトまたはカスタムのQoSポリシーグループは適用されません。これは、コマンドを使用してあとで実行できます `vserver object-store-server bucket modify`。

    の詳細については `vserver object-store-server bucket modify`、を"ONTAPコマンド リファレンス"参照してください。

注： Cloud Volumes ONTAP からバケットを処理する場合は、CLI手順 を使用してください。使用するノードが1つだけになるように、基盤となるアグリゲートを手動で選択することを強く推奨します。両方のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を与える可能性があります。

ONTAP CLIを使用した**S3**バケットの作成

1. アグリゲートとFlexGroupコンポーネントを自分で選択する場合は、権限レベルをadvancedに設定します（それ以外の場合はadmin権限レベルで十分です）。 `set -privilege advanced`

2. バケットを作成します。

   `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

   ローカルでの階層化を設定する場合は、Storage VMの名前にデータStorage VMまたは（システムStorage VMの名前）を指定できます `Cluster`。

   オプションを指定しない場合、800GBのバケットが作成され、システムで使用可能な最上位のサービスレベルが設定されます。

   パフォーマンスまたは使用量に基づいてバケットを作成する場合は、次のいずれかのオプションを使用します。

   - サービスレベル

     オプションに `-storage-service-level`、 `performance`、またはの `extreme`いずれかの値を指定します `value`。

   - 階層化

     オプションを含め `-used-as-capacity-tier true`ます。

     基盤となるFlexGroupボリュームを作成するアグリゲートを指定する場合は、次のオプションを使用します。

   - パラメータは `-aggr-list`、FlexGroupボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

     リスト内の各エントリによって、指定したアグリゲート上にコンスティチュエントが1つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

   FlexGroupボリューム全体で一貫したパフォーマンスが得られるように、ディスク タイプとRAIDグループ構成をすべてのアグリゲートで同じにする必要があります。

   - パラメータは `-aggr-list-multiplier`、FlexGroupボリュームの作成時にパラメータで指定したアグリゲートを繰り返し実行する回数を指定します `-aggr-list`。

     パラメータのデフォルト値 `-aggr-list-multiplier`は4です。

3. 必要に応じてQoSポリシーグループを追加します。

   `vserver object-store-server bucket modify -bucket bucket_name -qos-policy -group qos_policy_group`

4. バケットの作成を確認します。

   `vserver object-store-server bucket show [-instance]`

例

次の例では、Storage VM用のサイズの `1TB`バケットを作成し `vs1`、アグリゲートを指定しています。

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

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

System Managerを使用した**S3**バケットの作成

1. S3対応Storage VMに新しいバケットを追加する。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。
      - この時点で * Save * をクリックすると、次のデフォルト設定でバケットが作成されます。
        - グループポリシーがすでに有効になっていないかぎり、バケットへのアクセスはユーザに許可されません。

          オブジェクトストレージへのアクセスが無制限になるため、S3 rootユーザを使用してONTAPオブジェクトストレージの管理と権限の共有を行わないでください。代わりに、管理Privilegesを割り当てたユーザまたはグループを作成します。

        - システムで使用可能な最高のサービス品質（パフォーマンス）レベル。
      - [保存]*をクリックして、これらのデフォルト値でバケットを作成します。

追加の権限と制限を設定する

バケットの設定時に*[その他のオプション]*をクリックすると、オブジェクトロック、ユーザ権限、パフォーマンスレベルを設定できます。設定はあとで変更することもできます。

S3 オブジェクトストアを FabricPool の階層化に使用する場合は、パフォーマンスサービスレベルではなく、階層化に * 使用（階層化データのパフォーマンスが最適な低コストのメディアを使用）を選択することを検討してください。

バケットでバージョン管理が有効になっている場合は、S3クライアントを使用してオブジェクトの特定のバージョンにオブジェクトロックの保持期限を設定できます。オブジェクトの特定のバージョンをロックしても、そのオブジェクトの他のバージョンが削除されることはありません。後でリカバリするためにオブジェクトのバージョン管理を有効にする場合は、*バージョン管理を有効にする*を選択します。バケットでオブジェクトのロックを有効にすると、バージョン管理がデフォルトで有効になります。オブジェクトのバージョン管理の詳細については、を参照して "AmazonのS3バケットでのバージョン管理の使用"ください。

9.14.1以降では、S3バケットでオブジェクトロックがサポートされます。バケットの作成時にS3オブジェクトロックを有効にする必要があります。オブジェクトロックは既存のバケットでは有効にできません。オブジェクトロックはS3ネイティブのユースケースでのみ使用できます。S3プロトコルを使用するように設定されたマルチプロトコルNASボリュームでは、SnapLockを使用してWORMストレージにデータをコミットする必要があります。S3オブジェクトロックには標準のSnapLockライセンスが必要です。このライセンスはに含まれてい"ONTAP One"ます。

ONTAP Oneより前のバージョンでは、 SnapLockライセンスはセキュリティおよびコンプライアンスバンドルに含まれていました。セキュリティおよびコンプライアンスバンドルは現在提供されていませんが、引き続き有効です。現在は必須ではありませんが、既存のお客様は選択できます"ONTAP Oneへのアップグレード"。、"インストール"オブジェクトのロックを有効にする前に、これを実行してください。

SnapLockライセンスがインストールされていることを確認したら、バケット内のオブジェクトが削除または上書きされないように保護するには、*[オブジェクトのロックを有効にする]*を選択します。ロックは、すべてのバージョンまたは特定のバージョンのオブジェクトで有効にできます。また、クラスタノードのSnapLock Complianceクロックが初期化されている場合にのみ有効にできます。次の手順を実行します。

1. クラスタのいずれのノードでもSnapLockコンプライアンスクロックが初期化されていない場合は、**[Initialize SnapLock Compliance Clock]***ボタンが表示されます。クラスタノードの**SnapLock**コンプライアンスクロックを初期化するには、[SnapLockコンプライアンスクロックの初期化]*をクリックします。
2. オブジェクトに対して_ Write Once、Read Many（WORM）_権限を許可する時間ベースのロックを有効にするには、* Governance *モードを選択します。Governance_modeであっても、特定の権限を持つ管理者ユーザがオブジェクトを削除できます。
3. オブジェクトに対してより厳密な削除ルールと更新ルールを割り当てる場合は、*準拠*モードを選択します。このモードのオブジェクトロックでは、指定した保持期間が終了した時点でのみオブジェクトを期限切れにできます。保持期間を指定しないかぎり、オブジェクトは無期限にロックされたままになります。
4. 一定期間ロックを有効にする場合は、ロックの保持期間を日単位または年単位で指定します。

ロックは、バージョン管理に対応しているS3バケットとバージョン管理に対応していないS3バケットに適用されます。オブジェクト ロックは、NASオブジェクトには適用されません。

バケットの保護と権限の設定、およびパフォーマンス サービス レベルを設定できます。

権限を設定するには、事前にユーザとグループを作成しておく必要があります。

詳細については、を参照してください "新しいバケットのミラーを作成"。

バケットへのアクセスを確認

S3クライアントアプリケーション（ONTAP S3または外部のサードパーティアプリケーション）では、次のように入力して、新しく作成したバケットへのアクセスを確認できます。

- S3サーバのCA証明書。
- ユーザのアクセスキーとシークレットキー。
- S3サーバのFQDN名とバケット名。

ONTAP S3バケットサイズを拡張または縮小する

必要に応じて、既存のバケットのサイズを増減できます。

手順

バケットサイズは、System ManagerまたはONTAP CLIを使用して管理できます。

System Manager

1. [Storage]>[Buckets]*を選択し、変更するバケットを探します。
2. バケット名の横にあるをクリックし ⋮ 、*[編集]*を選択します。
3. [Edit bucket]*ウィンドウで、バケットの容量を変更します。
4. 保存。

CLI

1. バケットの容量を変更します。

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

MetroCluster構成のミラーされたアグリゲートまたはミラーされていないアグリゲートに**ONTAP S3**バケットを作成する

ONTAP 9.14.1以降では、MetroCluster FC構成およびIP構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットをプロビジョニングできます。

タスクの内容

- デフォルトでは、バケットはミラーされたアグリゲート上にプロビジョニングされます。
- MetroCluster環境でバケットを作成する場合も、で説明したのと同じプロビジョニングガイドラインが"バケットを作成する"適用されます。
- MetroCluster環境では、S3オブジェクトストレージの次の機能は*サポートされません*。
  - SnapMirror S3
  - S3バケットのライフサイクル管理
  - Compliance *モードでのS3オブジェクトのロック

    *ガバナンス*モードでのS3オブジェクトのロックがサポートされています。

  - ローカルFabricPool階層化

開始する前に

S3サーバを含むSVMがすでに存在している必要があります。

バケットを作成するプロセス

CLI

1. アグリゲートとFlexGroupコンポーネントを自分で選択する場合は、権限レベルをadvancedに設定します（それ以外の場合はadmin権限レベルで十分です）。 `set -privilege advanced`
2. バケットを作成します。

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   ミラーされたアグリゲートとミラーされていないアグリゲートのどちらを使用するかに応じて、オプションをまたは `false`に `true`設定し `-use-mirrored-aggregates`ます。

   > デフォルトでは、この `-use-mirrored-aggregates`オプションはに設定されて `true`います。

   - SVM名はデータSVMである必要があります。
   - オプションを指定しない場合、800GBのバケットが作成され、システムで使用可能な最上位のサービス レベルが設定されます。
   - パフォーマンスまたは使用量に基づいてバケットを作成する場合は、次のいずれかのオプションを使用します。
     - サービスレベル

       オプションに `-storage-service-level`、 `performance`、またはの `extreme`いずれかの値を指定します `value`。

     - 階層化

       オプションを含め `-used-as-capacity-tier true`ます。
   - 基盤となるFlexGroupボリュームを作成するアグリゲートを指定する場合は、次のオプションを使用します。
     - パラメータは `-aggr-list`、FlexGroupボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

       リスト内の各エントリによって、指定したアグリゲート上にコンスティチュエントが1つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

   FlexGroupボリューム全体で一貫したパフォーマンスが得られるように、ディスク タイプとRAIDグループ構成をすべてのアグリゲートで同じにする必要があります。

   - パラメータは `-aggr-list-multiplier`、FlexGroupボリュームの作成時にパラメータで指定したアグリゲートを繰り返し実行する回数を指定します `-aggr-list`。

     パラメータのデフォルト値 `-aggr-list-multiplier`は4です。

3. 必要に応じてQoSポリシーグループを追加します。

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. バケットの作成を確認します。

```
vserver object-store-server bucket show [-instance]
```

例

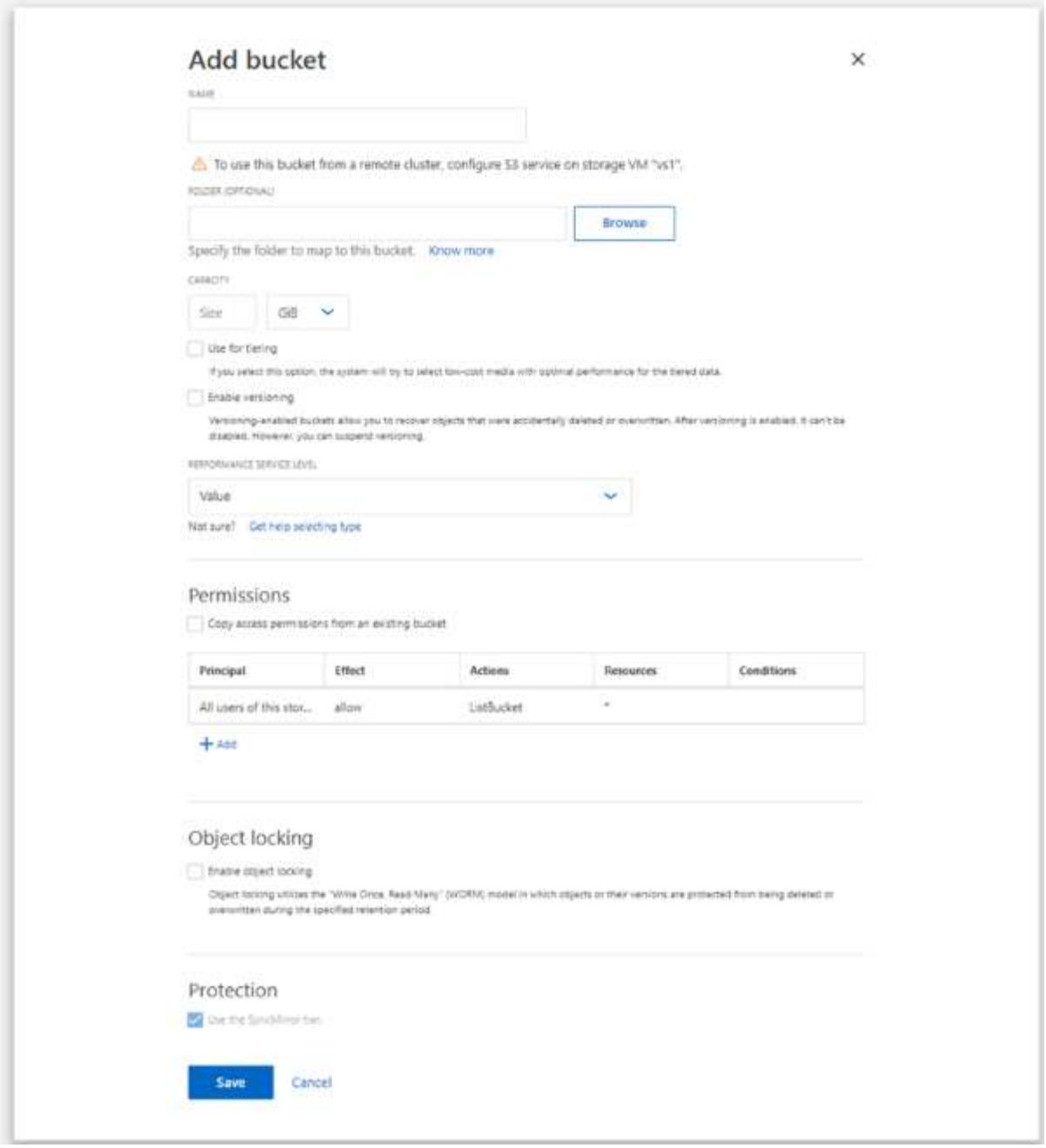
次の例では、ミラーされたアグリゲート上に1TBのSVM vs1のバケットを作成します。

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. S3対応Storage VMに新しいバケットを追加する。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      デフォルトでは、バケットはミラーされたアグリゲートにプロビジョニングされます。ミラーされていないアグリゲートにバケットを作成する場合は、**[**その他のオプション**]***を選択し、[保護]の[SyncMirror階層を使用する]*ボックスをオフにします（次の図を参照）。



- この時点で * Save * をクリックすると、次のデフォルト設定でバケットが作成されます。
  - グループポリシーがすでに有効になっていないかぎり、バケットへのアクセスはユーザに許可されません。

> オブジェクトストレージへのアクセスが無制限になるため、S3 rootユーザを使用してONTAPオブジェクトストレージの管理と権限の共有を行わないでください。代わりに、管理Privilegesを割り当てたユーザまたはグループを作成します。

  - システムで使用可能な最高のサービス品質（パフォーマンス）レベル。
- バケットの設定時にユーザの権限やパフォーマンスレベルを設定するには、「 * More Options * 」をクリックします。あとで設定を変更することもできます。

- 権限を設定するために * More Options * を使用する前に、ユーザーとグループを作成しておく必要があります。
- S3 オブジェクトストアを FabricPool の階層化に使用する場合は、パフォーマンスサービスレベルではなく、階層化に * 使用（階層化データのパフォーマンスが最適な低コストのメディアを使用）を選択することを検討してください。

2. S3クライアントアプリケーション（別のONTAPシステムまたは外部のサードパーティアプリケーション）で、次のように入力して新しいバケットへのアクセスを確認します。
   - S3サーバのCA証明書。
   - ユーザのアクセスキーとシークレットキー。
   - S3サーバのFQDN名とバケット名。

ONTAP S3バケットライフサイクル管理ルールを作成する

ONTAP 9 .13.1以降では、S3バケット内のオブジェクトライフサイクルを管理するためのライフサイクル管理ルールを作成できます。バケット内の特定のオブジェクトに対して削除ルールを定義し、それらのルールを使用してバケットオブジェクトを期限切れにすることができます。これにより、保持要件を満たし、S3オブジェクトストレージ全体を効率的に管理できます。

バケットオブジェクトに対してオブジェクトロックが有効になっている場合、オブジェクトの有効期限に関するライフサイクル管理ルールはロックされたオブジェクトには適用されません。オブジェクトのロックについては、を参照してください"バケットを作成する"。

開始する前に

- S3サーバとバケットを含むS3対応のSVMがすでに存在している必要があります。詳細については、を参照してください "S3用のSVMの作成" 。
- マルチプロトコルNASボリュームでS3を使用している場合、またはMetroCluster構成でS3を使用している場合は、バケットライフサイクル管理ルールがサポートされません。

タスクの内容

ライフサイクル管理ルールを作成する際に、バケットオブジェクトに次の削除操作を適用できます。

- 現在のバージョンの削除-このアクションは、ルールで指定されたオブジェクトを期限切れにします。バケットでバージョン管理が有効になっている場合は、S3によって、期限切れになったすべてのオブジェクトが使用できなくなります。バージョン管理が有効になっていない場合は、オブジェクトが永続的に削除されます。CLIアクションはです `Expiration`。
- Deletion of non-current versions - S3が最新でないオブジェクトを完全に削除できるタイミングを指定します。CLIアクションはです `NoncurrentVersionExpiration`。

最新でないバージョンは、現在のバージョンの作成時刻または変更時刻に基づいています。最新でないオブジェクトの削除を遅らせておくと、誤ってオブジェクトを削除または上書きした場合に役立ちます。たとえば、最新でないバージョンが最新でない状態になってから5日後に削除するように、有効期限ルールを設定できます。たとえば、2014年1月1日の午前10時30分（UTC）に、という名前のオブジェクト（バージョンID `111111`）を作成したとし `photo.gif`ます。2014年1月2日午前11時30分（UTC）に誤って（バージョンID） `111111`を削除する `photo.gif`と、新しいバージョンID（バージョンIDなど）を持つ削除マーカーが作成されます `4857693`。5日以内に元のバージョン（バージョンID `111111`）を復元してから、削除が永続的に行われるようになり `photo.gif`ます。2014年1月8日00:00 UTCに、有効期限のライフサイクルルールが実行され、非最新バージョンになってから5日後に（バージョンID `111111`）が完全に削除され `photo.gif`ます。

- 期限切れ削除マーカーの削除-このアクションは、期限切れのオブジェクト削除マーカーを削除します。バージョン管理が有効なバケットでは、削除マーカーが付いたオブジェクトがオブジェクトの現在のバージョンになります。オブジェクトは削除されず、アクションを実行することはできません。これらのオブジェクトに現在のバージョンが関連付けられていない場合、これらのオブジェクトは期限切れになります。CLIアクションはです `Expiration`。
- [Deletion of incomplete multipart uploads]-マルチパートアップロードを実行中のままにする最大時間（日数）を設定します。その後、それらは削除されます。CLIアクションはです `AbortIncompleteMultipartUpload`。

実行する手順は、使用するインターフェイスによって異なります。ONTAP 9.13、1では、CLIを使用する必要があります。ONTAP 9.14.1以降では、System Managerも使用できます。

CLIを使用したライフサイクル管理ルールの管理

ONTAP 9.13.1以降では、ONTAP CLIを使用して、S3バケット内のオブジェクトを期限切れにするライフサイクル管理ルールを作成できます。

開始する前に

CLIでは、バケットライフサイクル管理ルールを作成するときに、有効期限アクションタイプごとに必須フィールドを定義する必要があります。これらのフィールドは、最初の作成後に変更できます。次の表に、アクションタイプごとに固有のフィールドを示します。

アクションタイプ	一意のフィールド
NonCurrentVersionExpiration	• `-non-curr-days`-最新でないバージョンが削除されるまでの日数 • `-new-non-curr-versions`-保持する最新の非最新バージョンの数
有効期限	• `-obj-age-days`-オブジェクトの現在のバージョンを削除できるまでの作成からの日数 • `-obj-exp-date`-オブジェクトが期限切れになる日付 • `-expired-obj-del-markers`-オブジェクト削除マーカーのクリーンアップ
AbortIncompleteMultipartUpload	• `-after-initiation-days`-アップロードが中止されるまでの開始日数

バケットライフサイクル管理ルールを特定のオブジェクトのサブセットにのみ適用するには、管理者はルールの作成時に各フィルタを設定する必要があります。ルールの作成時にこれらのフィルタが設定されていない場合、ルールはバケット内のすべてのオブジェクトに適用されます。

以下の場合は、すべてのフィルタを最初に作成した後_except_に変更できます。+

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

手順

1. コマンドとexpirationアクションタイプの必須フィールドを使用し `vserver object-store-server bucket lifecycle-management-rule create`て、バケットライフサイクル管理ルールを作成します。

例

次のコマンドは、NonCurrentVersionExpirationバケットライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

例

次のコマンドは、Expirationバケットライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

例

次のコマンドは、AbortIncompleteMultipartUploadバケットライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

System Managerを使用したライフサイクル管理ルールの管理

ONTAP 9.14.1以降では、System Managerを使用してS3オブジェクトを期限切れにすることができます。S3オブジェクトのライフサイクル管理ルールを追加、編集、削除できます。また、あるバケット用に作成されたライフサイクルルールをインポートして、別のバケット内のオブジェクトに使用することもできます。アクティブなルールは、あとで無効にして有効にすることができます。

ライフサイクル管理ルールの追加

1. [ストレージ]>[バケット]*をクリックします。
2. 有効期限ルールを指定するバケットを選択します。
3. アイコンをクリックし、*[ライフサイクルルールの管理]*を選択します。
4. [追加]>[ライフサイクルルール]*をクリックします。
5. [ライフサイクルルールの追加]ページで、ルールの名前を追加します。
6. ルールの範囲を定義します。ルールをバケット内のすべてのオブジェクトに適用するか、特定のオブジェクトに適用するかを指定します。オブジェクトを指定する場合は、次のいずれかのフィルタ条件を少なくとも1つ追加します。
   a. prefix：ルールを適用するオブジェクトキー名のプレフィックスを指定します。通常は、オブジェクトのパスまたはフォルダです。1つのルールに1つのプレフィックスを指定できます。有効なプレフィックスが指定されていない場合、ルールがバケット内のすべてのオブジェクトに適用されます。
   b. tags：ルールを適用するオブジェクトのキーと値のペア（タグ）を3つまで指定します。フィルタリングには有効なキーのみが使用されます。この値はオプションです。ただし、値を追加する場合は、対応するキーに有効な値のみを追加してください。
   c. サイズ：オブジェクトの最小サイズと最大サイズの間でスコープを制限できます。どちらかまたは両方の値を入力できます。デフォルトの単位はMIBです。
7. アクションを指定します。
   a. オブジェクトの現在のバージョンを期限切れにする：現在のオブジェクトが作成されてから一定の日数が経過した後、または特定の日付に、すべてのオブジェクトを永続的に使用不可にするルールを設定します。このオプションは、*期限切れのオブジェクト削除マーカーを削除*オプションが選択されている場合は使用できません。
   b. 最新でないバージョンを完全に削除：最新でないバージョンが削除されるまでの日数と、保持するバージョンの数を指定します。
   c. 期限切れのオブジェクト削除マーカーを削除：期限切れの削除マーカーを持つオブジェクト、つまり現在のオブジェクトが関連付けられていないマーカーを削除するには、このアクションを選択します。

このオプションは、保持期間後にすべてのオブジェクトを自動的に削除する*[現在のバージョンのオブジェクトを期限切れにする]*オプションを選択すると使用できなくなります。オブジェクトタグをフィルタリングに使用している場合も、このオプションは使用できません。

d. 未完了のマルチパートアップロードを削除：未完了のマルチパートアップロードを削除するまでの日数を設定します。指定した保持期間内に実行中のマルチパートアップロードが失敗した場合は、完了していないマルチパートアップロードを削除できます。オブジェクトタグをフィルタリングに使用すると、このオプションは使用できなくなります。

e. [保存（ Save ）] をクリックします。

ライフサイクルルールのインポート

1. [ストレージ]>[バケット]*をクリックします。
2. 有効期限ルールをインポートするバケットを選択します。
3. アイコンをクリックし、*[ライフサイクルルールの管理]*を選択します。
4. [追加]>[ルールのインポート]*をクリックします。
5. ルールのインポート元のバケットを選択します。選択したバケットに対して定義されているライフサイクル管理ルールが表示されます。
6. インポートするルールを選択します。ルールは一度に1つずつ選択できます。デフォルトでは最初のルールが選択されています。
7. [* インポート *] をクリックします。

ルールの編集、削除、または無効化

編集できるライフサイクル管理操作は、ルールに関連付けられているもののみです。ルールがオブジェクトタグでフィルタされている場合は、**[**期限切れのオブジェクト削除マーカーを削除する**]***オプションと[不完全なマルチパートアップロードを削除する]*オプションは使用できません。

ルールを削除すると、そのルールは以前に関連付けられていたオブジェクトには適用されなくなります。

1. [ストレージ]>[バケット]*をクリックします。
2. ライフサイクル管理ルールを編集、削除、または無効にするバケットを選択します。
3. アイコンをクリックし、*[ライフサイクルルールの管理]*を選択します。
4. 必要なルールを選択します。一度に1つのルールを編集および無効にすることができます。一度に複数のルールを削除できます。
5. 、[削除]、または[無効化]*を選択し、手順を完了します。

ONTAP S3ユーザの作成

特定の権限を持つS3ユーザを作成します。許可されたクライアントだけに接続を制限するには、すべてのONTAPオブジェクトストアでユーザ認証が必要です。

始める前に。

S3対応Storage VMがすでに存在している必要があります。

タスクの内容

S3ユーザにはStorage VM内の任意のバケットへのアクセスを許可できます。S3ユーザを作成すると、そのユーザのアクセスキーとシークレットキーも生成されます。オブジェクトストアのFQDNとバケット名をユーザと共有する必要があります。

セキュリティを強化するため、ONTAP 9.15.1以降では、アクセスキーとシークレットキーはS3ユーザの作成時にのみ表示され、再度表示することはできません。キーを紛失した場合は、"新しいキーを再生成する必要があります"を参照してください。

バケットポリシーまたはオブジェクトサーバポリシーで、S3ユーザに特定のアクセス権限を付与できます。

新しいオブジェクトストアサーバを作成すると、ONTAPによってrootユーザ（UID 0）が作成されます。rootユーザは、すべてのバケットにアクセスできる権限を持つユーザです。NetAppでは、ONTAP S3をrootユーザとして管理するのではなく、特定のPrivilegesでadminユーザロールを作成することを推奨しています。

CLI

1. S3ユーザを作成します。
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - コメントの追加は任意です。
   - ONTAP 9 .14.1以降では、キーが有効になる期間をパラメータで定義できます `-key-time-to-live`。保持期間を次の形式で追加して、アクセスキーの有効期限が切れるまでの期間を指定できます `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`。たとえば、1日、2時間、3分、4秒の保持期間を入力する場合は、と入力します `P1DT2H3M4S`。指定されていないかぎり、キーは無期限に有効です。

     次の例は、Storage VMに `vs0`という名前のユーザを作成し `sm_user1`、キーの保持期間を1週間に設定します。

   ```
   vserver object-store-server user create -vserver vs0 -user sm_user1
   -key-time-to-live P1W
   ```

2. アクセスキーとシークレットキーは必ず保存してください。S3クライアントからのアクセスに必要になります。

System Manager

1. Storage > Storage VM* をクリックします。ユーザを追加するStorage VMを選択し、*[設定]*を選択して[S3]の下をクリックします 。
2. ユーザを追加するには、*[ユーザ]>[追加]*をクリックします。
3. ユーザの名前を入力します。
4. ONTAP 9.14.1以降では、ユーザに対して作成されるアクセス キーの保持期間を指定できます。キーが自動的に期限切れになるまでの保持期間を、日、時間、分、または秒単位で指定できます。デフォルトでは、キーが無期限に有効であることを示す値がに設定され `0`ます。
5. [保存（ Save ）] をクリックします。ユーザが作成され、そのユーザのアクセスキーとシークレットキーが生成されます。
6. アクセスキーとシークレットキーをダウンロードまたは保存します。S3クライアントからのアクセスに必要になります。

次のステップ

- S3グループを作成または変更する

バケットへのアクセスを制御するための**ONTAP S3**ユーザグループの作成または変更

適切なアクセス許可を設定したユーザのグループを作成することで、バケットへのアクセスを簡易化できます。

開始する前に

S3ユーザがS3対応SVMにすでに存在している必要があります。

タスクの内容

S3グループのユーザには1つのSVM内の任意のバケットへのアクセスを許可できますが、複数のSVMへのアクセスは許可できません。グループアクセス権限は、次の2つの方法で設定できます。

- バケットレベル

  S3ユーザのグループを作成したら、バケットポリシーのステートメントにグループ権限を指定すると、そのバケットにのみ適用されます。

- SVMレベル

  S3ユーザのグループを作成したら、グループ定義でオブジェクトサーバポリシーの名前を指定します。これらのポリシーによって、グループメンバーのバケットとアクセスが決まります。

System Manager

1. Storage VMを編集します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。
2. グループを追加：* Groups を選択し、 Add *を選択します。
3. グループ名を入力し、ユーザのリストから選択します。
4. 既存のグループポリシーを選択するか、ここで追加するか、あとで追加することができます。

CLI

1. S3グループを作成します。
   `vserver object-store-server group create -vserver` *`svm_name`* `-name` *`group_name`* `-users` *`user_name\(s\)`* `[-policies` *`policy_names`*`] [-comment` *`text`*`\]` `-policies`オブジェクトストアにバケットが1つしかない設定では、オプションは省略できます。グループ名はバケットポリシーに追加できます。 `-policies`オプションは、オブジェクトストレージサーバポリシーの作成後にコマンドを使用して追加でき `vserver object-store-server group modify`ます。

ONTAP S3キーを再生成して保持期間を変更する

アクセスキーとシークレットキーは、S3クライアントアクセスを有効にするためのユーザの作成時に自動的に生成されます。キーの有効期限が切れた場合や、キーが侵害された場合に、ユーザのキーを再生成できます。

アクセスキーの生成については、を参照してください"S3ユーザの作成"。

System Manager

1. Storage > Storage VM* をクリックし、 Storage VM を選択します。
2. [設定]タブで、* S3 *タイル内をクリックします 。
3. [ユーザ]タブで、アクセスキーがないか、ユーザのキーの有効期限が切れていることを確認します。
4. キーを再生成する必要がある場合は、ユーザーの横にあるをクリックし 、*キーの再生成*をクリックします。
5. デフォルトでは、生成されたキーは無期限に有効です。9.14.1以降では、キーの保持期間を変更できます。この期間が過ぎると、キーは自動的に期限切れになります。保持期間を日、時間、分、または秒単位で入力します。
6. [保存（ Save ）] をクリックします。キーが再生成されます。キーの保持期間の変更はすぐに反映されます。
7. アクセスキーとシークレットキーをダウンロードまたは保存します。S3クライアントからのアクセスに必要になります。

CLI

1. コマンドを実行して、ユーザのアクセスキーとシークレットキーを再生成し `vserver object-store-server user regenerate-keys`ます。
2. デフォルトでは、生成されたキーは無期限に有効です。9.14.1以降では、キーの保持期間を変更できます。この期間が過ぎると、キーは自動的に期限切れになります。保持期間は次の形式で追加できます。 `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`たとえば、1日、2時間、3分、4秒の保持期間を入力する場合は、と入力します `P1DT2H3M4S`。

```
vserver object-store-server user regenerate-keys -vserver svm_name
-user user -key-time-to-live 0
```

3. アクセスキーとシークレットキーを保存します。S3クライアントからのアクセスに必要になります。

アクセスポリシーステートメントの作成または変更

ONTAP S3バケットとオブジェクトストアサーバのポリシーの詳細

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

デフォルトの**ONTAP S3**バケットポリシーにアクセスルールを追加する

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

開始する前に

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

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

タスクの内容

新しいユーザとグループの新しいステートメントを追加したり、既存のステートメントの属性を変更したりできます。の詳細については `vserver object-store-server bucket policy`、を"ONTAPコマンド リファレンス"参照してください。

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

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

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

System Manager

手順

1. バケットを編集します。 * Storage > Bucket* をクリックし、目的のバケットをクリックして * Edit * をクリックします。権限を追加または変更するときは、次のパラメータを指定できます。
   - * Principal *：アクセス権を付与するユーザまたはグループ。
   - 影響：ユーザまたはグループへのアクセスを許可または拒否します。
   - * Actions *：特定のユーザまたはグループに対してバケットで許可されているアクション。
   - * Resources *：アクセスが許可または拒否されているバケット内のオブジェクトのパスと名前。

     デフォルトの * *bucketname** および * *bketname* / * _ * は、バケット内のすべてのオブジェクトへのアクセスを許可します。また、単一のオブジェクトへのアクセスを許可することもできます。たとえば、 ** _bketname/** _readme.txt * と指定します。
   - * Conditions *（オプション）：アクセス試行時に評価される式。たとえば、アクセスを許可または拒否するIPアドレスのリストを指定できます。

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

CLI

手順

1. バケットポリシーにステートメントを追加します。

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

次のパラメータでアクセス権限を定義します。

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

`-principal`	S3ユーザまたはグループのリスト。 • 最大10個のユーザまたはグループを指定できます。 • S3グループを指定する場合は、次の形式で指定する必要があります。`group/group_name`. • `*`には、パブリックアクセス（アクセスキーとシークレットキーを使用しないアクセス）を指定できます。 • プリンシパルを指定しない場合、Storage VM内のすべてのS3ユーザにアクセスが許可されます。
`-resource`	バケットとバケットに含まれるオブジェクト。ワイルドカード文字とを`?`使用 `*`して、リソースを指定するための正規表現を作成できます。リソースについては、ポリシーで変数を指定できます。これらのポリシー変数はプレースホルダであり、ポリシーの評価時にコンテキストに応じた値に置き換えられます。

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

例

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

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

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

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

ONTAP 9 .14.1以降では、バケットポリシーの変数を指定できます。次の例は、Storage VMとの`bucket1`サーババケットポリシーステートメントを作成し `svm1`、ポリシーリソースの変数としてを指定します `${aws:username}`。ポリシーが評価されると、ポリシー変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。たとえば、次のポリシーステートメントが評価されると `${aws:username}`、はS3処理を実行するユーザに置き換えられます。ユーザ `user1`が操作を実行すると、そのユーザにはAS `bucket1/user1/*`へのアクセスが許可され `bucket1`ます。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

ONTAP S3オブジェクトストアサーバポリシーの作成または変更

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

開始する前に

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

タスクの内容

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

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

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

- フルアクセス
- NoS3アクセス
- ReadOnlyAccess

また、新しいカスタムポリシーを作成し、新しいユーザとグループの新しいステートメントを追加したり、既存のステートメントの属性を変更したりすることもできます。の詳細については `vserver object-store-server policy`、を"ONTAPコマンド リファレンス"参照してください。

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

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

System Manager

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

手順

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

      グループポリシーを追加または変更するときは、次のパラメータを指定できます。

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

CLI

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

手順

1. オブジェクトストレージサーバポリシーを作成します。

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

2. ポリシーのステートメントを作成します。

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

   次のパラメータでアクセス権限を定義します。

`-effect`	アクセスを許可するか拒否するかを指定します。

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

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

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

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

ONTAP S3アクセス用の外部ディレクトリサービスの設定

ONTAP 9 .14.1以降では、外部ディレクトリのサービスがONTAP S3オブジェクトストレージに統合されました。この統合により、外部ディレクトリサービスによるユーザとアクセスの管理が簡素化されます。

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

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

開始する前に

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

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

照して "SVMに自己署名ルートCA証明書をインストールする"

5. SVM で TLS が有効になっている LDAP クライアントが構成されています。およびを参照してください"ONTAP NFSアクセス用のLDAPクライアント構成を作成する""LDAPクライアント設定をONTAP NFS SVMに関連付けて情報を取得する"。

LDAP用のS3アクセスの設定

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

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

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

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

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

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

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

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

認証にLDAP高速バインドモードを使用する

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

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

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

2. S3バケットにアクセスするLDAPユーザの権限がバケットポリシーで定義されていることを確認します。詳細については、を参照してください "バケットポリシーを変更する"。
3. LDAPグループのユーザが次の処理を実行できることを確認します。
   a. S3クライアントでアクセスキーを次の形式で設定します。
   `"NTAPFASTBIND" + base64-encode(user-name:password)`例 `"NTAPFASTBIND"：+base64-encode（ldapuser：password）。
   `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

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

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

Base64 クレデンシャル

ONTAP S3のデフォルト設定ではHTTPは除外され、HTTPSとTransport Layer Security（TLS）接続のみが使用されます。ONTAPでは自己署名証明書を生成できますが、サードパーティの認証局（CA）の証明書を使用することを推奨します。CA証明書を使用する場合は、クライアントアプリケーションとONTAPオブジェクトストアサーバの間に信頼された関係を作成します。

Base64を使用してエンコードされたクレデンシャルは簡単にデコードできることに注意してください。HTTPSを使用すると、man-in-the-middleパケットスニファによってエンコードされたクレデンシャルがキャプチャされなくなります。

事前に署名されたURLを作成する場合は、認証にLDAP高速バインドモードを使用しないでください。認証は、事前に署名されたURLに含まれるBase64アクセスキーのみに基づいて行われます。ユーザー名とパスワードは、Base64アクセスキーをデコードするすべてのユーザーに公開されます。

認証方式が**nsswitch**で**LDAP**が有効な場合の例

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

> APIを、SVMのデータLIFではなくクラスタ管理LIFに転送します。ユーザに独自のキーの生成を許可する場合、curlを使用するには、ユーザのロールにHTTP権限を追加する必要があります。この権限は、S3 API権限に追加されたものです。

バケットポリシーステートメントで指定されたnasgroupまたはnasgroupに含まれるユーザにUIDとGIDが設定されていない場合、これらの属性が見つからないと検索が失敗します。Active DirectoryはUIDではなくSIDを使用します。SIDエントリをUIDにマッピングできない場合は、必要なデータをONTAPに取り込む必要があります。

これには、SVMがActive Directoryで認証され、必要なユーザとグループの情報を取得できるようにを使用し"vserver active-directory create"ます。

または、を使用して"vserver cifs create"Active DirectoryドメインにSMBサーバを作成します。

ネームサーバとオブジェクトストアで異なるドメイン名を使用している場合、検索エラーが発生する可能性があります。検索エラーを回避するため、 NetApp、UPN形式のリソース認証に信頼できるドメインを使用することを推奨しています。 `nasgroup/group@trusted_domain.com`信頼されたドメインとは、SMBサーバーの信頼されたドメインリストに追加されたドメインです。 "優先する信頼ドメインの追加、削除、変更" SMB サーバー リストに表示されます。

認証方式がドメインで信頼できるドメインが**Active Directory**で設定されている場合にキーを生成する

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

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

APIを、SVMのデータLIFではなくクラスタ管理LIFに転送します。ユーザに独自のキーの生成を許可する場合、curlを使用するには、ユーザのロールにHTTP権限を追加する必要があります。この権限は、S3 API権限に追加されたものです。

認証方式が**domain**で、信頼できるドメインがない場合にキーを生成する

この処理は、LDAPが無効になっている場合、またはPOSIX以外のユーザがUIDとGIDを設定していない場合に実行できます。例：

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

APIを、SVMのデータLIFではなくクラスタ管理LIFに転送します。ユーザに独自のキーの生成を許可する場合、curlを使用するには、ユーザのロールにHTTP権限を追加する必要があります。この権限は、S3 API権限に追加されたものです。オプションのドメイン値（@FQDN）をユーザ名に追加する必要があるのは、信頼できるドメインがない場合だけです。

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

ONTAP 9 .14.1以降では、ONTAP管理者としてカスタムロールを作成し、ローカルグループ、ドメイングループ、またはLightweight Directory Access Protocol（LDAP）グループに付与して、それらのグループに属するユーザがS3クライアントアクセス用の独自のアクセスキーとシークレットキーを生成できるようにすることができます。

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

LDAPが無効になっている場合は、 "ONTAP S3 アクセス用の外部ディレクトリ サービスを構成する"ユーザーがアクセス キーを生成できるようにします。

開始する前に

次の点を確認します。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照して "S3用のSVMの作成"
2. そのStorage VMにバケットが作成されている。を参照して "バケットを作成する"
3. Storage VMにDNSが設定されています。を参照して "DNSサービスの設定"
4. LDAP サーバーの自己署名ルート証明機関 (CA) 証明書がストレージ VM にインストールされます。を参照して "SVMに自己署名ルートCA証明書をインストールする"
5. ストレージ VM 上で TLS が有効になっている LDAP クライアントが構成されています。を参照して "ONTAP NFSアクセス用のLDAPクライアント構成を作成する"
6. クライアント設定をSVMに関連付けます。を参照して "LDAPクライアント設定をONTAP NFS SVMに関連付ける"の詳細については `vserver services name-service ldap create`、を"ONTAPコマンドリファレンス"参照してください。
7. データStorage VMを使用している場合は、管理ネットワークインターフェイス（LIF）とVM上に、LIFのサービスポリシーを作成します。および `network interface service-policy create`の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

アクセスキー生成のためのユーザの設定

例 **25.** 手順

LDAPユーザ

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

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

の詳細については `vserver services name-service ns-switch modify`、を"ONTAPコマンド リファレンス"参照してください。

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

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

の詳細については `security login rest-role create`、を"ONTAPコマンド リファレンス"参照してください。

3. LDAPユーザーグループを作成します。 `security login`コマンドを実行し、S3 ユーザー REST API エンドポイントにアクセスするための新しいカスタム ロールを追加します。詳細はこちら `security login create`の中で"ONTAPコマンド リファレンス" 。

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

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

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

詳細については、を参照してください "ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使

用する"。

の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

LDAPグループにカスタムロールを追加すると、そのグループのユーザーはONTAPへの限定的なアクセスが可能になります。 `/api/protocols/s3/services/{svm.uuid}/users`エンドポイント。APIを呼び出すことで、LDAP グループのユーザーは独自のアクセスキーと秘密キーを生成し、S3 クライアントにアクセスできるようになります。生成できるのは自分のキーだけで、他のユーザのキーは生成できません。

ドメイン ユーザ

1. S3ユーザREST APIエンドポイントへのアクセス権を持つカスタム ロールを作成します。

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

この例では、 `s3-role`ストレージVM上のユーザーに対してロールが生成される `svm-1`読み取り、作成、更新のすべてのアクセス権が付与されます。

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

の詳細については `security login rest-role create`、を"ONTAPコマンド リファレンス"参照してください。

1. ドメインユーザーグループを作成します。 `security login`コマンドを実行し、S3 ユーザー REST API エンドポイントにアクセスするための新しいカスタム ロールを追加します。詳細はこちら `security login create`の中で"ONTAPコマンド リファレンス" 。

   ```
   security login create -vserver <vserver-name> -user-or-group-name
   domain\<group-name> -application http -authentication-method domain
   -role <custom-role-name>
   ```

   この例では、ドメイングループ `domain\group1`作成されます `svm-1` 、カスタムロール `s3role` API エンドポイントにアクセスするために追加されます。

   ```
   security login create -user-or-group-name domain\group1 -application
   http -authentication-method domain -role s3role -vserver svm-1
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

ドメイングループにカスタムロールを追加すると、そのグループ内のユーザーはONTAPへの限定的なアクセスが可能になります。 `/api/protocols/s3/services/{svm.uuid}/users`エンドポイント。APIを呼び出す

ことで、ドメイン グループのユーザーは独自のアクセス キーと秘密キーを生成し、S3 クライアントにアクセスできるようになります。生成できるのは自分のキーだけで、他のユーザのキーは生成できません。

S3ユーザまたはLDAPユーザとして、独自のアクセスキーを生成

ONTAP 9 14.1以降では、S3クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます（管理者が独自のキーを生成するロールをユーザに許可している場合）。次のONTAP REST APIエンドポイントを使用すると、自分専用のキーを生成できます。

S3 ユーザーを作成し、キーを生成する

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

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

ドメイン ユーザーの場合、S3 ユーザー名に次の形式を使用します。 `user@fqdn` 、 どこ `fqdn`ドメインの完全修飾ドメイン名です。

カールの例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON出力の例

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3 ユーザーのキーを再生成する

S3 ユーザーがすでに存在する場合は、そのアクセスキーとシークレットキーを再生成できます。このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

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

カールの例

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

JSON出力の例

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3オブジェクトストレージへのクライアントアクセスを有効にする

ONTAP S3アクセスによるリモート**FabricPool**階層化を有効にする

ONTAP S3をリモートFabricPoolの大容量（クラウド）階層として使用するには、ONTAP S3管理者がリモートのONTAPクラスタ管理者にS3サーバの設定に関する情報を提供する必要があります。

タスクの内容

FabricPoolクラウド階層を設定するには、次のS3サーバ情報が必要です。

- サーバ名（FQDN）
- バケット名
- CA証明書
- アクセスキー
- パスワード（シークレットアクセスキー）

さらに、次のネットワーク設定が必要です。

- 管理SVM用に設定されたDNSサーバに、リモートONTAP S3サーバのホスト名に関するエントリ（S3サーバのFQDN名とサーバのLIFのIPアドレスを含む）が必要です。
- クラスタピアリングは不要ですが、ローカルクラスタにインタークラスタLIFが設定されている必要があります。

ONTAP S3をクラウド階層として設定する方法については、FabricPoolのドキュメントを参照してください。

"FabricPool を使用したストレージ階層の管理"

ONTAP S3をローカルのFabricPool大容量階層として使用するには、作成したバケットに基づいてオブジェクトストアを定義し、そのオブジェクトストアを高パフォーマンス階層のアグリゲートに接続してFabricPoolを作成する必要があります。

開始する前に

ONTAP S3サーバ名とバケット名を確認し、（パラメータを指定して）クラスタLIFを使用してS3サーバを作成しておく必要があります `-vserver Cluster`。

タスクの内容

オブジェクトストアの設定には、S3サーバとバケットの名前や認証要件など、ローカルの大容量階層に関する情報が格納されます。

作成したオブジェクトストア設定を別のオブジェクトストアまたはバケットに再関連付けしないでください。ローカル階層用に複数のバケットを作成できますが、1つのバケットに複数のオブジェクトストアを作成することはできません。

ローカルの大容量階層にはFabricPoolライセンスは必要ありません。

手順

1. ローカルの大容量階層用のオブジェクトストアを作成します。

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - は、 `-container-name`作成したS3バケットです。
   - パラメータは `-access-key`、ONTAP S3サーバへの要求を承認します。
   - パラメータ（シークレットアクセスキー）は、 `-secret-password`ONTAP S3サーバへの要求を認証します。
   - パラメータをに `false`設定すると、`ONTAP S3`の証明書のチェックを無効にできます `-is-certificate-validation-enabled`。

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. オブジェクトストアの設定情報を表示して確認します。

   ```
   storage aggregate object-store config show
   ```

3. オプション： "Inactive Data Reportingを使用してボリューム内のアクセス頻度の低いデータの量を確認する"。

   ボリューム内のアクセス頻度の低いデータの量を確認すると、FabricPoolのローカル階層化に使用するアグリゲートを決定するのに役立ちます。

4. オブジェクトストアをアグリゲートに接続します。

   `storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name`

   オプションを使用すると、FlexGroupボリュームのコンスティチュエントを含むアグリゲートを接続できます `allow-flexgroup true`。

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. オブジェクトストアの情報を表示し、接続したオブジェクトストアが使用可能であることを確認します。

   `storage aggregate object-store show`

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

関連情報

- "ストレージ集約オブジェクトストアアタッチ"
- "ストレージ集約オブジェクトストア構成の作成"
- "ストレージ集約オブジェクトストア構成表示"
- "ストレージ集約オブジェクトストア表示"

S3クライアントアプリケーションが**ONTAP S3**サーバにアクセスできるようにする

S3クライアントアプリケーションからONTAP S3サーバにアクセスするには、ONTAP S3管理者がS3ユーザに設定情報を提供する必要があります。

開始する前に

S3クライアントアプリケーションは、次のAWS署名バージョンを使用してONTAP S3サーバで認証できる必要があります。

- 署名バージョン4、ONTAP 9.8以降
- 署名バージョン2、ONTAP 9.11.1以降

これ以外の署名バージョンはONTAP S3ではサポートされません。

ONTAP S3管理者がS3ユーザを作成し、バケット ポリシーまたはオブジェクト ストレージ サーバ ポリシーで個々のユーザまたはグループ メンバーとしてアクセス権限を付与しておく必要があります。

S3クライアント アプリケーションがONTAP S3サーバ名を解決できるように、ONTAP S3管理者がS3サーバ

のサーバ名（FQDN）とLIFのIPアドレスを提供する必要があります。

タスクの内容

ONTAP S3バケットにアクセスするには、S3クライアントアプリケーションのユーザがONTAP S3管理者から提供された情報を入力します。

ONTAP 9.9.1以降では、ONTAP S3サーバで次のAWSクライアント機能がサポートされます。

- ユーザ定義のオブジェクト メタデータ

  PUT（またはPOST）を使用してオブジェクトを作成するときに、一連のキーと値のペアをメタデータとして割り当てることができます。オブジェクトに対してGET / HEAD処理が実行されると、システムのメタデータとともにユーザ定義のメタデータが返されます。

- オブジェクトのタグ付け

  オブジェクトの分類用に、キーと値のペアをタグとして割り当てることができます。メタデータとは異なり、タグはオブジェクトの作成とは別にREST APIを使用して作成および読み取られ、オブジェクトの作成時または作成後の任意の時点で実装されます。

> クライアントがタグ情報を取得および設定できるようにするには、 `GetObjectTagging` `DeleteObjectTagging`バケットポリシーまたはグループポリシーを使用して、およびを `PutObjectTagging`許可する必要があります。

詳細については、AWS S3のドキュメントを参照してください。

手順

1. S3サーバ名とCA証明書を入力して、S3クライアントアプリケーションをONTAP S3サーバで認証します。
2. 次の情報を入力して、S3クライアントアプリケーションでユーザを認証します。
   - S3サーバ名（FQDN）とバケット名
   - ユーザのアクセスキーとシークレットキー

ONTAP S3ストレージサービスレベル

ONTAP には、対応する最小パフォーマンス要因にマッピングされた事前定義されたストレージサービスが含まれています。

クラスタまたは SVM で実際に使用可能なストレージサービスは、 SVM 内のアグリゲートを構成するストレージのタイプによって決まります。

次の表に、定義済みのストレージサービスと対応する最小パフォーマンス要因を示します。

ストレージサービス	想定 **IOPS** （ **SLA** ）	最大 **IOPS** （ **SLO** ）	最小ボリューム **IOPS**	推定レイテンシ	想定 **IOPS** の適用
値	128/TB	512/TB	75	17 ミリ秒	AFF の場合：はい それ以外の場合：いいえ
パフォーマンス	TBあたり2、048	4096/TB	500	2ミリ秒	○
最高レベル	TBあたり6、144	12288/TB	1000	1 ミリ秒	○

次の表に、メディアまたはノードのタイプごとに使用可能なストレージサービスレベルを示します。

メディアまたはノード	使用可能なストレージサービスレベル
ディスク	値
仮想マシンディスク	値
ハイブリッド	値
大容量フラッシュ	値
ソリッドステートドライブ（ SSD ） - AFF 以外のドライブです	値
パフォーマンスが最適化されたフラッシュ - SSD （ AFF ）	卓越したパフォーマンス、価値

ONTAP S3バケット用のCross-Origin Resource Sharing（CORS）の設定

ONTAP 9 .16.1以降では、Cross-Origin Resource Sharing（CORS）を設定して、異なるドメインのクライアントWebアプリケーションがONTAPバケットにアクセスできるようにすることができます。これにより、Webブラウザを使用してバケットオブジェクトにセキュアにアクセスできるようになります。

CORSはHTTP上に構築されたフレームワークで、1つのWebページで定義されたスクリプトが別のドメインのサーバのリソースにアクセスできるようにします。このフレームワークは、ウェブセキュリティの初期の基盤である_same-origin policy_を安全にバイパスするために使用されます。主な概念と用語については、以下で説明します。

由来

原点は、リソースの場所とIDを正確に定義します。次の値の組み合わせで表されます。

- URIスキーム（プロトコル）
- ホスト名（ドメイン名またはIPアドレス）
- ポート番号

ここに起源の簡単な例があります。 `https://www.mycompany.com:8001`オリジンがCORSとともに使用される場合、要求を行っているクライアントを識別します。

same-originポリシー

same-origin policy（SOP）は、ブラウザベースのスクリプトに適用されるセキュリティの概念と制限です。このポリシーでは、Webページから最初にロードされたスクリプトが、両方のページが同じオリジンにある限り、別のページのデータにアクセスできます。この制限により、悪意のあるスクリプトが別のオリジンのページ内のデータにアクセスするのを防ぐことができます。

一般的な**CORS**のユースケース

CORSにはいくつかの一般的なユースケースがあります。ほとんどの場合、AJAXリクエスト、フォント、スタイルシート、スクリプトのロード、クロスドメイン認証など、クロスドメインアクセスの明確に定義されたインスタンスが関係します。CORSは、シングルページアプリケーション（SPA）の一部として実装することもできます。

HTTPヘッダー

CORSは、HTTP要求および応答に挿入されるヘッダーを使用して実装されます。たとえば、アクセス制御を実装し、メソッドやヘッダーなど、許可される操作を示す応答ヘッダーがいくつかあります。HTTP要求に_Origin_headerがあると、クロスドメイン要求として定義されます。オリジン値は、CORSサーバーが有効なCORS設定を見つけるために使用されます。

HTTPプリフライト要求

これは、特定のメソッドやヘッダーなど、サーバがCORSをサポートしているかどうかを最初に確認するためのオプションの要求です。応答に基づいて、CORS要求を完了することも、完了しないこともできます。

ONTAPハケツト

バケットは、明確に定義されたネームスペースに基づいて格納およびアクセスされるオブジェクトのコンテナです。ONTAPバケットには次の2種類があります。

- NASおよびS3プロトコルでアクセス可能なNASバケット
- S3プロトコルでのみアクセス可能なS3バケット

ONTAPでの**CORS**の実装

CORSは、ONTAP 9 .16.1以降のリリースではデフォルトで有効になっています。CORSは、アクティブにするSVMごとに設定する必要があります。

> ONTAPクラスタでCORSを無効にする管理オプションはありません。ただし、ルールを定義しないか、既存のルールをすべて削除することで、効果的に無効にすることができます。

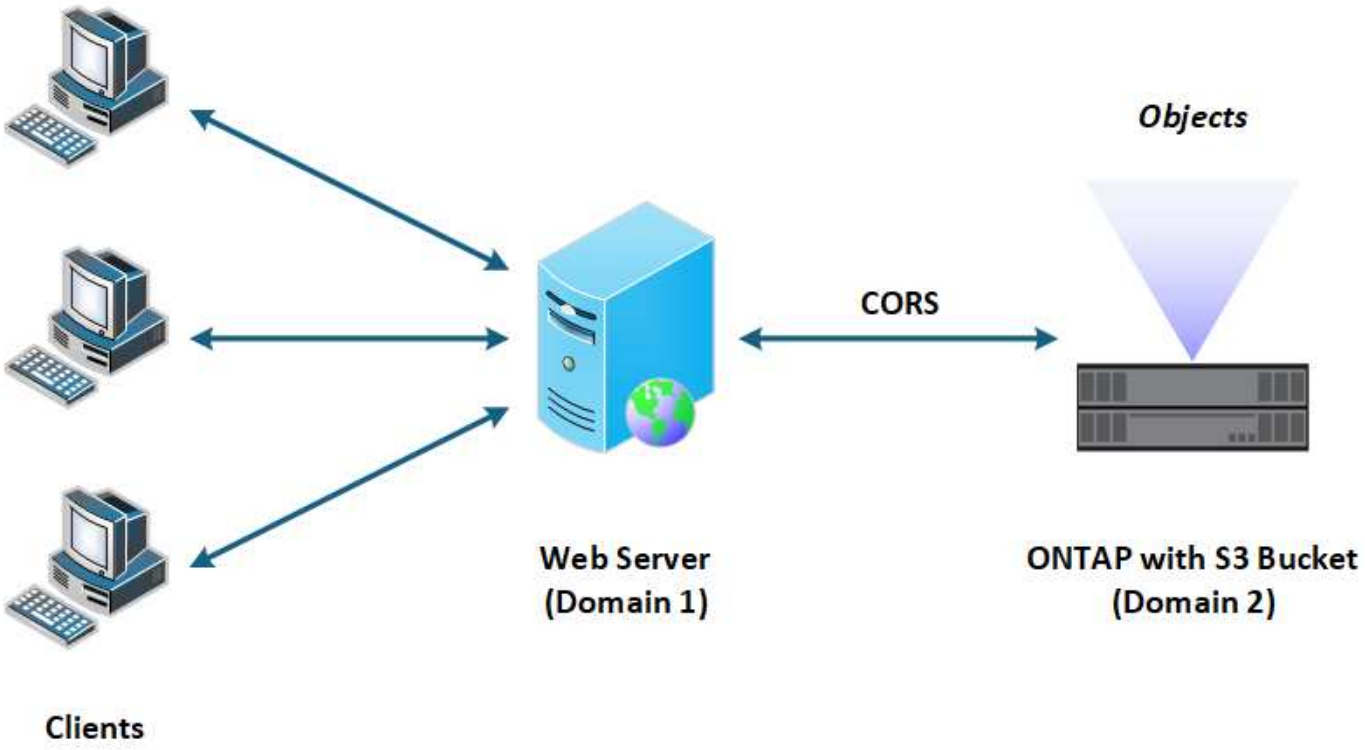
想定されるユースケース

ONTAP CORSの実装では、クロスドメインリソースアクセスのために、次のようないくつかのトポロジが可能になります。

- ONTAP S3バケット（同一または異なるSVMまたはクラスタ内）
- ONTAP NASバケット（同一または異なるSVMまたはクラスタ内）
- ONTAP S3バケットとNASバケット（同一または異なるSVMまたはクラスタ内）
- ONTAPバケットと外部ベンダーバケット
- 異なるタイムゾーンのバケット

概要

次の図は、CORSによってONTAP S3バケットへのアクセスを有効にする方法の概要を示しています。



CORSルールの定義

この機能をアクティブ化して使用するには、ONTAPでCORSルールを定義する必要があります。

設定アクション

ONTAPでは、次の3つの主要な設定ルールアクションがサポートされています。

- - 表示
- 作成
- 削除

ONTAPで定義されているCORSルールには、SVMとバケット、許可されているオリジン、メソッド、ヘッダーなど、いくつかのプロパティがあります。

管理オプション

ONTAPクラスタでCORSを管理する場合は、いくつかのオプションを使用できます。

ONTAPコマンドラインインターフェイス

CORSは、コマンドラインインターフェイスを使用して設定できます。詳細については、を参照してください CLIを使用したCORSの管理 。

ONTAP REST API

ONTAP REST APIを使用してCORSを設定できます。CORS機能をサポートする新しいエンドポイントは追加されていません。代わりに、次の既存のエンドポイントを使用できます。

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

詳細については、を "ONTAP自動化に関するドキュメント"参照してください。

S3 API

S3 APIを使用して、ONTAPバケットのCORS設定を作成および削除できます。S3クライアント管理者には、次のような十分なPrivilegesが必要です。

- アクセスキーまたはシークレットキーのクレデンシャル
- s3api経由のアクセスを許可するようにバケットに設定されたポリシー

アップグレードとリバート

CORSを使用してONTAP S3バケットにアクセスする場合は、いくつかの管理上の問題に注意する必要があります。

アップグレード

CORS機能は、すべてのノードを9.16.1にアップグレードするとサポートされます。混在モードのクラスタでは、この機能は有効なクラスタバージョン（ECV）が9.16.1以降の場合にのみ使用できます。

リバート

ユーザ側では、クラスタのリバートを続行する前に、すべてのCORS設定を削除する必要があります。内部的には、すべてのCORSデータベースが削除されます。これらのデータ構造をクリアして元に戻すコマンドを実行するように求められます。

CLIを使用したCORSの管理

ONTAP CLIを使用してCORSルールを管理できます。主な操作は以下のとおりです。CORSコマンドを発行するには、ONTAP * admin *権限レベルである必要があります。

作成

コマンドを使用して、CORSルールを定義できます `vserver object-store-server bucket cors-rule create`。の詳細については `vserver object-store-server bucket cors-rule create`、を"ONTAPコマンド リファレンス"参照してください。

パラメータ

ルールの作成に使用するパラメータを次に示します。

パラメータ	説明
`vserver`	ルールを作成するオブジェクトストアサーババケットをホストするSVM（SVM）の名前を指定します。
`bucket`	ルールを作成するオブジェクトストアサーバのバケットの名前。
`index`	ルールを作成するオブジェクトストアサーババケットのインデックスを指定するオプションのパラメータ。
`rule id`	オブジェクトストアサーババケットルールの一意の識別子。
`allowed-origins`	クロスオリジンリクエストの発信元を許可するオリジンのリスト。
`allowed-methods`	クロスオリジン要求で許可されるHTTPメソッドのリスト。
`allowed-headers`	クロスオリジン リクエストで許可される HTTP ヘッダーのリスト。
`expose-headers`	お客様がアプリケーションからアクセスできるCORS応答で送信される追加ヘッダーのリスト。
`max-age-in-seconds`	ブラウザが特定のリソースのプリフライトレスポンスをキャッシュする時間を指定するオプションのパラメータ。

例

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

- 表示

コマンドを使用すると、現在のルールとその内容のリストを表示できます `vserver object-store-server bucket cors-rule show`。の詳細については `vserver object-store-server bucket cors-rule show`、を"ONTAPコマンド リファレンス"参照してください。

パラメータを含める `-instance`と、各ルールに表示されるデータが展開されます。必要なフィールドを指定することもできます。

例

```
server object-store-server bucket cors-rule show -instance
```

削除

CORSルールのインスタンスを削除するには、deleteコマンドを使用します。ルールの値が必要な `index`ため、この操作は次の2つのステップで実行されます。

1. コマンドを実行し `show`てルールを表示し、そのインデックスを取得します。
2. インデックス値を使用してDELETEを発行します。

例

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

変更

既存のCORSルールを変更するCLIコマンドはありません。ルールを変更するには、次の手順を実行する必要があります。

1. 既存のルールを削除します。
2. 必要なオプションを指定して新しいルールを作成します。

SnapMirror S3でバケットを保護

ONTAP SnapMirror S3の詳細

ONTAP 9 .10.1以降では、SnapMirrorのミラーリングとバックアップの機能を使用してONTAP S3オブジェクトストアのバケットを保護できます。標準のSnapMirrorとは異なり、SnapMirror S3では、AWS S3などのNetApp以外のデスティネーションへのミラーリングとバックアップが可能です。

SnapMirror S3では、ONTAP S3バケットから次のデスティネーションへのアクティブなミラー階層とバックアップ階層がサポートされます。

ターゲット	アクティブなミラーとテイクオーバーのサポート	バックアップとリストアのサポート
ONTAP S3 • 同じSVM内のバケット • 同じクラスタの異なるSVMのバケット • 異なるクラスタのSVM内のバケット	○	○

ターゲット	アクティブなミラーとテイクオーバーのサポート	バックアップとリストアのサポート
StorageGRID	いいえ	○
AWS S3	いいえ	○
Cloud Volumes ONTAP for Azure	○	○
Cloud Volumes ONTAP for AWS	○	○
Cloud Volumes ONTAP for Google Cloud	○	○

ONTAP S3サーバ上の既存のバケットを保護することも、新しく作成したバケットですぐにデータ保護を有効にすることもできます。

SnapMirror S3の要件

- ONTAPのバージョン

  ソースクラスタとデスティネーションクラスタでONTAP 9 .10.1以降が実行されている必要があります。

  SnapMirror S3はMetroCluster構成ではサポートされません。

- ライセンス

  のアクセスを提供するには、ONTAPソースシステムとデスティネーションシステムに次のライセンスがソフトウェアスイートに含まれている"ONTAP One"必要があります。

  - ONTAP S3プロトコルとストレージ
  - 他のNetAppオブジェクトストアターゲット（ONTAP S3、StorageGRID、Cloud Volumes ONTAP）をターゲットにするためのSnapMirror S3
  - AWS S3などのサードパーティのオブジェクトストアをターゲットとするSnapMirror S3（で使用可能"ONTAP One互換バンドル"）
  - クラスタでONTAP 9.10.1が実行されている場合は、が"FabricPool ライセンス"必要です。

- ONTAP S3
  - ONTAP S3サーバでソースとデスティネーションのSVMが実行されている必要があります。
  - TLSアクセス用のCA証明書をS3サーバをホストするシステムにインストールすることを推奨しますが、必須ではありません。
    - S3サーバの証明書への署名に使用したCA証明書が、S3サーバをホストするクラスタの管理Storage VMにインストールされている必要があります。
    - 自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。
    - ソースまたはデスティネーションのStorage VMがHTTPSをリスンしていない場合は、CA証明書をインストールする必要はありません。
- ピアリング（ONTAP S3ターゲット用）
  - クラスタ間LIFが設定されている（リモートONTAPターゲット用）必要があり、ソースクラスタとデスティネーションクラスタのクラスタ間LIFが、ソースとデスティネーションのS3サーバのデータLIFに接続できるようになります。

- ソースクラスタとデスティネーションクラスタがピア関係にある（リモートONTAPターゲットの場合）。
- ソースとデスティネーションのStorage VMがピア関係にある（すべてのONTAPターゲットに対して）。

- SnapMirrorポリシー
  - すべてのSnapMirror S3関係にS3固有のSnapMirrorポリシーが必要ですが、複数の関係に同じポリシーを使用できます。
  - 独自のポリシーを作成するか、次の値を含むデフォルトの * Continuous * ポリシーをそのまま使用できます。
    - Throttle（スループット/帯域幅の上限）-無制限。
    - 目標復旧時点までの時間： 1 時間（ 3600 秒）

> 2つのS3バケットがSnapMirror関係にある場合、オブジェクトの現在のバージョンが期限切れになる（削除される）ようにライフサイクルポリシーが設定されていると、同じ処理がパートナーバケットにレプリケートされることに注意してください。これは、パートナーバケットが読み取り専用またはパッシブの場合でも同様です。

- rootユーザキーSnapMirror S3関係にはStorage VMのrootユーザアクセスキーが必要です。ONTAPではデフォルトで割り当てられません。SnapMirror S3関係を初めて作成する際は、ソースとターゲットの両方のストレージVMにキーが存在することを確認し、存在しない場合は再生成する必要があります。再生成が必要な場合は、アクセスキーとシークレットキーのペアを使用するすべてのクライアントとすべてのSnapMirrorオブジェクトストア設定が新しいキーに更新されていることを確認する必要があります。

S3サーバの設定については、次のトピックを参照してください。

- "Storage VMでS3サーバを有効にする"
- "ONTAP S3の設定プロセスの概要"

クラスタとStorage VMのピアリングについては、次のトピックを参照してください。

- "ミラーリングとバックアップの準備（System Manager、手順1~6）"
- "クラスタとSVMのピアリング（CLI）"

サポートされる**SnapMirror**関係

SnapMirror S3は、ファンアウト関係とカスケード関係をサポートしています。概要については、 "ファンアウト構成およびカスケード構成のデータ保護" 。

SnapMirror S3は、ファンイン環境（複数のソースバケットと1つのデスティネーションバケット間のデータ保護関係）をサポートしていません。SnapMirror S3では、複数のクラスタから単一のセカンダリクラスタへの複数のバケットミラーをサポートできますが、各ソースバケットにセカンダリクラスタ上の専用のデスティネーションバケットが必要です。

SnapMirror S3はMetroCluster環境ではサポートされていません。

S3バケットへのアクセスを制御

新しいバケットを作成するときに、ユーザとグループを作成してアクセスを制御できます。

SnapMirror S3はソースバケットからデスティネーションバケットにオブジェクトをレプリケートしますが、ユーザ、グループ、およびポリシーをソースオブジェクトストアからデスティネーションオブジェクトストアにレプリケートすることはありません。

フェイルオーバー時にクライアントがデスティネーションバケットにアクセスできるように、デスティネーションオブジェクトストアでユーザ、グループポリシー、権限などのコンポーネントを設定する必要があります。

ユーザがデスティネーションクラスタで作成されたときにソースキーを手動で指定していれば、ソースユーザとデスティネーションユーザで同じアクセスキーとシークレットキーを使用できます。例：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

詳細については、次のトピックを参照してください。

- "S3のユーザとグループの追加（System Manager）"
- "S3ユーザの作成（CLI）"
- "S3グループの作成と変更（CLI）"

SnapMirror S3で**S3**オブジェクトのロックとバージョン管理を使用

オブジェクトロックおよびバージョン管理が有効なONTAPバケットではSnapMirror S3を使用できますが、次の点を考慮する必要があります。

- オブジェクトロックが有効なソースバケットをレプリケートするには、デスティネーションバケットでもオブジェクトロックが有効になっている必要があります。また、ソースとデスティネーションの両方でバージョン管理を有効にする必要があります。これにより、両方のバケットでデフォルトの保持ポリシーが異なる場合にデスティネーションバケットに削除がミラーリングされる問題を回避できます。
- S3 SnapMirrorでは、オブジェクトの履歴バージョンはレプリケートされません。オブジェクトの現在のバージョンのみがレプリケートされます。

Object Lockedオブジェクトがデスティネーションバケットにミラーリングされると、元の保持期限が維持されます。ロック解除されたオブジェクトがレプリケートされた場合、デスティネーションバケットのデフォルトの保持期間が適用されます。例：

- バケットAのデフォルトの保持期間は30日、バケットBのデフォルトの保持期間は60日です。バケットAからバケットBにレプリケートされたオブジェクトは、デフォルトの保持期間であるバケットBよりも短い場合でも、30日間の保持期間が維持されます。
- バケットAにはデフォルトの保持期間はなく、バケットBにはデフォルトの保持期間が60日です。ロック解除されたオブジェクトがバケットAからバケットBにレプリケートされると、60日間の保持期間が適用されます。バケットAでオブジェクトが手動でロックされている場合、バケットBにレプリケートされても元の保持期間が維持されます。
- バケットAのデフォルトの保持期間は30日ですが、バケットBにはデフォルトの保持期間はありません。バケットAからバケットBにレプリケートされたオブジェクトは30日間の保持期間が維持されます。

リモートクラスタでのミラーとバックアップの保護

リモートクラスタの新しい**ONTAP S3**バケットのミラー関係を作成

新しい S3 バケットを作成すると、リモート クラスター上の SnapMirror S3 宛先にすぐに保護できます。

タスクの内容

タスクは、ソースシステムとデスティネーションシステムの両方で実行する必要があります。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件が完了している。
- ソースクラスタとデスティネーションクラスタの間にピア関係が確立され、ソースとデスティネーションのStorage VMの間にピア関係が確立されています。
- CA証明書は、ソースVMとデスティネーションVMに必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMの最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. [設定]タブで、* S3 *タイル内をクリックします 。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します。
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。すでに存在するキーを再生成しないでください。
2. ソースとデスティネーションの両方のStorage VMで、Storage VMを編集してユーザを追加し、グループにユーザを追加します。

   [ストレージ]>[Storage VM]をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。

   詳細については、を参照してください "S3ユーザとグループの追加" 。
3. ソース クラスターで、既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。権限の検証はオプションですが、推奨されます。
   b. 名前を入力し、 Storage VM を選択してサイズを入力し、 * その他のオプション * をクリックします。
   c. [**Permissions**] で、 [**Add**] をクリックします。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-次の値が表示されていることを確認します。

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - リソース-デフォルト値または必要なその他の値を使用します `(bucketname, bucketname/*)`。

        これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの

管理"。

d. [**Protection**] で、 **[Enable SnapMirror (ONTAP or Cloud)**] をオンにします。次に、次の値を入力します。

- デスティネーション
  - * ターゲット： ONTAP システム *
  - * cluster * ：リモートクラスタを選択します。
  - * Storage VM * ：リモートクラスタの Storage VM を選択します。
  - * S3 サーバ CA 証明書 * ： _source_certificate の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書： * destination_certificate の内容をコピーして貼り付けます。

5. チェック * 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
6. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
7. [保存（ Save ）] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage VMに作成された新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にできます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。

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

   rootユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   すでに存在するキーを再生成しないでください。

2. ソースとデスティネーションの両方のSVMにバケットを作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. ソースとデスティネーションの両方のSVMでデフォルトのバケットポリシーにアクセスルールを追加します。

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

   例

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. ソース SVM で、既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - Type `continuous` - SnapMirror S3関係の唯一のポリシータイプ（必須）。
   - `-rpo`-目標復旧時点の時間を秒単位で指定します（オプション）。
   - `-throttle`-スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. ソースクラスタとデスティネーションクラスタの管理SVMにCAサーバ証明書をインストールします。

   a. ソースクラスタで、*destination_S3*サーバ証明書に署名した*CA*証明書をインストールします。
      security certificate install -type server-ca -vserver _src_admin_svm -cert -name dest_server_certificate

   b. デスティネーションクラスタで、*source_S3*サーバ証明書に署名した*CA*証明書をインストールします。
      security certificate install -type server-ca -vserver _dest_admin_svm -cert-name src_server_certificate

外部のCAベンダーによって署名された証明書を使用している場合は、ソースとデスティネーションの管理SVMに同じ証明書をインストールします。

の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

6. ソース SVM で、SnapMirror S3 関係を作成します。

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

   例

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
   test-policy
   ```

7. ミラーリングがアクティブであることを確認します。
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "スナップミラー作成"
- "snapmirror policy create"
- "snapmirror show"

リモートクラスタの既存の**ONTAP S3**バケットのミラー関係を作成

既存のS3バケットの保護はいつでも開始できます。たとえば、S3の設定をONTAP 9 10.1より前のリリースからアップグレードした場合などです。

タスクの内容

タスクはソースクラスタとデスティネーションクラスタの両方で実行する必要があります。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件が完了している。
- ソースクラスタとデスティネーションクラスタの間にピア関係が確立され、ソースとデスティネーションのStorage VMの間にピア関係が確立されています。
- CA証明書は、ソースVMとデスティネーションVMに必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

手順

ミラー関係は、System ManagerまたはONTAP CLIを使用して作成できます。

System Manager

1. このStorage VMの最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。
   a. [ストレージ]>[Storage VM]*を選択し、Storage VMを選択します。
   b. [設定]タブで、* S3 *タイル内をクリックします 。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します。
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。*すでに存在するキーを再生成しないでください。
2. ソースとデスティネーションの両方のStorage VMに既存のユーザとグループが存在し、正しいアクセス権があることを確認します。**[ストレージ]>[Storage VM]***を選択し、**Storage VM**を選択して[設定]タブを選択します。最後に、 S3 タイルを探し 、を選択して Users タブを選択し、 Groups *タブを選択して、ユーザとグループのアクセス設定を表示します。

   詳細については、を参照してください "S3ユーザとグループの追加" 。
3. ソース クラスターで、既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   a. [保護]>[概要]を選択し、[ローカルポリシー設定]*をクリックします。
   b. の横にあるを選択し 、[追加]*をクリックします。
   c. ポリシーの名前と説明を入力します。
   d. ポリシースコープ（クラスタまたはSVM）を選択します。
   e. SnapMirror S3関係の場合は*[Continuous]*を選択します。
   f. スロットル値および * 目標復旧時点 * 値を入力します。
4. 既存のバケットのバケットアクセスポリシーが引き続きニーズを満たしていることを確認します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、保護するバケットを選択します。
   b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
      - * 主な内容と効果 * ：ユーザーグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション：次の値が表示されていることを確認します。

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - リソース:デフォルト値または必要なその他の値を使用し `(*bucketname, bucketname*/*)` ます。

        これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの管理"。
5. SnapMirror S3保護で既存のバケットを保護します。
   a. [* Storage * > * Buckets] をクリックして、保護するバケットを選択します。

b. [*Protect] をクリックして、次の値を入力します。

- デスティネーション
  - * ターゲット * ： ONTAP システム
  - * cluster * ：リモートクラスタを選択します。
  - * Storage VM * ：リモートクラスタの Storage VM を選択します。
  - * S3 サーバ CA 証明書 * ： _source_certificate の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書 * ： _destination_certificate の内容をコピーして貼り付けます。

6. チェック * 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
7. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存（ Save ）] をクリックします。既存のバケットがデスティネーションStorage VMの新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にできます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにrootユーザキーが存在することを確認し、存在しない場合は再生成します `vserver object-store-server user show`。+ rootユーザのアクセスキーがあることを確認します。存在しない場合は、「 `vserver object-store-server user regenerate-keys -vserver svm_name -user root`+ Do not regenerate the key if one already exists」と入力します。
2. ミラーターゲットとして使用するデスティネーションSVMにバケットを作成します。

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケットポリシーのアクセスルールが正しいことを確認します。

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   ```

`-principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

例

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. ソース SVM で、既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous`–SnapMirror S3関係の唯一のポリシータイプ（必須）。
   - `-rpo`–目標復旧時点の時間を秒単位で指定します（オプション）。
   - `-throttle`–スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. ソースクラスタとデスティネーションクラスタの管理SVMにCA証明書をインストールします。

   a. ソースクラスタで、*destination_S3*サーバ証明書に署名した*CA*証明書をインストールします。*security certificate install -type server-ca -vserver _src_admin_svm -cert -name dest_server_certificate*

   b. デスティネーションクラスタで、*source_S3*サーバ証明書に署名した*CA*証明書をインストールします *security certificate install -type server-ca -vserver _dest_admin_svm -cert-name src_server_certificate*。+外部のCAベンダーが署名した証明書を使用している場合は、ソースとデスティネーションの管理SVMに同じ証明書をインストールします。

   の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

6. ソース SVM で、SnapMirror S3 関係を作成します。

   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

7. ミラーリングがアクティブであることを確認します。
`snapmirror show -policy-type continuous -fields status`

関連情報

- "スナップミラー作成"
- "snapmirror policy create"
- "snapmirror show"

リモートクラスタのデスティネーション**ONTAP S3**バケットからテイクオーバーする

ソースバケットのデータが使用できなくなった場合は、SnapMirror関係を解除してデスティネーションバケットを書き込み可能にし、データの提供を開始できます。

タスクの内容

テイクオーバー処理が実行されると、ソースバケットが読み取り専用に変換され、元のデスティネーションバケットが読み取り/書き込みに変換されるため、SnapMirror S3関係が反転されます。

無効にしたソースバケットが再び使用可能になると、SnapMirror S3は2つのバケットの内容を自動的に再同期します。Volume SnapMirror環境の場合のように、関係を明示的に再同期する必要はありません。

テイクオーバー処理はリモートクラスタから開始する必要があります。

SnapMirror S3はソースバケットからデスティネーションバケットにオブジェクトをレプリケートしますが、ユーザ、グループ、およびポリシーをソースオブジェクトストアからデスティネーションオブジェクトストアにレプリケートすることはありません。

フェイルオーバー時にクライアントがデスティネーションバケットにアクセスできるように、デスティネーションオブジェクトストアでユーザ、グループポリシー、権限などのコンポーネントを設定する必要があります。

ユーザがデスティネーションクラスタで作成されたときにソースキーを手動で指定していれば、ソースユーザとデスティネーションユーザで同じアクセスキーとシークレットキーを使用できます。例：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

System Manager

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. [保護]>[関係]をクリックし、[SnapMirror S3]*を選択します。
2. をクリックし、**[フェイルオーバー]***を選択し、[フェイルオーバー]*をクリックします。

CLI

1. デスティネーションバケットのフェイルオーバー処理を開始します。
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー処理のステータスを確認します。
   `snapmirror show -fields status`

   例

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

関連情報

- "S3のユーザとグループの追加（System Manager）"
- "S3ユーザの作成（CLI）"
- "S3グループの作成と変更（CLI）"
- "スナップミラーフェイルオーバーの開始"
- "snapmirror show"

リモートクラスタのデスティネーション**SVM**から**ONTAP S3**バケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、デスティネーションバケットからオブジェクトをリストアすることでデータを再取り込みできます。

タスクの内容

デスティネーションバケットは、既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、デスティネーションバケットの使用済み論理スペースよりも大きくする必要があります。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はリモートクラスタから開始する必要があります。

System Manager

バックアップしたデータをリストアします。

1. [保護]>[関係]をクリックし、[SnapMirror S3]*を選択します。
2. をクリックし ⋮ 、*[リストア]*を選択します。
3. 「 * ソース * 」で、「 * 既存バケット」（デフォルト）または「 * 新規バケット」を選択します。
   - 既存の Bucket * （デフォルト）にリストアするには、次の操作を実行します。
     - クラスタとStorage VMを選択して既存のバケットを検索します。
     - 既存のバケットを選択します。
     - destination_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
   - 新しいバケットへのリストアを実行するには、次の値を入力します。
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンスサービスレベル。詳細については、を参照してください "ストレージサービスレベル" 。
     - destination_S3 サーバ CA 証明書の内容。
4. 「 * Destination * 」の下にある _source_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
5. [保護] 、 [関係] の順にクリックして、復元の進行状況を監視します。

ロックされたバケットの復元

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックバケットをデスティネーションとして選択できます。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、元のバケットのオブジェクトロックモードと保持期間がレプリケートされます。新しいバケットに対して別のロック保持期間を定義することもできます。この保持期間は、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：バケットでオブジェクトロックが有効になっていない場合でも、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

CLI

1. リストア用の新しいデスティネーションバケットを作成します。詳細については、を参照してください "新しいONTAP S3バケット用のクラウドバックアップ関係を作成する"。
2. デスティネーションバケットのリストア処理を開始します。
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*

例

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

の詳細については `snapmirror restore`、を"ONTAPコマンド リファレンス"参照してください。

ローカルクラスタでのミラーとバックアップの保護

ローカルクラスタの新しい**ONTAP S3**バケットのミラー関係を作成する

新しいS3バケットを作成すると、同じクラスタ内のSnapMirror S3宛先にすぐに保護できます。データは、ソースとは異なるストレージVMまたは同じストレージVM内のバケットにミラーリングできます。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件が完了している。
- ソースとデスティネーションのStorage VMの間にピア関係が確立されている。
- CA証明書は、ソースVMとデスティネーションVMに必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMの最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. [設定]タブで、[S3]タイル内をクリックし ます。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。すでに存在するキーを再生成しないでください。
2. ソースとデスティネーションの両方のStorage VMで、Storage VMを編集してユーザを追加します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。

   詳細については、を参照してください "S3ユーザとグループの追加" 。
3. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   a. [保護]>[概要]をクリックし、[ローカルポリシー設定]*をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、 Storage VM を選択してサイズを入力し、 * その他のオプション * をクリックします。
   c. [**Permissions**] で、 [**Add**] をクリックします。権限の検証はオプションですが、推奨されます。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-次の値が表示されていることを確認します。

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - リソース-デフォルト値または必要なその他の値を使用します。(`bucketname, bucketname/*`)

        これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの管理"。
   d. [**Protection**] で、 **[Enable SnapMirror (ONTAP or Cloud)]** をオンにします。次に、次の値を入

力します。

- デスティネーション
  - * ターゲット * ： ONTAP システム
  - * cluster * ：ローカルクラスタを選択します。
  - * Storage VM *：ローカルクラスタのStorage VMを選択します。
  - * S3 サーバ CA 証明書 * ：ソース証明書の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書 * ：デスティネーション証明書の内容をコピーして貼り付けます。

5. チェック * 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
6. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
7. [保存（ Save ）] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage VMに作成された新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にできます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。
   ```
   vserver object-store-server user show
   ```

   rootユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。
   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   すでに存在するキーを再生成しないでください。

2. ソースとデスティネーションの両方のSVMにバケットを作成します。

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
   ```

3. ソースとデスティネーションの両方のSVMでデフォルトのバケットポリシーにアクセスルールを追加します。

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

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous`–SnapMirror S3関係の唯一のポリシータイプ（必須）。
   - `-rpo`–目標復旧時点の時間を秒単位で指定します（オプション）。
   - `-throttle`–スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 管理SVMにCAサーバ証明書をインストールします。

   a. *source_S3*サーバの証明書に署名した*CA*証明書を管理*SVM*にインストールします。
      security certificate install -type server-ca -vserver _admin_svm -cert -name src_server_certificate

   b. *destination_S3*サーバの証明書に署名した*CA*証明書を管理*SVM*にインストールします
      security certificate install -type server-ca -vserver _admin_svm -cert -name dest_server_certificate。+外部のCAベンダーが署名した証明書を使用する場合は、管理SVMにこの証明書をインストールするだけです。

      の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

6. SnapMirror S3 関係を作成します。
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

7. ミラーリングがアクティブであることを確認します。
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "スナップミラー作成"
- "snapmirror policy create"
- "snapmirror show"

ローカルクラスタの既存の**ONTAP S3**バケットのミラー関係を作成する

S3設定をONTAP 9 .10.1より前のリリースからアップグレードした場合など、同じクラスタ上の既存のS3バケットの保護はいつでも開始できます。データは、ソースと同じStorage VMまたは別のStorage VMのバケットにミラーリングできます。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件が完了している。
- ソースとデスティネーションのStorage VMの間にピア関係が確立されている。
- CA証明書は、ソースVMとデスティネーションVMに必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMの最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. [設定]タブで、* S3 *タイル内をクリックします 。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します。
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。キーがすでに存在する場合は再生成しない
2. ソースとデスティネーションの両方のStorage VMに既存のユーザとグループが存在し、正しいアクセス権があることを確認します。**[ストレージ]>[Storage VM]***を選択し、**Storage VM**を選択して、[設定]タブを選択します。最後に、 S3 タイルを探し 、を選択して Users タブを選択し、 Groups *タブを選択して、ユーザとグループのアクセス設定を表示します。

   詳細については、を参照してください "S3ユーザとグループの追加" 。
3. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. 既存のバケットのバケットアクセスポリシーが引き続きニーズを満たしていることを確認します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、保護するバケットを選択します。
   b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-次の値が表示されていることを確認します。

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - リソース-デフォルト値または必要なその他の値を使用します *(bucketname, bucketname/*)*。

        これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの管理"。
5. SnapMirror S3で既存のバケットを保護します。
   a. [* Storage * > * Buckets] をクリックして、保護するバケットを選択します。

b. [*Protect] をクリックして、次の値を入力します。

- デスティネーション
  - * ターゲット * ： ONTAP システム
  - * cluster * ：ローカルクラスタを選択します。
  - * Storage VM * ：同じ Storage VM または別の Storage VM を選択します。
  - * S3 サーバ CA 証明書 * ： _source_certificate の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書 * ： _destination_certificate の内容をコピーして貼り付けます。

6. チェック * 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
7. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存（ Save ）] をクリックします。既存のバケットがデスティネーションStorage VMの新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にできます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにrootユーザキーが存在することを確認し、存在しない場合は再生成します。
   `vserver object-store-server user show`

   rootユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   すでに存在するキーを再生成しないでください。

2. ミラーターゲットとして使用するデスティネーションSVMにバケットを作成します。

   `vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケットポリシーへのアクセスルール

が正しいことを確認します。

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

例

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo _integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous`–SnapMirror S3関係の唯一のポリシータイプ（必須）。
   - `-rpo`–目標復旧時点の時間を秒単位で指定します（オプション）。
   - `-throttle`–スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 管理SVMにCAサーバ証明書をインストールします。

   a. *source_S3*サーバの証明書に署名した*CA*証明書を管理*SVM*にインストールします。
   security certificate install -type server-ca -vserver _admin_svm -cert -name src_server_certificate

   b. *destination_S3*サーバの証明書に署名した*CA*証明書を管理*SVM*にインストールします
   security certificate install -type server-ca -vserver _admin_svm -cert -name dest_server_certificate。+外部のCAベンダーが署名した証明書を使用する場合は、管理SVMにこの証明書をインストールするだけです。

   の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

6. SnapMirror S3 関係を作成します。
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy`

policy_name]

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

7. ミラーリングがアクティブであることを確認します。
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "スナップミラー作成"
- "snapmirror policy create"
- "snapmirror show"

ローカルクラスタのデスティネーション**ONTAP S3**バケットからテイクオーバーする

ソースバケットのデータが使用できなくなった場合は、SnapMirror関係を解除してデスティネーションバケットを書き込み可能にし、データの提供を開始できます。

タスクの内容

テイクオーバー処理が実行されると、ソースバケットが読み取り専用に変換され、元のデスティネーションバケットが読み取り/書き込みに変換されるため、SnapMirror S3関係が反転されます。

無効にしたソースバケットが再び使用可能になると、SnapMirror S3は2つのバケットの内容を自動的に再同期します。標準のVolume SnapMirror環境のように、関係を明示的に再同期する必要はありません。

デスティネーションバケットがリモートクラスタにある場合は、リモートクラスタからテイクオーバー処理を開始する必要があります。

System Manager

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. [保護]>[関係]をクリックし、[SnapMirror S3]*を選択します。
2. をクリックし、**[**フェイルオーバー**]***を選択し、[フェイルオーバー]*をクリックします。

CLI

1. デスティネーションバケットのフェイルオーバー処理を開始します。
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー処理のステータスを確認します。
   `snapmirror show -fields status`

例

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

関連情報

- "スナップミラーフェイルオーバーの開始"
- "snapmirror show"

ローカルクラスタのデスティネーション**SVM**から**ONTAP S3**バケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、デスティネーションバケットからオブジェクトをリストアすることでデータを再取り込みできます。

タスクの内容

デスティネーションバケットは、既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、デスティネーションバケットの使用済み論理スペースよりも大きくする必要があります。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はローカルクラスタから開始する必要があります。

System Manager

バックアップデータをリストアします。

1. [* 保護] 、 [関係] の順にクリックし、バックアップを選択します。
2. をクリックし ⋮ 、*[リストア]*を選択します。
3. 「 * ソース * 」で、「 * 既存バケット」（デフォルト）または「 * 新規バケット」を選択します。
   - 既存の Bucket * （デフォルト）にリストアするには、次の操作を実行します。
     - クラスタとStorage VMを選択して既存のバケットを検索します。
     - 既存のバケットを選択します。
4. デスティネーションのS3サーバCA証明書の内容をコピーして貼り付けます。
   - 新しいバケットへのリストアを実行するには、次の値を入力します。
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンスサービスレベル。詳細については、を参照してください "ストレージサービスレベル" 。
     - デスティネーションS3サーバCA証明書の内容。
5. 「 * Destination * 」の下にあるソース S3 サーバ CA 証明書の内容をコピーして貼り付けます。
6. ［ * 保護 * ］ > ［ 関係 ］ の順にクリックして、リストアの進行状況を監視します。

ロックされたバケットの復元

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックバケットをデスティネーションとして選択できます。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、元のバケットのオブジェクトロックモードと保持期間がレプリケートされます。新しいバケットに対して別のロック保持期間を定義することもできます。この保持期間は、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：バケットでオブジェクトロックが有効になっていない場合でも、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

CLI

1. オブジェクトを新しいバケットにリストアする場合は、新しいバケットを作成します。詳細については、を参照してください "新しいONTAP S3バケット用のクラウドバックアップ関係を作成する"。
2. デスティネーションバケットのリストア処理を開始します。
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

例

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

の詳細については `snapmirror restore`、を"ONTAPコマンド リファレンス"参照してください。

クラウドターゲットを使用したバックアップ保護

ONTAP SnapMirror S3のクラウドターゲットの関係の要件

ソースとターゲットの環境が、クラウドターゲットに対するSnapMirror S3バックアップ保護の要件を満たしていることを確認します。

データバケットにアクセスするには、オブジェクトストアプロバイダとの有効なアカウントクレデンシャルが必要です。

クラスタをクラウドオブジェクトストアに接続する前に、クラスタ間LIFとIPspaceをクラスタに設定しておく必要があります。ローカルストレージからクラウドオブジェクトストアにデータをシームレスに転送できるように、各ノードにクラスタ間LIFを作成する必要があります。

StorageGRIDターゲットについて、次の情報を確認しておく必要があります。

- サーバ名（完全修飾ドメイン名（FQDN）またはIPアドレスで指定）
- バケット名。既存のバケットを指定する必要があります。
- アクセスキー
- シークレットキー

さらに、StorageGRIDサーバ証明書に署名するために使用されるCA証明書は、ONTAP S3クラスタの管理ストレージVMにインストールする必要があります。 `security certificate install`指示。詳細については、「"CA証明書をインストールしています"StorageGRIDを使用する場合」を参照してください。

AWS S3ターゲットについて、次の情報を確認しておく必要があります。

- サーバ名（完全修飾ドメイン名（FQDN）またはIPアドレスで指定）
- バケット名。既存のバケットを指定する必要があります。
- アクセスキー
- シークレットキー

ONTAPクラスタの管理Storage VMのDNSサーバが、FQDN（使用する場合）をIPアドレスに解決できる必要があります。

関連情報

- "セキュリティ証明書のインストール"

新しい**ONTAP S3**バケット用のクラウドバックアップ関係を作成する

新しい S3 バケットを作成すると、オブジェクト ストア プロバイダー (StorageGRID システムまたは Amazon S3 デプロイメント) 上の SnapMirror S3 ターゲット バケットにすぐにバックアップできます。

開始する前に

- オブジェクトストアプロバイダの有効なアカウントクレデンシャルと設定情報が必要です。
- ソースシステムにクラスタ間ネットワークインターフェイスとIPspaceが設定されている。
- •ソース Storage VM の DNS 設定でターゲットの FQDN を解決できる必要があります。

System Manager

1. Storage VMを編集してユーザを追加し、グループにユーザを追加します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**をクリックして[設定]をクリックし、 S3 * の下をクリックし ます。

      詳細については、を参照してください "S3ユーザとグループの追加" 。
2. ソースシステムにクラウドオブジェクトストアを追加します。
   a. [保護（ Protection ）] > [概要（ Overview ）] * をクリックし、 [クラウドオブジェクトストア（ Cloud Object Stores ）] を
   b. [* 追加] をクリックし、 [* Amazon S3 *] または [* StorageGRID *] を選択します。
   c. 次の値を入力します。
      - クラウド オブジェクト ストアの名前
      - URLの形式（パスまたは仮想ホスト）
      - Storage VM（S3対応）
      - オブジェクト ストアのサーバ名（FQDN）
      - オブジェクト ストアの証明書
      - アクセスキー
      - シークレットキー
      - コンテナ（バケット）名
3. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   a. [保護]>[概要]をクリックし、[ローカルポリシー設定]*をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、 Storage VM を選択してサイズを入力し、 * その他のオプション * をクリックします。
   c. [**Permissions**] で、 [**Add**] をクリックします。権限の検証はオプションですが、推奨されます。
      - * Principal および Effect * ：ユーザーグループの設定に対応する値を選択するか、デフォルト値を受け入れます。
      - アクション：次の値が表示されていることを確認します。

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- リソース:デフォルト値または必要なその他の値を使用し `_(bucketname, bucketname/*)`ます。

  これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの管理"。

d. [* 保護 *] で、 [* SnapMirror （ ONTAP またはクラウド）を有効にする *] をオンにし、 [* クラウドストレージ *] を選択して、 [* クラウドオブジェクトストア *] を選択します。

[Save] をクリックすると、ソース Storage VM に新しいバケットが作成され、クラウドオブジェクトストアにバックアップされます。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにrootユーザキーが存在することを確認し、存在しない場合は再生成します `vserver object-store-server user show`。+ rootユーザのアクセスキーがあることを確認します。存在しない場合は、「 `vserver object-store-server user regenerate-keys -vserver svm_name -user root`+ Do not regenerate the key if one already exists」と入力します。
2. ソースSVMにバケットを作成します。
   `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. デフォルトのバケットポリシーにアクセスルールを追加します。
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   例

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：* `type continuous`–SnapMirror S3関係の唯一のポリシータイプ（必須）。* `-rpo`–目標復旧時点の時間を秒単位で指定します（オプション）。* `-throttle`–スループット/帯域幅の上

限をキロバイト/秒単位で指定します（オプション）。

例

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. ターゲットがStorageGRIDシステムの場合は、ソースクラスタの管理SVMにStorageGRID CAサーバ証明書をインストールします。
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

6. SnapMirror S3デスティネーションオブジェクトストアを定義します。
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

パラメータ：* `-object-store-name`–ローカルONTAPシステム上のオブジェクトストアターゲットの名前。* `-usage`–このワークフローで使用し `data`ます。* `-provider-type`– `AWS_S3`および `SGWS`（StorageGRID）ターゲットがサポートされています。* `-server`–ターゲットサーバのFQDNまたはIPアドレス。* `-is-ssl-enabled`–SSLの有効化はオプションですが、推奨されます。+の詳細について `snapmirror object-store config create`は、を"ONTAPコマンド リファレンス"参照してください。

例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. SnapMirror S3 関係を作成します。
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

パラメータ：* `-destination-path`-前の手順で作成したオブジェクトストアの名前と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. ミラーリングがアクティブであることを確認します。
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "スナップミラー作成"
- "snapmirror policy create"
- "snapmirror show"

既存の**ONTAP S3**バケットのクラウドバックアップ関係を作成する

既存のS3バケットのバックアップはいつでも開始できます。たとえば、S3の設定をONTAP 9 .10.1より前のリリースからアップグレードした場合などです。

開始する前に

- オブジェクトストアプロバイダの有効なアカウントクレデンシャルと設定情報が必要です。
- ソースシステムにクラスタ間ネットワークインターフェイスとIPspaceが設定されている。
- ソースStorage VMのDNS設定でターゲットのFQDNを解決できる必要があります。

System Manager

1. ユーザとグループが正しく定義されていることを確認します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。

   詳細については、を参照してください "S3ユーザとグループの追加" 。

2. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
   c. ポリシーの名前と説明を入力します。
   d. ポリシースコープ（クラスタまたはSVM）を選択します
   e. SnapMirror S3関係の場合は*[Continuous]*を選択します。
   f. スロットル * とリカバリ・ポイントの目標値 * を入力します。
3. ソースシステムにクラウドオブジェクトストアを追加します。
   a. [保護（ Protection ）] > [概要（ Overview ）] * をクリックし、 [クラウドオブジェクトストア（ Cloud Object Store ）] を選択
   b. [* 追加] をクリックし、 [* Amazon S3 * または * その他 * （ StorageGRID Webscale ）] を選択します。
   c. 次の値を入力します。
      - クラウド オブジェクト ストアの名前
      - URLの形式（パスまたは仮想ホスト）
      - Storage VM（S3対応）
      - オブジェクト ストアのサーバ名（FQDN）
      - オブジェクト ストアの証明書
      - アクセスキー
      - シークレットキー
      - コンテナ（バケット）名
4. 既存のバケットのバケットアクセスポリシーが引き続きニーズを満たしていることを確認します。
   a. [* Storage * > * Buckets] をクリックして、保護するバケットを選択します。
   b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-次の値が表示されていることを確認します。
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - リソース-デフォルト値または必要なその他の値を使用します *(`bucketname`, `bucketname/*`)*。

これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの管理"。

5. SnapMirror S3を使用してバケットをバックアップします。
   a. [* Storage *] > [* Buckets] をクリックし、バックアップするバケットを選択します。
   b. [* Protect （保護）] をクリックし、 [* Target （ターゲット）] の下の [* Cloud Storage （クラウドストレージ）] を選択してから、 [* Cloud Object Store （クラウドオブジェクトストア）]

Save をクリックすると、既存のバケットがクラウドオブジェクトストアにバックアップされます。

CLI

1. デフォルトのバケットポリシーのアクセスルールが正しいことを確認します。
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   例

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. 既存の SnapMirror S3 ポリシーがなく、デフォルトのポリシーを使用しない場合は、SnapMirror S3 ポリシーを作成します。
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：* `type continuous`–SnapMirror S3関係の唯一のポリシータイプ（必須）。* `-rpo`–目標復旧時点の時間を秒単位で指定します（オプション）。* `-throttle`–スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

   例

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. ターゲットがStorageGRIDシステムの場合は、ソースクラスタの管理SVMにStorageGRID CA証明書をインストールします。
   `security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

4. SnapMirror S3デスティネーションオブジェクトストアを定義します。

`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

パラメータ：* `-object-store-name`–ローカルONTAPシステム上のオブジェクトストアターゲットの名前。* `-usage`–このワークフローで使用し `data`ます。* `-provider-type`– `AWS_S3`および `SGWS`（StorageGRID）ターゲットがサポートされています。* `-server`–ターゲットサーバのFQDNまたはIPアドレス。* `-is-ssl-enabled`–SSLの有効化はオプションですが、推奨されます。+の詳細について `snapmirror object-store config create`は、を"ONTAPコマンド リファレンス"参照してください。

例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. SnapMirror S3 関係を作成します。
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

パラメータ：* `-destination-path`-前の手順で作成したオブジェクトストアの名前と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトをそのまま使用することもできます。

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. ミラーリングがアクティブであることを確認します。
`snapmirror show -policy-type continuous -fields status`

関連情報

- "スナップミラー作成"
- "snapmirror policy create"
- "snapmirror show"

クラウドターゲットから**ONTAP S3**バケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、デスティネーションバケットからリストアしてデータを再取り込みできます。

タスクの内容

デスティネーションバケットは、既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、デスティネーションバケットの使用済み論理スペースよりも大きくする必要がありま

す。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

System Manager

バックアップデータをリストアします。

1. [保護]>[関係]をクリックし、[SnapMirror S3]*を選択します。
2. をクリックし、*[リストア]*を選択します。
3. 「 * ソース * 」で、「 * 既存バケット」（デフォルト）または「 * 新規バケット」を選択します。
   - 既存の Bucket * （デフォルト）にリストアするには、次の操作を実行します。
     - クラスタとStorage VMを選択して既存のバケットを検索します。
     - 既存のバケットを選択します。
     - destination_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
   - 新しいバケットへのリストアを実行するには、次の値を入力します。
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンスサービスレベル。詳細については、を参照してください "ストレージサービスレベル" 。
     - デスティネーションS3サーバCA証明書の内容。
4. 「 * Destination * 」の下にある _source_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
5. [保護] 、 [関係] の順にクリックして、復元の進行状況を監視します。

CLIの手順

1. リストア用の新しいデスティネーションバケットを作成します。詳細については、を参照してください "バケットのバックアップ関係の作成（クラウドターゲット）"。
2. デスティネーションバケットのリストア処理を開始します。
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   例

   次の例は、デスティネーションバケットを既存のバケットにリストアします。
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   の詳細については `snapmirror restore`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapMirror S3ポリシーを変更する

S3 SnapMirrorポリシーを変更してRPOとスロットル値を調整することができます。

System Manager

1. [保護]>[関係]*をクリックし、変更する関係の保護ポリシーを選択します。
2. ポリシー名の横にあるをクリックし ⋮ 、*[編集]*をクリックします。

CLI

SnapMirror S3 ポリシーを変更します。

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

パラメータ：

- `-rpo`：目標復旧時点の時間を秒単位で指定します。
- `-throttle`：スループット/帯域幅の上限をキロバイト/秒単位で指定します。

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

関連情報

- "snapmirror policy modify"

SnapshotでS3データを保護

ONTAP S3スナップショットの詳細

ONTAP 9 .16.1以降では、ONTAP Snapshotテクノロジを使用して、ONTAP S3バケットの読み取り専用のポイントインタイムイメージを生成できます。

S3のSnapshot機能を使用すると、Snapshotを手動で作成することも、Snapshotポリシーを使用して自動的に生成することもできます。S3 SnapshotはS3バケットとしてS3クライアントに提供されます。S3クライアントを使用して、Snapshotのコンテンツを参照し、リストアできます。

ONTAP 9 .16.1では、S3 SnapshotはS3バケット内のオブジェクトの現在のバージョンのみをキャプチャします。バージョン管理されたバケットの最新以外のバージョンはS3 Snapshotにキャプチャされません。また、Snapshotの作成後にオブジェクトタグが変更された場合、ポイントインタイムのオブジェクトタグはSnapshotにキャプチャされません。

S3 Snapshotはクラスタ時間に依存します。時刻を同期するには、クラスタ内のNTPサーバを設定する必要があります。詳細については、を参照してください "クラスタ時間を管理します。"。

クォータとスペース使用量

クォータは、S3バケットで使用されているオブジェクトの数と論理サイズを追跡します。S3 Snapshotが作成されると、S3 Snapshotにキャプチャされたオブジェクトは、ファイルシステムからSnapshotが削除されるまで、バケットのオブジェクト数と使用サイズにカウントされます。

マルチパートオブジェクト

マルチパートオブジェクトの場合、最後のオブジェクトのみがスナップショットにキャプチャされます。マルチパートオブジェクトの部分的なアップロードはSnapshotにキャプチャされません。

バージョン管理に対応しているバケットとバージョン管理に対応していないバケット上の**Snapshot**

バージョン管理に対応しているバケットとバージョン管理に対応していないバケットの両方にSnapshotを作成できます。スナップショットには、スナップショットがキャプチャされた時点での現在のオブジェクトバージョンのみが含まれます。

バージョン管理されたバケットとスナップショット

オブジェクトのバージョン管理が有効になっているバケットでは、Snapshotの作成後に最新のオブジェクトバージョンのコンテンツが保持されます。バケット内の最新でないバージョンは除外されます。

次の例を考えてみましょう。オブジェクトのバージョン管理が有効になっているバケットで、オブジェクト`obj1`のバージョンは`v1`、`v2`、`v3`、`v4`、`v5`です。`v3`（キャプチャ時点の最新バージョン）から `obj1`スナップショットを作成した `snap1`。閲覧すると `snap1`、 `obj1`はv3で作成されたコンテンツを含むオブジェクトとして表示されます。以前のバージョンのコンテンツは返されません。

> 最新でないバージョンは、Snapshotが削除されるまでファイルシステムに保持されます。

バージョン管理に対応していないバケットとスナップショット

バージョン管理に対応していないバケットでは、S3 SnapshotはSnapshotの作成前に最新のコミットの内容を保持します。

次の例を考えてみましょう。オブジェクトのバージョン管理を利用できないバケットで、でオブジェクトが`obj1`数回上書きされています（`T1`、`T2`、`T3`、`T4`、`T5`）。`T3`と`T4`の間に`S3 Snapshot`を作成しました `snap1`。閲覧すると `snap1`、 `obj1`T3で作成されたコンテンツと一緒に表示されます。

オブジェクトの有効期限と**Snapshot**

ONTAP S3オブジェクトの有効期限とS3 Snapshot機能は、互いに独立して機能します。ONTAPオブジェクトの有効期限機能は、S3バケットに対して定義されたライフサイクル管理ルールに従ってオブジェクトバージョンの期限が切れます。S3 Snapshotは、Snapshotが作成された時点のバケットオブジェクトの静的なコピーです。

バケットでオブジェクトのバージョン管理が有効になっている場合、そのバケットに定義された有効期限ルールによってオブジェクトの特定のバージョンが削除されたときに、そのバージョンが1つ以上のS3 Snapshotに現在のバージョンとしてキャプチャされていれば、そのバージョンのコンテンツはファイルシステムに残ります。そのオブジェクトバージョンは、そのSnapshotが削除された場合にのみファイルシステムに存在しなくなります。

同様に、バージョン管理が無効になっているバケットでは、有効期限ルールに基づいてオブジェクトが削除されても、そのオブジェクトが既存のS3 Snapshotにキャプチャされたままの場合、オブジェクトはファイルシステムに保持されます。オブジェクトをキャプチャしているSnapshotが削除されると、オブジェクトはファイルシステムから完全に削除されます。

S3オブジェクトの有効期限とライフサイクルの管理については、を参照してください"バケットライフサイクル管理ルールを作成する"。

S3 Snapshotニカンスルセイケンシコウ

ONTAP 9 .16.1では、次の機能の除外とシナリオに注意してください。

- S3バケットに対して生成できるSnapshotは最大1023個です。
- クラスタをONTAP 9より前のバージョンのONTAPにリバートする前に、クラスタ内のすべてのバケットからS3 Snapshotとメタデータをすべて削除する必要があります。16.1
- Snapshotを含むオブジェクトを含むS3バケットを削除する必要がある場合は、そのバケット内のすべてのオブジェクトに対応するSnapshotをすべて削除しておく必要があります。
- S3 Snapshotは、次の構成ではサポートされません。
  - SnapMirror関係のバケット
  - オブジェクトロックが有効になっているバケット
  - NetAppコンソール
  - System Manager
  - ONTAP MetroClusterコウセイ

ONTAP S3 Snapshotを作成する

S3 Snapshotを手動で生成することも、Snapshotポリシーを設定してS3 Snapshotを自動的に作成することもできます。Snapshotは、データのバックアップとリカバリに使用するオブジェクトの静的コピーとして機能します。Snapshotの保持期間を決定するために、指定した間隔でSnapshotを自動的に作成するSnapshotポリシーを作成できます。

S3 Snapshotを使用すると、オブジェクトのバージョン管理を有効にするかどうかに関係なく、S3バケット内のオブジェクトデータを保護できます。

Snapshotは、S3バケットでオブジェクトのバージョン管理が有効になっていない場合にデータ保護を確立する際に特に役立ちます。これは、以前のオブジェクトバージョンを使用できない場合にリストア処理で使用できるポイントインタイムレコードとして機能するためです。

タスクの内容

- スナップショットには、次の命名規則が適用されます（手動スナップショットと自動スナップショットの両方）。
  - S3 Snapshot名の最大文字数は30文字です
  - S3 Snapshot名に使用できる文字は、小文字のアルファベット、数字、ドット（.）、ハイフン（-）のみです。
  - S3 Snapshot名の末尾の文字はアルファベットまたは数字にする必要があります
  - S3 Snapshot名にサブ文字列を含めることはできません `s3snap`
- S3プロトコルでは、バケットの命名制限によってバケット名は63文字に制限されます。ONTAP S3スナップショットはS3プロトコルでバケットとして提供されるため、Snapshotバケット名にも同様の制限が適用されます。デフォルトでは、元のバケット名がベースバケット名として使用されます。
- どのスナップショットがどのバケットに属しているかを簡単に識別できるように、スナップショットバケット名は、ベースバケット名と、スナップショット名の前に付加された特別な文字列で構成され

-s3snap-`ます。Snapshotバケット名の形式は、です `<base_bucket_name>-s3snap-<snapshot_name>`。

たとえば、次のコマンドを実行して `snap1`onを `bucket-a`作成すると、という名前のSnapshotバケットが作成され `bucket-a-s3snap-snap1`ます。ベースバケットにアクセスする権限がある場合は、S3クライアントからこのバケットにアクセスできます。

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- 63文字を超えるSnapshotバケット名を作成することはできません。
- 自動Snapshot名には、ポリシースケジュール名とタイムスタンプが含まれます。これは、トラディショナルボリュームSnapshotの命名規則に似ています。スケジュールされたSnapshotの名前は `daily-2024-01-01-0015`、など `hourly-2024-05-22-1105`です。

S3 Snapshotを手動で作成する

ONTAP CLIを使用して、S3 Snapshotを手動で作成できます。この手順では、ローカルクラスタにのみSnapshotが作成されます。

手順

1. S3 Snapshotを作成します。

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

次の例は `vs0`、Storage VMと `website-data`バケットにという名前のSnapshotを作成します `pre-update`。

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

バケットへの**S3 Snapshot**ポリシーの割り当て

S3バケットレベルのSnapshotポリシーを設定すると、ONTAPによってスケジュールされたS3 Snapshotが自動的に作成されます。従来のSnapshotポリシーと同様に、S3 Snapshotに対して最大5つのスケジュールを設定できます。

Snapshotポリシーは、通常、Snapshotを作成するスケジュール、各スケジュールで保持するコピーの数、およびスケジュールのプレフィックスを指定します。たとえば、毎日午前12時10分にS3 Snapshotを1つ作成し、最新の2つのコピーを保持して、という名前を付けることができます `daily-<timestamp>`。

デフォルトのSnapshotポリシーで保持される内容は次のとおりです。

- 6時間ごとのスナップショット

- 2つの日単位のスナップショット
- 2つの週単位のスナップショット

開始する前に

- SnapshotポリシーをS3バケットに割り当てる前に、作成しておく必要があります。

> S3 Snapshotのポリシーには、他のONTAP Snapshotポリシーと同じルールが適用されます。ただし、いずれかのSnapshotスケジュールに保持期間が設定されているSnapshotポリシーをS3バケットに割り当てることはできません。

Snapshotを自動生成するためのSnapshotポリシーの作成の詳細については、を参照してください"カスタムSnapshotポリシーの設定の概要"。

手順

1. バケットにSnapshotポリシーを割り当てます。

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

または

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

> クラスタをONTAP 9 .16.1より前のバージョンのONTAPにリバートする必要がある場合は、すべてのバケットのの値が（または -）に設定されている `none`ことを確認して `snapshot-policy`ください。

関連情報

"ONTAP S3スナップショットの詳細"

ONTAP S3 Snapshotの表示とリストア

ONTAP S3のSnapshot機能を使用すると、S3クライアントからバケットのS3 Snapshotのコンテンツを表示および参照できます。また、S3 SnapshotからS3クライアント上の単一のオブジェクト、一連のオブジェクト、またはバケット全体をリストアできます。

開始する前に

バケットのONTAP S3 Snapshotを表示、参照、およびリストアするには、Snapshotが作成されている必要があります。また、S3プロトコルクライアントからS3ベースバケットにアクセスできる必要があります。

S3 Snapshotのリストと表示

S3 Snapshotの詳細を表示して比較し、エラーを特定できます。ONTAP CLIを使用すると、S3バケットに作

成されたすべてのSnapshotを表示できます。

手順

1. S3 Snapshotを表示します。

```
vserver object-store-server bucket snapshot show
```

クラスタ上のすべてのバケットに対して作成されたS3 Snapshotの名前、Storage VM、バケット、作成時間、およびの情報を確認できます `instance-uuid`。

2. バケット名を指定して、そのバケットに対して作成されたすべてのS3 Snapshotの名前、作成時間、およびそのバケットに対して作成されたすべてのS3 Snapshotを表示することもできます `instance-uuid`。

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

S3 Snapshotのコンテンツを参照する

環境で障害や問題が発生した場合は、S3バケットのSnapshotの内容を参照してエラーを特定できます。また、S3のSnapshotを参照して、リストアするエラーのないコンテンツを特定することもできます。

S3 Snapshotは、S3クライアントにSnapshotバケットとして提供されます。Snapshotバケット名の形式は、です `<base_bucket_name>-s3snap-<snapshot_name>`。S3 API処理を使用して、Storage VM内のすべてのSnapshotバケットを表示できます `ListBuckets`。

S3 snapshotバケットはベースバケットのアクセスポリシーを継承し、読み取り専用の処理のみをサポートします。ベースバケットにアクセスする権限がある場合は、S3 Snapshotバケットに対して読み取り専用のS3 API処理（ `HeadObject`、 `GetObject`、 `GetObjectTagging` `ListObjects`、、 `ListObjectVersions`、 `GetObjectAcl`、および `CopyObject`。

> S3 Snapshotバケットでこの `CopyObject`処理がサポートされるのは、ソースバケットのSnapshotである場合のみです。Snapshotのストレージデスティネーションである場合はサポートされません。

これらの操作の詳細については、を参照してください"ONTAP S3でサポートされる操作"。

S3 Snapshotからコンテンツをリストア

S3クライアントでリストア処理を実行して、Snapshotバケットから元のバケットまたは別のバケットにコンテンツをコピーすることで、単一のオブジェクト、一連のオブジェクト、またはバケット全体をリカバリできます。スナップショットを参照して、コピーするスナップショットコンテンツを決定できます。

バケット全体、プレフィックスが付いたオブジェクト、または単一のオブジェクトをリストアするには、コマンドを使用し `aws s3 cp`ます。

手順

1. ベースS3バケットのSnapshotを作成します。

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. Snapshotを使用してベースバケットをリストアします。
   - バケット全体をリストアします。Snapshotバケット名は、の形式で指定し `<base_bucket_name>-s3snap-<snapshot_name>`ます。

     ```
     aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
     s3://<base-bucket>  --recursive
     ```

   - ディレクトリ内のオブジェクトを次のプレフィックスでリストアし `dir1`ます。

     ```
     aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
     s3://<base_bucket_name>/dir1 --recursive
     ```

   - 次の名前の単一オブジェクトをリストアし `web.py`ます。

     ```
     aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
     s3://<base_bucket_name>/web.py
     ```

ONTAP S3 Snapshotの削除

不要になったS3 Snapshotを削除して、バケット内のストレージスペースを解放できます。S3 Snapshotを手動で削除したり、S3バケットに関連付けられているSnapshotポリシーを変更して、スケジュールで保持するSnapshotの数を変更したりできます。

S3バケットのSnapshotポリシーは、従来のONTAP Snapshotポリシーと同じ削除ルールに従います。Snapshotポリシーの作成の詳細については、を参照してください"Snapshot ポリシーを作成します"。

タスクの内容

- オブジェクトのバージョン（バージョン管理されたバケット内）またはオブジェクト（バージョン管理されていないバケット内）が複数のSnapshotにキャプチャされた場合、オブジェクトを保護している最後のSnapshotが削除されるまで、そのオブジェクトはファイルシステムから削除されません。
- Snapshotを含むオブジェクトを含むS3バケットを削除する必要がある場合は、そのバケット内のすべてのオブジェクトのSnapshotをすべて削除しておく必要があります。
- クラスタをONTAP 9 .16.1より前のバージョンのONTAPにリバートする必要がある場合は、すべてのバケットのS3 Snapshotをすべて削除しておく必要があります。コマンドを実行してS3バケットのSnapshotメタデータを削除することも必要になる場合があり `vserver object-store-server bucket clear-snapshot-metadata`ます。詳細については、を参照して "S3 Snapshotメタデータをクリア"ください。
- スナップショットをバッチで削除すると、複数のスナップショットにキャプチャされた多数のオブジェクトを削除できるため、スナップショットを個別に削除する場合よりも多くのスペースが解放されます。その結果、ストレージオブジェクト用により多くのスペースを再利用できます。

手順

1. 特定のS3 Snapshotを削除するには、次のコマンドを実行します。

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. バケット内のS3 Snapshotをすべて削除するには、次のコマンドを実行します。

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

S3 Snapshotメタデータをクリア

S3 Snapshotでは、Snapshotメタデータもバケット内で生成されます。Snapshotメタデータは、すべてのSnapshotがバケットから削除されても引き続きバケットに格納されます。Snapshotメタデータが存在すると、次の処理がブロックされます。

- ONTAP 9より前のONTAPバージョンにクラスタをリバートします。16.1
- バケットでのSnapMirror S3の設定

これらの処理を実行する前に、バケットからSnapshotメタデータをすべて消去する必要があります。

開始する前に

メタデータのクリアを開始する前に、バケットからすべてのS3 Snapshotを削除しておく必要があります。

手順

1. バケットからSnapshotメタデータを消去するには、次のコマンドを実行します。

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

S3イベントの監査

ONTAP S3イベントの監査について

ONTAP 9 .10.1以降では、ONTAP S3環境でデータイベントと管理イベントを監査できます。S3の監査機能は既存のNASの監査機能と同様で、S3とNASの監査機能はクラスタ内に共存できます。

SVMでS3監査の設定を作成して有効にすると、S3イベントがログファイルに記録されます。ログに記録するイベントを指定できます。

リリース別のオブジェクトアクセス（データ）イベント

9.11.1：

- ListBucketVersions
- ListBucket（9.10.1のListObjectからこの名前に変更）
- ListAllMyBuckets（9.10.1のListBucketsはこの名前に変更）

9.10.1：

- ヘッドオブジェクト
- GetObject
- PutObject
- deleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- リストアップロード
- ListParts

リリース別の管理イベント

9.15.1：

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1：

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1：

- PutBucketLifecycle

- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1：

- GetBucketPolicy
- CopyObject
- パーツコピーをアップロード
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1：

- GetBucketVersioning
- PutBucketVersioning

9.10.1：

- ヘッドバケット
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

ログの形式はJavaScript Object Notation（JSON）です。

S3とNFSの監査設定の合計数は、クラスタあたり400 SVMです。

次のライセンスが必要です。

- ONTAP S3プロトコルおよびストレージ向けのONTAP ONE（旧Core Bundleに含まれていたもの）

詳細については、を参照してください "ONTAP監査プロセスの仕組み"。

監査の保証

デフォルトでは、S3とNASの監査が保証されます。ONTAPでは、あるノードを使用できない場合でも、監査可能なバケットアクセスイベントがすべて記録されることが保証されます。要求されたバケット処理は、その処理の監査レコードが永続的ストレージのステージングボリュームに保存されるまで完了できません。スペース不足やその他の問題が原因で監査レコードをステージングファイルでコミットできない場合は、クライアント処理が拒否されます。

カンサヨウノスヘエスヨウケン

ONTAP監査システムでは、監査レコードは最初に個 々 のノード上のバイナリステージングファイルに格納されます。定期的に統合され、ユーザが読解可能なイベントログに変換されて、SVMの監査イベントログディ

レクトリに格納されます。

ステージングファイルは専用のステージングボリュームに格納されます。このボリュームは、監査設定の作成時にONTAPによって作成されます。各アグリゲートに1つのステージングボリュームがあります。

監査の設定に十分な使用可能スペースがあることを計画する必要があります。

- 監査対象バケットを含むアグリゲート内のステージングボリューム。
- （変換されたイベントログが格納されるディレクトリを含むボリューム）。

S3監査の設定を作成するときに次の2つの方法のいずれかを使用して、イベントログの数とボリュームの利用可能なスペースを制御できます。

- 最大数値。パラメータは、 `-rotate-limit`保持する必要がある監査ファイルの最小数を制御します。
- 時間制限。パラメータは、ファイルを保持できる最大期間を制御します。 `-retention-duration`

どちらのパラメータでも、構成済みの監査ファイルを超えると、古い監査ファイルを削除して新しい監査ファイル用のスペースを確保できます。両方のパラメータの値は0で、すべてのファイルを維持する必要があることを示します。したがって、十分なスペースを確保するためには、いずれかのパラメータをゼロ以外の値に設定することを推奨します。

監査が保証されるため、ローテーション制限の前に監査データに使用できるスペースがなくなると、新しい監査データを作成できなくなり、クライアントがデータにアクセスできなくなります。したがって、この値と監査に割り当てられるスペースは慎重に選択する必要があり、監査システムからの使用可能なスペースに関する警告に対応する必要があります。

詳細については、を参照してください "監査の基本概念"。

ONTAP S3監査の設定を計画する

S3監査の設定にはいくつかのパラメータを指定するか、デフォルトを受け入れる必要があります。特に、適切な空きスペースを確保するのに役立つログローテーションパラメータを検討する必要があります。

の詳細については `vserver object-store-server audit create`、を"ONTAPコマンド リファレンス"参照してください。

一般パラメータ

監査の設定を作成するときに指定する必要がある必須パラメータが2つあります。また、指定できるオプションのパラメータも3つあります。

情報の種類	オプション	必須
SVM 名 _ 監査設定を作成するSVMの名前。 SVMがすでに存在し、S3に対して有効になっている必要があります。	`-vserver` *`svm_name`*	○

_ ログデスティネーションパス _ 変換された監査ログを格納する場所を指定します。SVM上にすでに存在しているパスを指定する必要があります。 パスは最大864文字で、読み取り/書き込み権限が必要です。 パスが無効な場合、監査設定コマンドは失敗します。	`-destination text`	○
_ 監査するイベントのカテゴリ _ 監査できるイベントカテゴリは次のとおりです。 • データGetObject、PutObject、およびDeleteObjectイベント • 管理PutBucketイベントおよびDeleteBucketイベント デフォルトでは、データイベントのみが監査されます。	`-events {data|management}, …`	いいえ

監査ログファイルの数を制御するには、次のいずれかのパラメータを入力します。値を入力しない場合は、すべてのログファイルが保持されます。

情報の種類	オプション	必須
ログファイルのローテーションの上限 _ 保持する監査ログファイルの数を指定します。この数を超えると、最も古いログファイルがローテーションから除外されます。たとえば、値5を入力すると、最後の5つのログファイルが保持されます。 値0は、すべてのログファイルが保持されることを示します。デフォルト値は0です。	`-rotate-limit integer`	いいえ
ログファイル継続時間制限 ログファイルが削除されるまでの保持期間を指定します。たとえば、5d0h0mと入力すると、5日以上経過したログが削除されます。 値0は、すべてのログファイルが保持されることを示します。デフォルト値は0です。	`-retention duration integer_time`	いいえ

監査ログのローテーションのパラメータ

サイズまたはスケジュールに基づいて監査ログのローテーションを実行できます。デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。

ログサイズに基づくログのローテーション

デフォルトのログローテーション方式とデフォルトのログサイズを使用する場合は、ログローテーションのパラメータを設定する必要はありません。デフォルトのログサイズは100MBです。

デフォルトのログサイズを使用しない場合は、カスタムログサイズを指定するようにパラメータを設定できます `-rotate-size`。

ログサイズのみに基づいてローテーションをリセットする場合は、次のコマンドを使用してパラメータの設定を解除し `-rotate-schedule-minute`ます。

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

スケジュールに基づいたログのローテーション

スケジュールに基づく監査ログのローテーションを選択した場合は、時間に基づくローテーションパラメータを任意の組み合わせで使用して、ログのローテーションをスケジュールできます。

- 時間に基づくローテーションを使用する場合、 `-rotate-schedule-minute`パラメータは必須です。
- その他の時間ベースのローテーションパラメータはすべてオプションです。
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- ローテーションスケジュールは、時間に関連するすべての値を使用して計算されます。たとえば、パラメータのみを指定する `-rotate-schedule-minute`と、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。
- 時間に基づくローテーションパラメータを1つか2つだけ指定した場合（、など `-rotate-schedule-month` `-rotate-schedule-minutes`）、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

  たとえば、監査ログのローテーションを、1月、3月、8月の月曜日、水曜日、土曜日の午前10時30分に実行するように指定できます。

- との `-rotate-schedule-day`両方に値を指定すると `-rotate-schedule-dayofweek`、それらは独立して考慮されます。

  たとえば、にFridayを指定し、 `-rotate-schedule-day`に13を指定する `-rotate-schedule-dayofweek`と、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日、および指定した月の13日にも実行されます。

- スケジュールのみに基づいてローテーションをリセットする場合は、次のコマンドを使用しての設定を解除します `-rotate-size parameter`。

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

ログサイズとスケジュールに基づいたログのローテーション

ログサイズとスケジュールに基づいてログファイルをローテーションするように選択するには、-rotate-sizeパ

ラメータと時間ベースのローテーションパラメータの両方を任意の組み合わせで設定します。たとえば、が10MBに設定され、 `-rotate-schedule-minute`が15に設定されている場合 `-rotate-size`、ログファイルのサイズが10MBに達したとき、または1時間ごとの15分（いずれか早い方）にログファイルがローテーションされます。

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

ONTAP S3監査の設定を作成して有効にする

S3監査を実装するには、まずS3対応のSVMで永続的なオブジェクトストアの監査設定を作成してから、設定を有効にします。

開始する前に

- S3対応のSVMが必要です。
- ローカル階層にステージングボリューム用の十分なスペースがあることを確認してください。

タスクの内容

監査の設定は、監査対象のS3バケットを含むSVMごとに必要です。新規または既存のS3サーバでS3監査を有効にすることができます。監査の設定は、 * vserver object-store-server audit delete * コマンドで削除されるまで S3 環境で維持されます。

S3監査の設定は、監査用に選択したSVM内のすべてのバケットに適用されます。監査が有効なSVMには、監査対象バケットと未監査バケットを含めることができます。

ログサイズまたはスケジュールに基づいて自動的にログがローテーションされるようにS3監査を設定することを推奨します。自動ログローテーションを設定しない場合、すべてのログファイルがデフォルトで保持されます。S3 ログファイルのローテーションは、 * vserver object-store-server audit rotate-log * コマンドを使用して手動で実行することもできます。

SVMがSVMディザスタリカバリのソースである場合、デスティネーションパスをルートボリュームに配置することはできません。

手順

1. ログサイズまたはスケジュールに基づいて監査ログのローテーションを行うには、監査の設定を作成します。

監査ログのローテーションの基準	入力するコマンド
ログサイズ	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integer_d`*`][`*`integer_h`*`][`*`integer_m`*`][`*`integer_s`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`

監査ログのローテーションの基準	入力するコマンド
スケジュール	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integerd`*`][`*`integerh`*`] [`*`integerm`*`][`*`integers`*`]] } [-rotate-schedule-month` *`chron_month`*`] [-rotate-schedule-dayofweek` *`chron_dayofweek`*`] [-rotate-schedule-day` *`chron_dayofmonth`*`] [-rotate-schedule-hour` *`chron_hour`*`] -rotate-schedule-minute` *`chron_minute`* `-rotate-schedule-minute`時間に基づく監査ログのローテーションを設定する場合、パラメータは必須です。

2. S3監査を有効にします。

   `vserver object-store-server audit enable -vserver` *`svm_name`*

例

次の例は、サイズに基づくローテーションを使用してすべてのS3イベント（デフォルト）を監査する監査の設定を作成します。ログは/audit_logディレクトリに格納されます。ログファイルのサイズの上限は200MBです。ログは、サイズが200MBに達するとローテーションされます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

次の例は、サイズに基づくローテーションを使用してすべてのS3イベント（デフォルト）を監査する監査の設定を作成します。ログファイルのサイズの上限は100MB（デフォルト）で、ログは5日間保持されてから削除されます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

次の例は、時間に基づくローテーションを使用してS3管理イベントと集約型アクセスポリシーのステージングイベントを監査する監査の設定を作成します。監査ログのローテーションは、毎月、すべての曜日の午後12時30分に実行されます。ログのローテーション回数の上限は5回です。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

ONTAP S3の監査用のバケットを選択します。

監査が有効なSVMでは、監査対象のバケットを指定する必要があります。

開始する前に

- S3の監査が有効になっているSVMがあります。

タスクの内容

S3 監査の設定は SVM 単位で有効になりますが、監査用に有効になっている SVM 内のバケットを選択する必要があります。SVMにバケットを追加し、新しいバケットを監査する場合は、この手順でバケットを選択する必要があります。SVMの監査で未監査のバケットをS3監査用に有効にすることもできます。

監査の設定は、コマンドで削除するまでバケットの設定が維持され `vserver object-store-server audit event-selector delete`ます。

手順

1. S3監査のバケットを選択：

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`：監査対象のイベントアクセスのタイプ（、 `write-only`または `all`）を指定します `read-only`（デフォルトは `all`）。
   - `-permission`：監査するイベント権限のタイプ（、 `deny-only`または `all`） `all`を指定します。 `allow-only`

例

次の例は、読み取り専用アクセスで許可されたイベントのみをログに記録するバケットの監査設定を作成します。

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

ONTAP S3の監査設定を変更する

SVMでは、個 々 のバケットの監査パラメータや、監査対象として選択したすべてのバケットの監査の設定を変更できます。

監査設定を変更する対象	入力するコマンド
個々のバケット	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`]` `[`*`parameters to modify`*`]`
SVM内のすべてのバケット	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

例

次の例は、書き込み専用アクセスイベントのみを監査するように、個 々 のバケットの監査設定を変更します。

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

次の例は、 SVM 内のすべてのバケットの監査の設定を変更して、ログサイズの上限を 10MB に変更し、 3 つのログファイルを保持するように変更します。

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

ONTAP S3監査の設定の表示

監査の設定が完了したら、監査が適切に設定されて有効になっていることを確認できます。また、クラスタ内のすべてのオブジェクトストアの監査の設定に関する情報を表示することもできます。

タスクの内容

バケットとSVMの監査の設定に関する情報を表示できます。

- バケット：コマンドを使用します。 `vserver object-store-server audit event-selector show`

  パラメータを指定せずにコマンドを実行すると、オブジェクトストアの監査が設定されたクラスタ内のすべてのSVM内のバケットに関する次の情報が表示されます。

  - SVM名
  - バケット名
  - アクセスと権限の値
- SVM：コマンドを使用します。 `vserver object-store-server audit show`

  パラメータを指定せずにコマンドを実行すると、オブジェクトストアの監査が設定されたクラスタ内のすべてのSVMに関する次の情報が表示されます。

  - SVM名
  - 監査の状態
  - ターゲットディレクトリ

パラメータを指定すると、表示する監査設定情報を指定できます `-fields`。

手順

S3監査の設定に関する情報を表示します。

設定を変更する対象	入力するコマンド
バケット	`vserver object-store-server audit event-selector show [-vserver svm_name] [parameters]`
SVM	`vserver object-store-server audit show [-vserver svm_name] [parameters]`

例

次の例は、単一のバケットの情報を表示します。

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

次の例は、SVM上のすべてのバケットに関する情報を表示します。

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

次の例は、すべてのSVMの名前、監査の状態、イベントタイプ、ログ形式、およびターゲットディレクトリを表示します。

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

次の例は、すべてのSVMの名前と監査ログに関する詳細を表示します。

```
cluster1::> vserver object-store-server audit show -log-save-details

                  Rotation                              Rotation
      Vserver     File Size Rotation Schedule           Limit
      ----------- --------- ------------------------- --------
      vs1         100MB     -                         0
```

次の例は、すべてのSVMに関するすべての監査設定情報をリスト形式で表示します。

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                           Log Format: json
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

認証とアクセス制御

ニンシヨウトアクセスセイキヨノカイヨウ

ONTAPクラスタの認証とONTAP Webサービスへのアクセス制御を管理できます。

System ManagerまたはCLIを使用して、クライアントや管理者によるクラスタやストレージへのアクセスを制御し、保護することができます。

従来のSystem Manager（ONTAP 9.7以前でのみ使用可能）を使用している場合は、 "System Managerクラシック（ONTAP 9 .0 ~ 9.7）"

クライアント認証と許可

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

カンリシヤニンシヨウト**RBAC**

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

管理者認証と**RBAC**の管理

ONTAPでの管理者認証と**RBAC**の詳細

ONTAPのクラスタ管理者およびStorage Virtual Machine（SVM）管理者のログインアカウントを有効にすることができます。管理者が実行できる機能は、Role-Based Access Control（RBAC；ロールベースアクセス制御）を使用して定義することもできます。

ローカルの管理者アカウントには、次の種類の認証を使用した管理Storage Virtual Machine（SVM）またはデータSVMへのアクセスを許可できます。

- "パスワード"
- "SSH公開鍵"
- "SSL証明書"
- "SSH多要素認証（MFA）"

  ONTAP 9 .3以降では、パスワードと公開鍵による認証がサポートされています。

リモート管理者アカウントには、次の種類の認証を使用した管理SVMまたはデータSVMへのアクセスを許可できます。

- "Active Directory"

ONTAP 9.13.1以降では、Active Directoryユーザのプライマリまたはセカンダリ認証方式としてSSH公開鍵を使用できます。

- "SAML認証（管理SVMのみ）"

  ONTAP 9.3 以降では、 Service Processor Infrastructure 、 ONTAP API 、または System Manager のいずれかの Web サービスを使用することで、管理 SVM へのアクセスに Security Assertion Markup Language （ SAML ）認証を使用できます。

- "LDAPまたはNIS"

ONTAP管理者認証とRBACのワークフロー

ローカルまたはリモートの管理者アカウントに対して認証を有効にすることができます。ローカルアカウントのアカウント情報はストレージシステム上にあり、リモートアカウントのアカウント情報は別の場所にあります。各アカウントには、事前定義されたロールまたはカスタムロールを割り当てることができます。

1 設定ワークシートに記入

ログインアカウントを作成してロールベースアクセス制御（RBAC）を設定する前に、の各項目の情報を収集する必要があります"設定ワークシート"。

2 管理者アカウントがローカルかリモートかを判断する

- *ローカルの場合：*"パスワード"、"SSH"、、"SSH MFA"または"SSL"アクセスを有効にします。
- *リモートの場合：*リモートアクセスのタイプを確認します。アクセスタイプに応じて、"Active Directoryアクセスの有効化"、"LDAPまたはNISアクセスの有効化"、または"SAML認証の設定（管理SVMのみ）"。

3 ロールベースアクセスの設定

管理者がアクセスできるコマンドは、管理者に割り当てられたロールで決まります。ロールは管理者アカウントの作成時に割り当てられ、あとから割り当てることができます。"変更済み"および"SVM"管理者用に、または"カスタムロールの定義"必要に応じて事前定義されたロールを使用できます"クラスタ"。

4 管理者アカウントの管理

アカウントアクセスを有効にした方法によっては、 "ローカルアカウントヲシヨウシタコウカイ" 、 管理"公開鍵とX.509証明書" 、設定"SSHログイン用のCisco Duo 2FA" 、インストール"CA 署名済みサーバデジタル証明書" 、または設定する"Active Directory" 、 "LDAP、またはNIS"アクセス。これらのタスクは、アカウント アクセスを有効にする前でも有効にした後でも実行できます。

5 追加のセキュリティ機能の設定

- "マルチ管理者認証の管理"特定の操作を指定された管理者による承認が必要になるようにする場合。
- "動的許可の管理"ユーザーの信頼レベルに基づいて追加の承認チェックを動的に適用する場合。

- "ジャストインタイム（JIT）権限昇格を構成する"ユーザーが特定のタスクを実行するために一時的に昇格された権限にアクセスできるようにする場合。

ONTAP管理者認証とRBACのセットアップのワークシート

ログインアカウントを作成してロールベースアクセス制御（RBAC）を設定する前に、設定ワークシートの各項目の情報を収集する必要があります。

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

ログインアカウントの作成または変更

次の値は、コマンドでログインアカウントによるStorage VMへのアクセスを有効にするときに指定します `security login create`。の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

同じ値は、コマンドでアカウントによるStorage VMへのアクセス方法を変更するときに指定し `security login modify`ます。の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	アカウントがアクセスするStorage VMの名前。デフォルト値はクラスタの管理Storage VMの名前です。	
`-user-or-group-name`	アカウントのユーザ名またはグループ名。グループ名を指定した場合、そのグループ内の各ユーザのアクセスが有効になります。1つのユーザ名またはグループ名を複数のアプリケーションに関連付けることができます。	
`-application`	Storage VMへのアクセスに使用するアプリケーション。 • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	アカウントの認証に使用する認証方式。 • `cert`SSL証明書による認証 • `domain`Active Directory認証 • `nsswitch`LDAP認証またはNIS認証 • `password`ユウサハスワアトニンシヨウ • `publickey`コウカイニンシヨウ • `community`SNMPコミュニティストリング • `usm`SNMPユウサセキユリテイモテル • `saml`Security Assertion Markup Language（SAML）認証	
`-remote-switch-ipaddress`	リモートスイッチのIPアドレス。リモートスイッチは、クラスタスイッチヘルスモニタ（CSHM）で監視されるクラスタスイッチ、またはMetroClusterヘルスモニタ（MCC-HM）で監視されるファイバチャネル（FC）スイッチです。このオプションは、アプリケーションがで、認証方式が `usm`の場合にのみ適用され `snmp`ます。	
`-role`	アカウントに割り当てられているアクセス制御ロール。 • クラスタ（管理Storage VM）の場合、デフォルト値はです `admin`。 • データStorage VMの場合、デフォルト値はです `vsadmin`。	
`-comment`	（任意）アカウントの説明テキスト。テキストは二重引用符（"）で囲む必要があります。	
`-is-ns-switch-group`	アカウントがLDAPグループアカウントかNISグループアカウントか(`yes`、または `no`）。	

`-second-authentication-method`	多要素認証の場合の2番目の認証方式： • `none`多要素認証を使用しない場合のデフォルト値 • `publickey`がpasswordまたはnsswitchの場合の公開鍵認証 `authmethod` • `password`が公開鍵の場合のユーザパスワード認証 `authmethod` • `nsswitch`authmethod がpublickeyの場合のユーザパスワード認証 認証の順序は、常に公開鍵が先でパスワードがあとです。	
`-is-ldap-fastbind`	ONTAP 9.11.1 以降では、true に設定すると、nsswitch 認証の LDAP 高速バインドが有効になります。デフォルトは false です。LDAP高速バインドを使用するには、 `-authentication-method`値をに設定する必要があり `nsswitch`ます。"ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"です。	

Cisco Duoセキュリティ情報の設定

次の値は、コマンドでStorage VMに対してSSHログインを使用したCisco Duo二要素認証を有効にするときに指定します `security login duo create`。の詳細については `security login duo create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	Duo認証設定を適用するStorage VM（ONTAP CLIではVserver）。	
`-integration-key`	DuoにSSHアプリケーションを登録するときに取得した統合キー。	
`-secret-key`	DuoにSSHアプリケーションを登録するときに取得したシークレット キー。	

`-api-host`	DuoにSSHアプリケーションを登録するときに取得したAPIホスト名。例： `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Duo認証を妨げるサービスまたは構成エラーの場合は、失敗 `safe`（アクセスを許可）または `secure`（アクセスを拒否）します。デフォルトはです `safe`。これは、Duo APIサーバーにアクセスできないなどのエラーが原因でDuo認証が失敗した場合、認証がバイパスされることを意味します。	
`-http-proxy`	指定したHTTPプロキシを使用します。HTTPプロキシで認証が必要な場合は、プロキシURLにクレデンシャルを含めます。例： `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	またはの `false`` いずれか `true`。デフォルトはです `false`。の場合 `true`、Duoはユーザーの電話機にプッシュログイン要求を自動的に送信し、プッシュが使用できない場合は通話に戻ります。これにより、パスコード認証が実質的に無効になります。の場合 `false`、ユーザは認証方式を選択するように求められます。 で設定した場合は `autopush = true`、を設定することをお勧めします `max-prompts = 1`。	

`-max-prompts`	ユーザーが2番目のファクターで認証に失敗した場合、Duoはユーザーに再度認証を求めるプロンプトを表示します。このオプションは、アクセスを拒否する前にDuoが表示するプロンプトの最大数を設定します。には、 `2`、または `3` を指定する必要があります `1`。デフォルト値はです `1`。 たとえば、ユーザが最初のプロンプトで正常に認証する必要がある場合 `max-prompts = 1`、ユーザが最初のプロンプトで誤った情報を入力した場合、 `max-prompts = 2`再度認証を求めるプロンプトが表示されます。 で設定した場合は `autopush = true`、を設定することをお勧めします `max-prompts = 1`。 最高のエクスペリエンスを得るために、publickey認証のみを使用するユーザは常に `max-prompts`に設定され `1`ます。	
`-enabled`	Duo 2要素認証を有効にします。デフォルトではに設定され `true`ます。有効にすると、設定されているパラメータに従って、SSHログイン時にDuo 2要素認証が実行されます。Duoが無効（に設定）の場合、 `false`Duo認証は無視されます。	
`-pushinfo`	このオプションは、アクセスされているアプリケーションまたはサービスの名前など、プッシュ通知の追加情報を提供します。これにより、ユーザは正しいサービスにログインしていることを確認し、セキュリティレイヤを追加できます。	

カスタムロールの定義

次の値は、コマンドでカスタムロールを定義するときに指定し `security login role create`ます。の詳細については `security login role create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	（オプション）ロールに関連付けられているStorage VM（ONTAP CLIではVserverと表示されます）の名前。	
`-role`	ロールの名前。	
`-cmddirname`	ロールでアクセスできるコマンドまたはコマンド ディレクトリ。コマンド サブディレクトリの名前は二重引用符（"）で囲む必要があります。たとえば、 `"volume snapshot"` です。すべてのコマンドディレクトリを指定するには、と入力する必要があります `DEFAULT`。	

-access	（任意）ロールのアクセスレベル。コマンドディレクトリの場合： • none（カスタムロールのデフォルト値）コマンドディレクトリ内のコマンドへのアクセスを拒否します。 • readonly`コマンドディレクトリとそのサブディレクトリ内のコマンドへのアクセスを許可`show • `all`コマンドディレクトリとそのサブディレクトリ内のすべてのコマンドへのアクセスを許可します。 for *nonintrinsic commands*（末尾が、、 modify、、 delete`または `show`でないコマンド`create）： • none（カスタムロールのデフォルト値）コマンドへのアクセスを拒否します。 • `readonly`該当なし • `all`コマンドへのアクセスを許可します。 組み込みコマンドへのアクセスを許可または拒否するには、コマンドディレクトリを指定する必要があります。	
-query	（任意）アクセスレベルのフィルタリングに使用されるクエリーオブジェクト。コマンドまたはコマンドディレクトリ内のコマンドの有効なオプションの形式で指定します。クエリオブジェクトは二重引用符（"）で囲む必要があります。たとえば、コマンドディレクトリがの場合、 volume`クエリオブジェクトは `"-aggr aggr0"`アグリゲートに対してのみアクセスを有効にします `aggr0。	

ユーザアカウントに公開鍵を関連付ける

次の値は、コマンドでユーザアカウントにSSH公開鍵を関連付けるときに指定します `security login publickey create`。の詳細については `security login publickey create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	（オプション）アカウントがアクセスするStorage VMの名前。	
`-username`	アカウントのユーザ名。デフォルト値。 `admin`クラスタ管理者のデフォルト名です。	
`-index`	公開鍵のインデックス番号。デフォルト値は、アカウントに対して最初に作成された鍵では0、それ以外の場合は既存の一番大きいインデックス番号に1を加えた値です。	
`-publickey`	OpenSSH公開鍵。鍵は二重引用符（"）で囲む必要があります。	
`-role`	アカウントに割り当てられているアクセス制御ロール。	
`-comment`	（オプション）公開鍵についての説明。テキストを二重引用符（"）で囲む必要があります。	

`-x509-certificate`	（オプション）ONTAP 9.13.1以降では、X.509証明書とSSH公開鍵の関連付けを管理できます。 X.509証明書をSSH公開鍵に関連付けると、証明書が有効かどうかをSSHログイン時にONTAPがチェックします。証明書の有効期限が切れている、または証明書が失効している場合、ログインは許可されず、関連付けられているSSH公開鍵は無効になります。有効な値は次のとおりです。 • `install`：指定したPEMでエンコードされたX.509証明書をインストールし、SSH公開鍵に関連付けます。インストールする証明書の全文を含めます。 • `modify`：PEMでエンコードされた既存のX.509証明書を指定された証明書に更新し、SSH公開鍵に関連付けます。新しい証明書の全文を含めます。 • `delete`：既存のX.509証明書とSSH公開鍵の関連付けを削除します。	

動的認証グローバル設定の構成

ONTAP 9 .15.1以降では、コマンドで次の値を指定します `security dynamic-authorization modify`。の詳細については `security dynamic-authorization modify`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	信頼スコア設定を変更する必要があるStorage VMの名前。このパラメータを省略すると、クラスタレベルの設定が使用されます。	

`-state`	ダイナミック許可モード。有効な値： • `disabled`：（デフォルト）動的認可はディセーブルです。 • `visibility`:このモードは、ダイナミック認可のテストに役立ちます。このモードでは、信頼スコアはすべての制限されたアクティビティでチェックされますが、強制はされません。ただし、拒否された、または追加の認証チャレンジの対象となるアクティビティはすべてログに記録されます。 • `enforced`：モードでのテストを完了した後の使用を想定して`visibility`います。このモードでは、すべての制限されたアクティビティで信頼スコアがチェックされ、制限条件が満たされるとアクティビティ制限が適用されます。抑制間隔も適用されるため、指定された間隔内での追加の認証チャレンジを防ぐことができます。	
`-suppression-interval`	指定された間隔内で追加の認証チャレンジを防止します。間隔はISO-8601形式で、1分～1時間の値を指定できます。0に設定すると、抑制間隔はディセーブルになり、認証チャレンジが必要な場合は常にユーザにプロンプトが表示されます。	
`-lower-challenge-boundary`	多要素認証（MFA）チャレンジの割合の下限。有効な範囲は0～99です。値100は無効です。これにより、すべての要求が拒否されます。デフォルト値は0です。	

-upper-challenge-boundary	上限MFAチャレンジパーセンテージの境界。有効な範囲は0～100です。これは下部境界の値以上である必要があります。100の値は、すべての要求が拒否されるか、追加の認証チャレンジの対象となることを意味します。チャレンジなしで許可される要求はありません。デフォルト値は90です。	

CA署名済みサーバ デジタル証明書のインストール

次の値は、コマンドでStorage VMをSSLサーバとして認証する際に使用するデジタル証明書署名要求（CSR）を生成するときに指定します `security certificate generate-csr`。の詳細については `security certificate generate-csr`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-common-name	証明書の名前。Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）またはカスタム共通名です。	
-size	秘密鍵のビット数。この値が高いほど、鍵のセキュリティは向上します。デフォルト値はです `2048`。指定できる値は `512`、、 `1024` `1536`、および `2048`です。	
-country	Storage VMの国（2文字のコード）。デフォルト値はです `US`。コードのリストについては、を参照してください"ONTAPコマンド リファレンス"。	
-state	Storage VMの都道府県。	
-locality	Storage VMの局所性。	
-organization	Storage VMの組織。	
-unit	Storage VMの組織内の単位。	
-email-addr	Storage VMの管理者連絡先のEメールアドレス。	

-hash-function	証明書の署名に使用する暗号化ハッシュ関数。デフォルト値はです SHA256。指定できる値は SHA1、SHA256、および `MD5`です。	

次の値は、コマンドで、クラスタまたはStorage VMをSSLサーバとして認証する際に使用するCA署名デジタル証明書をインストールするときに指定します security certificate install。次の表には、アカウント設定に関連するオプションのみを示します。の詳細については security certificate install、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-vserver	証明書をインストールするStorage VMの名前。	
-type	証明書のタイプ。 • `server`サーバ証明書および中間証明書 • `client-ca`SSLクライアントのルートCAの公開鍵証明書 • `server-ca`ONTAPがクライアントであるSSLサーバのルートCAの公開鍵証明書 • `client`ONTAPをSSLクライアントとして使用するための自己署名またはCA署名のデジタル証明書および秘密鍵	

Active Directoryドメインコントローラアクセスの設定

次の値は、データStorage VM用のSMBサーバを設定済みで、Storage VMをゲートウェイまたは_tunnel_（Active Directoryドメインコントローラによるクラスタへのアクセスの場合）として設定する場合は、コマンドで指定します security login domain-tunnel create。の詳細については security login domain-tunnel create、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
-vserver	SMBサーバが設定されているStorage VMの名前。	

次の値は、SMBサーバを設定していない場合に、コマンドでActive DirectoryドメインにStorage VMコンピュータアカウントを作成するときに指定します vserver active-directory create。の詳細については vserver active-directory create、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値

`-vserver`	Active Directoryコンピュータアカウントを作成するStorage VMの名前。	
`-account-name`	コンピュータアカウントのNetBIOS名。	
`-domain`	Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）。	
`-ou`	ドメイン内の組織単位。デフォルト値はです `CN=Computers`。ONTAPは、この値をドメイン名に追加して、Active Directory識別名を生成します。	

LDAPまたは**NIS**サーバアクセスの設定

次の値は、コマンドでStorage VMのLDAPクライアント設定を作成するときに指定します `vserver services name-service ldap client create`。の詳細については `vserver services name-service ldap client create`、を"ONTAPコマンド リファレンス"参照してください。

次の表には、アカウント設定に関連するオプションのみを示します。

フィールド	説明	あなたの価値
`-vserver`	クライアント設定のStorage VMの名前。	
`-client-config`	クライアント設定の名前。	
`-ldap-servers`	クライアントが接続するLDAPサーバのIPアドレスおよびホスト名をカンマで区切ったリスト。	
`-schema`	クライアントがLDAPクエリの作成に使用するスキーマ。	

`-use-start-tls`	クライアントがStart TLSを使用してLDAPサーバとの通信を暗号化するか、または `false` を使用するか（`true`）。 Start TLSは、データStorage VMへのアクセスでのみサポートされます。管理Storage VMへのアクセスではサポートされません。	

次の値は、コマンドでLDAPクライアント設定をStorage VMに関連付けるときに指定します `vserver services name-service ldap create`。の詳細については `vserver services name-service ldap create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	クライアント設定を関連付けるStorage VMの名前。	
`-client-config`	クライアント設定の名前。	
`-client-enabled`	Storage VMがLDAPクライアント設定を使用できるか、または `false` を使用できるか（`true`）。	

次の値は、コマンドでStorage VMにNISドメイン設定を作成するときに指定します `vserver services name-service nis-domain create`。の詳細については `vserver services name-service nis-domain create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	ドメイン設定を作成するStorage VMの名前。	
`-domain`	ドメインの名前。	
`-nis-servers`	ドメイン設定で使用されるNISサーバのIPアドレスとホスト名をカンマで区切ったリスト。	

次の値は、コマンドでネームサービスソースの参照順序を指定するときに指定します `vserver services name-service ns-switch create`。の詳細については `vserver services name-service ns-switch create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-vserver`	ネームサービスの参照順序を設定するStorage VMの名前。	
`-database`	ネームサービスデータベース： • `hosts`ファイルトDNSネエムサアヒス • `group`ファイル、LDAP、オヨヒNISノネエムサアヒス • `passwd`ファイル、LDAP、オヨヒNISノネエムサアヒス • `netgroup`ファイル、LDAP、オヨヒNISノネエムサアヒス • `namemap`ファイルトLDAPネエムサアヒス	
`-sources`	ネームサービスソースの検索順序（カンマで区切ったリスト）： • `files` • `dns` • `ldap` • `nis`	

SAMLアクセスの設定

SAML認証を設定するには、コマンドでSAML .3以降のONTAP 9値を指定します `security saml-sp create`。の詳細については `security saml-sp create`、を"ONTAPコマンド リファレンス"参照してください。

フィールド	説明	あなたの価値
`-idp-uri`	アイデンティティプロバイダ（IdP）メタデータのダウンロード元のIdPホストのFTPアドレスまたはHTTPアドレス。	
`-sp-host`	SAMLサービスプロバイダホスト（ONTAPシステム）のホスト名またはIPアドレス。デフォルトでは、クラスタ管理LIFのIPアドレスが使用されます。	

`-cert-ca`および `-cert-serial`、または `-cert-common-name`	サービスプロバイダホスト（ONTAPシステム）のサーバ証明書の詳細。サービスプロバイダの証明書発行認証局(CA)と証明書のシリアル番号、またはサーバー証明書の共通名のいずれかを入力できます。	
`-verify-metadata-server`	IdPメタデータサーバのIDの検証が必要か `true`、または `false`を参照）。この値は常にに設定することを推奨します `true`。	

ログインアカウントの作成

ONTAPログインアカウントの作成について

クラスタおよび SVM の管理者アカウントは、ローカルまたはリモートのいずれかとして有効にできます。ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。ADアカウント情報はドメインコントローラに保存されます。LDAPおよびNISアカウントは、LDAPサーバおよびNISサーバ上に存在します。

クラスタ管理者とSVM管理者

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

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

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

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

命名規則

リモートクラスタおよびSVMの管理者アカウントには、次の汎用名は使用できません。

- "adm"
- "ビン"
- "CLI"
- "デーモン"
- "ftp"
- "ゲーム"

- "停止"
- "LP"
- "メール"
- "男"
- "naroot"
- " NetApp "
- "ニュース"
- "誰もいない"
- "演算子"
- "ルート"
- "シャットダウン"
- "sshd"
- "同期"
- "sys"
- " uucp"
- "WWW"

マージされたロール

同じユーザに対して複数のリモートアカウントを有効にすると、そのユーザには各アカウントに対して指定されたロールがすべて割り当てられます。つまり、LDAPまたはNISアカウントにロールが割り当てられ、同じユーザのADグループアカウントにロールが割り当てられている `vsadmin-volume`場合、 `vsadmin`ADユーザはより包括的な機能を使用してログインし `vsadmin`ます。ロールは、 _ merged__ と呼ばれます。

ローカルアカウントアクセスを有効にする

ローカル**ONTAP**アカウントアクセスの有効化について

ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。コマンドを使用して、ローカルアカウントが管理またはデータSVMにアクセスできるようにすることができます `security login create`。

関連情報

- "security login create"

ONTAPアカウントパスワードアクセスの有効化

コマンドを使用して、管理者アカウントがパスワードを使用して管理またはデータSVMにアクセスできるようにすることができます `security login create`。コマンドを入力すると、パスワードの入力を求められます。

タスクの内容

ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追

加できます `security login modify`。

の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. ローカル管理者アカウントがパスワードを使用して SVM にアクセスできるようにします。

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   次のコマンドは、事前定義されたロールが割り当てられた `backup`クラスタ管理者アカウントが、パスワードを使用した管理SVMへのアクセスを`engCluster`許可し `admin1`ます。コマンドを入力すると、パスワードの入力を求められます。

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPアカウントの**SSH**公開鍵アクセスの有効化

コマンドを使用して、管理者アカウントがSSH公開鍵を使用して管理またはデータSVMにアクセスできるようにすることができます `security login create`。

タスクの内容

- アカウントがSVMにアクセスするためには、アカウントに公開鍵を関連付けておく必要があります。

  ユーザアカウントへの公開鍵の関連付け

  このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追加できます `security login modify`。

  の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

クラスタでFIPSモードを有効にする場合は、サポートされているキーアルゴリズムのない既存のSSH公開鍵アカウントを、サポートされるキータイプで再設定する必要があります。FIPSを有効にする前にアカウントを再設定する必要があります。そうしないと、管理者認証が失敗します。

次の表に、ONTAP SSH接続でサポートされるホストキータイプアルゴリズムを示します。これらのキータイプは、SSH公開認証の設定には適用されません。

ONTAP リリース	FIPSモードでサポートされるキータイプ	FIPS以外のモードでサポートされるキータイプ
9.11.1以降	ECDSA - sha2 - nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss+ ssh-rsa
9.10.1以前	ECDSA - sha2 -nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss+ ssh-rsa

ssh-ed25519ホスト・キー・アルゴリズムのサポートは、ONTAP 9 .11.1以降で削除されました。

詳細については、を参照してください "FIPS を使用してネットワークセキュリティを設定する"。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. ローカル管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにします。

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   次のコマンドは、事前定義のロールが割り当てられた `vsadmin-volume`SVM管理者アカウントが、SSH公開鍵を使用してSVMにアクセス`engData1`できるようにし `svmadmin1`ます。

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

終了後

管理者アカウントに公開鍵が関連付けられていない場合は、アカウントがSVMにアクセスする前に関連付けておく必要があります。

ユーザアカウントへの公開鍵の関連付け

多要素認証（**MFA**）アカウントを有効にする

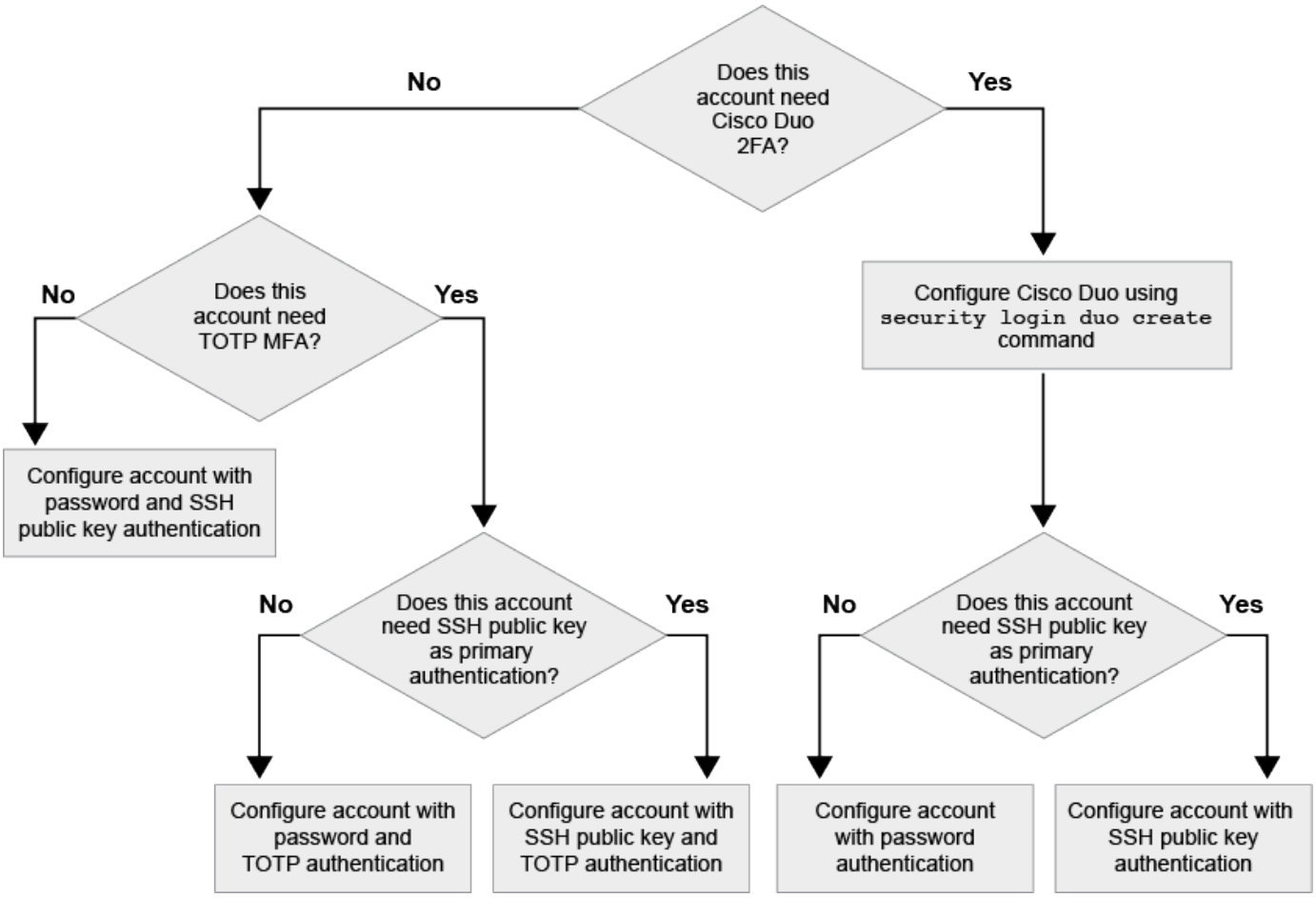
ONTAP多要素認証の詳細

多要素認証（MFA）を使用すると、ユーザが管理Storage VMまたはデータStorage VMにログインする際に2つの認証方式を指定する必要があるため、セキュリティを強化できます。

ONTAPのバージョンに応じて、SSH公開鍵、ユーザパスワード、および時間ベースのワンタイムパスワード（TOTP）を組み合わせて多要素認証に使用できます。Cisco Duo（ONTAP 9 14.1以降）を有効にして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

使用可能なバージョン	最初の認証方法	2番目の認証方法
ONTAP 9 .14.1	SSH公開鍵	TOTP
	ユーザパスワード	TOTP
	SSH公開鍵	Cisco Duo
	ユーザパスワード	Cisco Duo
ONTAP 9 .13.1	SSH公開鍵	TOTP
	ユーザパスワード	TOTP
ONTAP 9.3	SSH公開鍵	ユーザパスワード

MFAが設定されている場合は、クラスタ管理者が最初にローカルユーザアカウントを有効にしてから、ローカルユーザがアカウントを設定する必要があります。



SSHおよび**TOTP**を使用した**ONTAP**多要素認証の有効化

多要素認証（MFA）を使用すると、管理SVMまたはデータSVMにログインする際にユーザに2つの認証方式の指定を要求することで、セキュリティを強化できます。

タスクの内容

- このタスクを実行するには、クラスタ管理者である必要があります。
- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追加できます `security login modify`。

  の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

  "管理者に割り当てられているロールの変更"

- 認証に公開鍵を使用している場合は、アカウントがSVMにアクセスする前にアカウントに公開鍵を関連付ける必要があります。

  "ユーザアカウントに公開鍵を関連付ける"

  このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ONTAP 9.12.1以降では、FIDO2（Fast Identity Online）またはPIV（Personal Identity Verification）認証標準を使用して、SSHクライアントMFAにYubikeyハードウェア認証デバイスを使用できます。

SSH公開鍵とユーザパスワードを使用して**MFA**を有効にする

3以降では、クラスタ管理者がONTAP 9公開鍵とユーザパスワードを使用して、MFAを使用してログインするためのローカルユーザアカウントを設定できます。

1. ローカルユーザアカウントでSSH公開鍵とユーザパスワードを使用してMFAを有効にします。

```
security login create -vserver <svm_name> -user-or-group-name
<user_name> -application ssh -authentication-method <password|publickey>
-role admin -second-authentication-method <password|publickey>
```

   次のコマンドでは、事前定義された `admin`ロールのSVM管理者アカウントで、SSH公開鍵とユーザパスワードの両方を使用してSVMにログインする`engData1`必要があり `admin2`ます。

```
cluster-1::> security login create -vserver engData1 -user-or-group-name
admin2 -application ssh -authentication-method publickey -role admin
-second-authentication-method password

Please enter a password for user 'admin2':
Please enter it again:
Warning: To use public-key authentication, you must create a public key
for user "admin2".
```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

TOTPで**MFA**を有効にする

SSH.13.1以降では、ONTAP 9公開鍵またはユーザパスワードと時間ベースのワンタイムパスワード（TOTP）の両方を使用してローカルユーザに管理SVMまたはデータSVMへのログインを要求することで、セキュリティを強化できます。TOTPを使用してMFAのアカウントを有効にしたあと、ローカルユーザはにログインする必要があります"設定を完了します"。

TOTPは、現在の時刻を使用してワンタイムパスワードを生成するコンピュータアルゴリズムです。TOTPを使用する場合は、常にSSH公開鍵またはユーザパスワードに続く2番目の認証形式になります。

開始する前に

これらのタスクを実行するには、ストレージ管理者である必要があります。

手順

最初の認証方法としてユーザパスワードまたはSSH公開鍵を使用し、2番目の認証方法としてTOTPを使用してMFAを設定できます。

ユーザパスワードと**TOTP**で**MFA**を有効にする

1. ユーザパスワードとTOTPを使用して、ユーザアカウントで多要素認証を有効にします。

   新規ユーザーアカウントの場合

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   既存のユーザーアカウントの場合

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. TOTPを使用したMFAが有効になっていることを確認します。

   ```
   security login show
   ```

SSH公開鍵と**TOTP**を使用して**MFA**を有効にする

1. SSH公開鍵とTOTPを使用した多要素認証のユーザアカウントを有効にします。

   新規ユーザーアカウントの場合

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   既存のユーザーアカウントの場合

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

2. TOTPを使用したMFAが有効になっていることを確認します。

```
security login show
```

の詳細については `security login show`、を"ONTAPコマンド リファレンス"参照してください。

終了後

- 管理者アカウントに公開鍵が関連付けられていない場合は、アカウントがSVMにアクセスする前に関連付けておく必要があります。

  "ユーザアカウントへの公開鍵の関連付け"

- TOTPを使用したMFAの設定を完了するには、ローカルユーザがログインする必要があります。

  "TOTPを使用したMFA用のローカルユーザアカウントの設定"

関連情報

- "ONTAP 9での多要素認証（TR-4647）"
- "ONTAPコマンド リファレンス"

TOTPを使用した**MFA**用のローカル**ONTAP**ユーザアカウントの設定

ONTAP 9.13.1以降では、時間ベースのワンタイムパスワード（TOTP）を使用して多要素認証（MFA）でユーザアカウントを設定できます。

開始する前に

- ユーザアカウントの第2の認証方法として、ストレージ管理者が必要です"TOTPでMFAを有効にする"。
- プライマリユーザアカウントの認証方法は、ユーザパスワードまたは公開SSHキーである必要があります。
- スマートフォンと連携するようにTOTPアプリを設定し、TOTPシークレットキーを作成する必要があります。

  Microsoft Authenticator、Google Authenticator、Authy、およびその他のTOTP互換オーセンティケータがサポートされています。

手順

1. 現在の認証方法でユーザーアカウントにログインします。

   現在の認証方法は、ユーザパスワードまたはSSH公開鍵である必要があります。

2. アカウントでTOTP設定を作成します。

```
security login totp create -vserver "<svm_name>" -username
"<account_username >"
```

3. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

関連情報

- "セキュリティ ログイン トップ 作成"
- "セキュリティ ログイン トップ 表示"

ONTAPユーザアカウントの**TOTP**シークレットキーのリセット

アカウントのセキュリティを保護するために、TOTPシークレットキーが侵害されたり紛失したりした場合は、それを無効にして新しいシークレットキーを作成する必要があります。

キーが侵害された場合に**TOTP**をリセット

TOTPシークレットキーが侵害されたにもかかわらずアクセスできる場合は、侵害されたキーを削除して新しいキーを作成できます。

1. ユーザパスワードまたはSSH公開鍵と侵害されたTOTPシークレットキーを使用してユーザアカウントにログインします。
2. 侵害されたTOTPシークレットキーを削除します。

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 新しいTOTPシークレットキーを作成します。

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver <svm_name> -username
<account_username>
```

キーを紛失した場合に**TOTP**をリセット

TOTPシークレットキーが失われた場合は、ストレージ管理者にに問い合わせてください"キーを無効にします"。キーが無効になったら、最初の認証方法を使用してログインし、新しいTOTPを設定できます。

開始する前に

ストレージ管理者がTOTPシークレットキーを無効にする必要があります。ストレージ管理者アカウントがない場合は、ストレージ管理者に連絡してキーを無効にしてください。

手順

1. ストレージ管理者がTOTPシークレットを無効にしたら、プライマリの認証方法を使用してローカルアカウントにログインします。
2. 新しいTOTPシークレットキーを作成します。

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver <svm_name> -username
<account_username>
```

関連情報

- "セキュリティ ログイン トップ 作成"
- "セキュリティ ログイン トップ 削除"
- "セキュリティ ログイン トップ 表示"

ONTAPユーザアカウントの**TOTP**シークレットキーを無効にする

ローカルユーザの時間ベースのワンタイムパスワード（TOTP）シークレットキーが失われた場合、失われたキーをストレージ管理者が無効にしてからユーザが新しいTOTPシークレットキーを作成する必要があります。

タスクの内容

このタスクは、クラスタ管理者アカウントからのみ実行できます。

ステップ

1. TOTPシークレットキーを無効にします。

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

の詳細については `security login totp modify`、を"ONTAPコマンド リファレンス"参照してください。

コマンドを使用して、管理者アカウントがSSL証明書を使用して管理またはデータSVMにアクセスできるようにすることができます `security login create`。

タスクの内容

- アカウントがSVMにアクセスするためには、CA署名済みサーバデジタル証明書をインストールしておく必要があります。

  CA署名済みサーバ証明書の生成とインストール

  このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追加できます `security login modify`。

  管理者に割り当てられているロールの変更

> クラスタ管理者アカウントの場合、証明書認証は、 `ontapi`の `rest`各アプリケーションでサポートされ `http`ます。SVM管理者アカウントの場合、証明書認証はアプリケーションと `rest`アプリケーションでのみサポートされ `ontapi`ます。

ステップ

1. ローカル管理者アカウントがSSL証明書を使用してSVMにアクセスできるようにします。

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   次のコマンドは、デフォルト `vsadmin`ロールのSVM管理者アカウントが、SSLデジタル証明書を使用してSVMにアクセス`engData2`できるようにし `svmadmin2`ます。

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

終了後

CA署名済みサーバデジタル証明書がインストールされていない場合は、アカウントがSVMにアクセスする前にインストールしておく必要があります。

CA署名済みサーバ証明書の生成とインストール

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

Active Directory ONTAPアカウントアクセスの有効化

コマンドを使用して、Active Directory（AD）のユーザアカウントまたはグループアカウントが管理SVMまたはデータSVMにアクセスできるようにすることができます `security login create`。ADグループのすべてのユーザは、グループに割り当てられたロールを使用してSVMにアクセスできます。

タスクの内容

- アカウントがSVMにアクセスするためには、ADドメインコントローラからクラスタまたはSVMへのアクセスを設定しておく必要があります。

  Active Directoryドメインコントローラアクセスの設定

  このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- SSH.13.1以降では、ユーザパスワードを使用して、プライマリまたはセカンダリの認証方式としてONTAP 9公開鍵を使用できます。

  SSH公開鍵をプライマリ認証として使用することを選択した場合、AD認証は行われません。

- ONTAP 9 .11.1以降では、AD LDAPサーバでサポートされている場合にを使用できます"ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"。
- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追加できます `security login modify`。

  の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

  管理者に割り当てられているロールの変更

ADグループアカウントへのアクセスは、、 `ontapi`および `rest`アプリケーションでのみサポートされ `SSH`ます。ADグループは、多要素認証に一般的に使用されるSSH公開鍵認証ではサポートされません。

開始する前に

- クラスタ時間とADドメインコントローラの時間の誤差が5分以内になるように同期する必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. ADユーザまたはグループの管理者アカウントがSVMにアクセスできるようにします。

   ◦ ADユーザの場合：*

ONTAPバージョン	第1の認証方式	第2の認証方式	コマンド
9.13.1以降	公開鍵	なし	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

9.13.1以降	ドメイン	公開鍵	新規ユーザーの場合
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			既存のユーザーの場合
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0以降	ドメイン	なし	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

◦ ADグループの場合：*

ONTAPのバージョン	第1の認証方式	第2の認証方式	コマンド
9.0以降	ドメイン	なし	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

終了後

ADドメインコントローラからクラスタまたはSVMへのアクセスを設定していない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

Active Directoryドメインコントローラアクセスの設定

関連情報

- "security login create"

LDAPまたは**NIS ONTAP**アカウントアクセスの有効化

コマンドを使用して、LDAPまたはNISのユーザアカウントが管理またはデータSVMにアクセスできるようにすることができます `security login create`。LDAPサーバまたはNISサーバからSVMへのアクセスを設定していない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

タスクの内容

- グループアカウントはサポートされていません。
- アカウントがSVMにアクセスするためには、LDAPサーバまたはNISサーバからSVMへのアクセスを設定しておく必要があります。

  LDAPサーバまたはNISサーバアクセスの設定

  このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追加できます `security login modify`。

  の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

  管理者に割り当てられているロールの変更

- .4以降では、LDAPサーバまたはONTAP 9サーバを介したリモートユーザに対して多要素認証（MFA）がサポートされます。
- ONTAP 9 .11.1以降では、LDAPサーバでサポートされていればを使用できます"ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"。

- LDAPの既知の問題のため、LDAPユーザアカウント情報のフィールド（、 `userPassword`など）では（コロン）文字を `gecos`使用しないで ':' ください。そうしないと、そのユーザの検索操作が失敗します。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. LDAPまたはNISのユーザまたはグループアカウントがSVMにアクセスできるようにします。

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   "ログインアカウントの作成または変更"

   次のコマンドは、事前定義されたロールが割り当てられた `backup`LDAPまたはNISのクラスタ管理者アカウントが、管理SVMにアクセスできるengClusterようにし `guest2`ます。

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

2. LDAPユーザまたはNISユーザのMFAログインを有効にします。

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh
   -authentication-method nsswitch -role admin -is-ns-switch-group no -second
   -authentication-method publickey
   ```

   認証方法はと指定でき、2つ目の認証方法はと `nsswitch`指定できます `publickey`。

   次の例は、MFA認証を有効にします。

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2
   -application ssh -authentication-method nsswitch -vserver
   cluster-1 -second-authentication-method publickey"
   ```

終了後

LDAPサーバまたはNISサーバからSVMへのアクセスを設定していない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

LDAPサーバまたはNISサーバアクセスの設定

関連情報

- "セキュリティログイン"

アクセス制御ロールを管理します。

ONTAPアクセス制御ロールの管理について

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

ONTAP管理者に割り当てられているロールを変更する

コマンドを使用すると、クラスタ管理者アカウントまたはSVM管理者アカウントのロールを変更できます `security login modify`。事前定義またはカスタムのロールを割り当てることができます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. クラスタ管理者または SVM 管理者のロールを変更します。

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   "ログインアカウントの作成または変更"

   次のコマンドは、ADクラスタ管理者アカウントのロールを事前定義された `readonly`ロールに変更し `DOMAIN1\guest1`ます。

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   次のコマンドは、ADグループアカウント内のSVM管理者アカウントのロールをカスタムロールに `vol_role`変更します `DOMAIN1\adgroup`。

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP管理者のカスタムロールの定義

カスタムロールを定義するには、コマンドを使用し `security login role create`ます。このコマンドは、必要な回数だけ実行して、ロールに関連付ける機能を正確に組み合わせることができます。

タスクの内容

- ONTAPコマンドまたはコマンドディレクトリへのアクセスは、ロール（事前定義またはカスタム）によって許可または拒否されます。

  コマンドディレクトリ(`volume`など）は、関連するコマンドとコマンドサブディレクトリのグループです。この手順で説明されている場合を除き、コマンドディレクトリへのアクセスを許可または拒否すると、ディレクトリおよびそのサブディレクトリ内の各コマンドへのアクセスが許可または拒否されます。

- 特定のコマンドまたはサブディレクトリへのアクセスは、親ディレクトリへのアクセスよりも優先されます。

  コマンドディレクトリを使用してロールを定義したあとに、特定のコマンドまたは親ディレクトリのサブディレクトリに対して別のアクセスレベルで再度定義した場合、コマンドまたはサブディレクトリに指定されたアクセスレベルは親のアクセスレベルよりも優先されます。

> クラスタ管理者のみが使用できるコマンドやコマンドディレクトリ（コマンドディレクトリなど） `security`へのアクセスを許可するロールをSVM管理者に割り当てることはできません。 `admin`

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. カスタムロールを定義します。

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   次のコマンドは、ロールに対し、コマンドディレクトリ内のコマンドへのフルアクセス `volume`と、サブディレクトリ内のコマンドへの読み取り専用アクセスを `volume snapshot`許可し `vol_role`ます。

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   次のコマンドは、ロールに対し、コマンドディレクトリ内のコマンドへの読み取り専用アクセス `storage`、サブディレクトリ内のコマンドへのアクセスなし、 `storage encryption`および非組み込みコマンドへのフルアクセスを `storage aggregate plex offline`許可し `SVM_storage`ます。

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

の詳細については `security login role create`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "security login role create"
- "ストレージアグリゲートのプレックスがオフライン"
- "ストレージ暗号化"

ONTAPクラスタ管理者の事前定義されたロール

ほとんどの場合、クラスタ管理者用に事前定義されたロールで十分です。必要に応じてカスタムロールを作成できます。デフォルトでは、クラスタ管理者には事前定義されたロールが割り当てられ `admin`ます。

次の表に、クラスタ管理者用の事前定義されたロールを示します。

ロール	アクセスレベル	コマンドまたはコマンドディレクトリに移動します
管理者	すべて	すべてのコマンドディレクトリ(`DEFAULT`)
ADMIN-NO-FSA（ONTAP 9.12.1以降で使用可能）	読み取り / 書き込み	• すべてのコマンドディレクトリ(`DEFAULT`) • `security login rest-role` • `security login role`

読み取り専用です	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	なし
volume file show-disk-usage	AutoSupport	すべて
• set • system node autosupport	なし	その他すべてのコマンドディレクトリ(DEFAULT)
バックアップ	すべて	vserver services ndmp
読み取り専用	volume	なし
その他すべてのコマンドディレクトリ(DEFAULT)	読み取り専用	すべて
• security login password 自分のユーザアカウントのローカルパスワードとキーの情報のみを管理する場合 • set	• ONTAP 9.8以降、読み取り専用 • ONTAP 9.8より前のバージョンでは、なし	security

読み取り専用	その他すべてのコマンドディレクトリ(DEFAULT)	SnapLock
すべて	• set • volume create • volume modify • volume move • volume show	なし
• volume move governor • volume move recommend	なし	その他すべてのコマンドディレクトリ(DEFAULT)
なし	なし	すべてのコマンドディレクトリ(DEFAULT)

`autosupport`ロールは事前定義されたアカウントに割り当てられ `autosupport`、AutoSupport OnDemandで使用されます。ONTAPでは、アカウントを変更または削除することはできません `autosupport`。また、ONTAPでは、他のユーザアカウントにロールを割り当てることもできません `autosupport`。

関連情報

- "セキュリティログイン"
- "設定"
- "ボリューム"
- "SVMサービスNDMP"

ONTAP SVM管理者の事前定義されたロール

SVM管理者用に、ほとんどのニーズに合わせて事前定義されたロールが用意されています。必要に応じてカスタムロールを作成できます。デフォルトでは、SVM管理者には事前定義されたロールが割り当てられ`vsadmin`ます。

次の表に、SVM管理者用の事前定義されたロールを示します。

ロール名	機能

vsadmin	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、およびファイルの管理 • LUNの管理 • SnapLock処理の実行（privileged deleteを除く） • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
vsadmin-volume	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、およびファイルの管理 • LUNの管理 • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • ネットワークインターフェイスの監視 • SVMの健全性の監視
vsadmin-protocol	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • LUNの管理 • ネットワークインターフェイスの監視 • SVMの健全性の監視

vsadmin-backup	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • NDMP処理の管理 • リストアしたボリュームの読み取り/書き込み許可 • SnapMirror関係とSnapshotの管理 • ボリュームとネットワーク情報の表示
vsadmin-snaplock	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、およびファイルの管理 • SnapLock処理の実行（privileged deleteを含む） • プロトコルの設定：NFSとSMB • サービスの設定： DNS 、 LDAP 、 NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視
vsadmin -読み取り専用	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • SVMの健全性の監視 • ネットワークインターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

System Managerを使用した**ONTAP**管理者アクセスの管理

管理者がSystem Managerで実行できる機能は、管理者に割り当てられたロールによって決まります。System Managerには、クラスタ管理者とStorage VM管理者用の事前定義されたロールが用意されています。ロールは管理者アカウントの作成時に割り当てるか、あとで別のロールを割り当てることができます。

アカウントアクセスを有効にした方法によっては、次のいずれかの操作が必要になる場合があります。

- 公開鍵をローカルアカウントに関連付けます。
- CA署名済みサーバデジタル証明書をインストールする。
- AD、LDAP、またはNISアクセスを設定

これらのタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

管理者へのロールの割り当て

次のように、管理者にロールを割り当てます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [Users and Roles]*の横にあるを選択します → 。
3. [ユーザ]*でを選択します + Add 。
4. ユーザー名を指定し、 * 役割 * のドロップダウンメニューで役割を選択します。
5. ユーザのログイン方法とパスワードを指定します。

管理者のロールの変更

管理者のロールを次のように変更します。

手順

1. [クラスタ]>[設定]*をクリックします。
2. ロールを変更するユーザの名前を選択し、ユーザ名の横に表示されるをクリックします ⋮ 。
3. [編集（ Edit ）] をクリックします。
4. [*Role] のドロップダウンメニューで、ロールを選択します。

ONTAPでの **JIT** 権限の昇格へのアクセス

ONTAP 9.17.1以降、クラスタ管理者は"ジャストインタイム（JIT）権限昇格を構成する" ONTAPユーザーが特定のタスクを実行するために一時的に権限を昇格できるようにします。ユーザーにJITが設定されている場合、ユーザーはタスクを実行するために必要な権限を持つロールに一時的に権限を昇格できます。セッションの有効期限が切れると、ユーザーは元のアクセスレベルに戻ります。

クラスタ管理者は、ユーザーがJIT昇格にアクセスできる期間を設定できます。例えば、クラスタ管理者は、30日間（*JIT*有効期間）にわたり、セッションごとに30分（セッション有効期間）のJIT昇格アクセス制限を設定できます。30日間の期間中、ユーザーは必要に応じて何度でも権限を昇格できますが、各セッションは30分に制限されます。

タスクの内容

- JIT権限の昇格は、SSHを使用してONTAPにアクセスするユーザーのみが利用できます。権限の昇格は現在のSSHセッション内でのみ可能ですが、必要に応じて任意の数の同時SSHセッション内で権限を昇格できます。
- JIT 権限の昇格は、パスワード、nsswitch、またはドメイン認証を使用してログインするユーザーに対してのみサポートされます。多要素認証 (MFA) は JIT 権限の昇格ではサポートされていません。
- 構成されたセッションまたは JIT の有効期間が経過した場合、またはクラスター管理者がユーザーの JIT アクセスを取り消した場合、ユーザーの JIT セッションは終了します。

開始する前に

- JIT権限の昇格を利用するには、クラスタ管理者がアカウントのJITアクセスを設定する必要があります。クラスタ管理者は、権限を昇格できるロールと、昇格した権限にアクセスできる期間を決定します。

手順

1. 構成されたロールに権限を一時的に昇格します。

```
security jit-privilege elevate
```

このコマンドを入力すると、ログインパスワードの入力を求められます。アカウントにJITアクセスが設定されている場合、設定されたセッション期間中、昇格されたアクセス権限が付与されます。セッション期間が終了すると、元のアクセスレベルに戻ります。設定されたJIT有効期間内であれば、必要に応じて何度でも権限を昇格できます。

2. JIT セッションの残り時間を表示します。

```
security jit-privilege show-remaining-time
```

現在 JIT セッション中の場合、このコマンドは残り時間を表示します。

3. 必要に応じて、JIT セッションを早めに終了します。

```
security jit-privilege reset
```

現在 JIT セッション中の場合、このコマンドは JIT セッションを終了し、元のアクセス レベルを復元します。

ONTAPで**JIT**権限の昇格を構成する

ONTAP 9.17.1以降、クラスタ管理者はジャストインタイム（JIT）権限昇格を設定して、 ONTAPユーザが特定のタスクを実行するために一時的に権限を昇格できるようにすることができます。ユーザにJITが設定されている場合、一時的に"特権を高める"タスクを実行するために必要な権限を持つロールに切り替えます。セッション期間が終了すると、ユーザーは元のアクセスレベルに戻ります。

クラスター管理者は、ユーザーがJIT昇格にアクセスできる期間を設定できます。例えば、JIT昇格へのユーザーアクセスを、30日間（*JIT*有効期間）にわたり、1セッションあたり30分（セッション有効期間）に制限するように設定できます。30日間の期間中、ユーザーは必要に応じて何度でも権限を昇格できますが、各セッションは30分に制限されます。

JIT 権限昇格は最小権限の原則をサポートしており、ユーザーは昇格された権限を必要とするタスクを、その権限を永続的に付与することなく実行できます。これにより、不正アクセスやシステムへの偶発的な変更のリスクを軽減できます。以下の例は、JIT 権限昇格の一般的なユースケースを示しています。

- 一時的なアクセスを許可する `security login create`そして `security login delete`ユーザーのオンボーディングとオフボーディングを有効にするコマンド。
- 一時的なアクセスを許可する `system node image update`そして `system node upgrade-revert`更新ウィンドウ中に、コマンドアクセスが無効になります。更新が完了すると、コマンドアクセスは無効になります。

- 一時的なアクセスを許可する `cluster add-node`、 `cluster remove-node`、 そして `cluster modify`クラスタの拡張または再構成を有効にします。クラスタの変更が完了すると、コマンドアクセスは取り消されます。
- 一時的なアクセスを許可する `volume snapshot restore`復元操作とバックアップターゲットの管理が可能になります。復元または設定が完了すると、コマンドアクセスは取り消されます。
- 一時的なアクセスを許可する `security audit log show`コンプライアンス チェック中に監査ログのレビューとエクスポートを有効にします。

より広範なJITの一般的な使用例については、こちらをご覧ください。 JITの一般的なユースケース 。

クラスタ管理者は、 ONTAPユーザーの JIT アクセスを設定し、クラスタ全体でグローバルに、または特定の SVM に対してデフォルトの JIT 有効期間を設定できます。

タスクの内容

- JIT権限の昇格は、SSHを使用してONTAPにアクセスするユーザーのみが利用できます。昇格された権限はユーザーの現在のSSHセッション内でのみ利用可能ですが、必要に応じて複数の同時SSHセッション内で権限を昇格できます。
- JIT 権限の昇格は、パスワード、nsswitch、またはドメイン認証を使用してログインするユーザーに対してのみサポートされます。多要素認証 (MFA) は JIT 権限の昇格ではサポートされていません。

開始する前に

- ONTAPクラスタ管理者である必要があります。 `admin`次のタスクを実行するための特権レベル。

グローバル**JIT**設定を変更する

デフォルトのJIT設定は、 ONTAPクラスタ全体、または特定のSVMごとに変更できます。これらの設定により、JITアクセスが設定されているユーザーのデフォルトのセッション有効期間と最大JIT有効期間が決まります。

タスクの内容

- デフォルト `default-session-validity-period`値は1時間です。この設定は、ユーザーがJITセッションで昇格された権限にアクセスできる時間を決定します。この時間を超えると、再度昇格が必要になります。
- デフォルト `max-jit-validity-period`値は90日間です。この設定は、設定された開始日以降、ユーザーがJIT昇格にアクセスできる最大期間を決定します。個々のユーザーに対してJITの有効期間を設定できますが、最大JIT有効期間を超えることはできません。

手順

1. 現在の JIT 設定を確認します。

   ```
   security jit-privilege show -vserver <svm_name>
   ```

   `-vserver`はオプションです。SVMを指定しない場合、コマンドはグローバルJIT設定を表示します。

2. JIT 設定をグローバルまたは SVM に対して変更します。

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

SVMを指定しない場合、コマンドはグローバルJIT設定を変更します。次の例では、SVMのデフォルトのJITセッション期間を45分、最大JIT期間を30日に設定します。 `svm1`：
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

この例では、ユーザーは一度に 45 分間 JIT 昇格にアクセスでき、構成された開始日から最大 30 日間 JIT セッションを開始できます。

ユーザーの **JIT** 権限昇格アクセスを構成する

ONTAPユーザーに JIT 権限の昇格アクセスを割り当てることができます。

手順

1. ユーザーの現在の JIT アクセスを確認します。

```
security jit-privilege user show -username <username>
```

`-username`はオプションです。ユーザー名を指定しない場合、コマンドはすべてのユーザーのJITアクセスを表示します。

2. ユーザーに新しい JIT アクセスを割り当てます。

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- もし `-vserver`指定されていない場合は、クラスター レベルで JIT アクセスが割り当てられます。
- `-role`ユーザーが昇格されるRBACロールです。指定しない場合は、 `-role`デフォルトは `admin` 。
- `-session-validity-period`ユーザーが昇格されたロールにアクセスできる期間です。この期間を過ぎると、新しいJITセッションを開始する必要があります。指定しない場合は、グローバルまたはSVM `default-session-validity-period`が使用されます。
- `-jit-validity-period`設定された開始日以降にユーザーがJITセッションを開始できる最大期間です。指定しない場合は、 `session-validity-period`が使用されます。このパラメータはグローバルまたはSVMを超えることはできません。 `max-jit-validity-period` 。
- `-start-time`ユーザーがJITセッションを開始できる日時です。指定されていない場合は、現在の日時が使用されます。

  次の例では、 `ontap_user`アクセスするには `admin`新しい `JIT` セッションを開始する前に、1時間ロールを実行します。 `ontap_user` 2025年7月1日午後1時から60日間JITセッションを開始できるようになります。+

```
security jit-privilege user create -username ontap_user -role admin -session
-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"
```

3. 必要に応じて、ユーザーの JIT アクセスを取り消します。

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

このコマンドは、ユーザーのJITアクセスを、たとえアクセス期限が切れていなくても取り消します。 `-vserver`が指定されていない場合、JITアクセスはクラスターレベルで取り消されます。ユーザーがアクティブなJITセッションに参加している場合は、セッションが終了します。

JITの一般的なユースケース

以下の表は、JIT権限昇格の一般的なユースケースを示しています。各ユースケースでは、関連するコマンドへのアクセスを提供するためにRBACロールを設定する必要があります。各コマンドは、コマンドとそのパラメータに関する詳細情報が記載されているONTAPコマンドリファレンスにリンクされています。

ユースケース	コマンド	詳細
ユーザーとロールの管理	• `security login create` • `security login delete`	オンボーディングまたはオフボーディング中に、一時的に昇格してユーザーを追加/削除したり、役割を変更したりします。
証明書管理	• `security certificate create` • `security certificate install`	証明書のインストールまたは更新のために短期アクセスを許可します。
SSH/CLI アクセス制御	• `security login create -application ssh`	トラブルシューティングやベンダー サポートのために、一時的に SSH アクセスを許可します。
ライセンス管理	• `system license add` • `system license delete`	機能のアクティブ化または非アクティブ化中にライセンスを追加または削除する権限を付与します。
システムのアップグレードとパッチ適用	• `system node image update` • `system node upgrade-revert`	アップグレードウィンドウに昇格し、その後取り消します。
ネットワークセキュリティ設定	• `security login role create` • `security login role modify`	ネットワーク関連のセキュリティロールへの一時的な変更を許可します。

ユースケース	コマンド	詳細
クラスタ管理	• `cluster add-node` • `cluster remove-node` • `cluster modify`	クラスターの拡張または再構成のために昇格します。
SVMの管理	• `vserver create` • `vserver delete` • `vserver modify`	プロビジョニングまたは廃止のために、SVM 管理者権限を一時的に付与します。
ボリュームの管理	• `volume create` • `volume delete` • `volume modify`	ボリュームのプロビジョニング、サイズ変更、または削除のために昇格します。
Snapshotの管理	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	リカバリ中にスナップショットを削除または復元する場合は昇格します。
ネットワーク設定	• `network interface create` • `network port vlan create`	メンテナンス期間中のネットワーク変更の権限を付与します。
ディスク/アグリゲート管理	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	ディスクの追加や削除、あるいはアグリゲートの管理を行うために昇格します。
データ保護	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	SnapMirror関係を構成または復元するために一時的に昇格します。
パフォーマンス調整	• `qos policy-group create` • `qos policy-group modify`	パフォーマンスのトラブルシューティングやチューニングのために昇格します。
監査ログへのアクセス	• `security audit log show`	コンプライアンス チェック中に監査ログの確認またはエクスポートを行うために一時的に昇格します。

ユースケース	コマンド	詳細
イベントとアラートの管理	• `event notification create` • `event notification modify`	イベント通知または SNMP トラップを構成またはテストするには、Elevate を使用します。
コンプライアンス主導のデータアクセス	• `volume show` • `security audit log show`	監査人が機密データやログを確認できるように、一時的な読み取り専用アクセスを許可します。
特権アクセスのレビュー	• `security login show` • `security login role show`	特権アクセスの確認とレポートのために一時的に昇格します。読み取り専用の昇格アクセスを一定期間のみ許可します。

関連情報

- "クラスタ"
- "イベント通知"
- "network"
- "QoS ポリシーグループ"
- "セキュリティ"
- "SnapMirror"
- "storage"
- "システム"
- "ボリューム"
- "SVM"

管理者アカウントの管理

ONTAP管理者アカウントの管理について

アカウントアクセスを有効にした方法によっては、ローカルアカウントへの公開鍵の関連付け、 CA 署名済みサーバデジタル証明書のインストール、 AD 、 LDAP 、 NIS のアクセスの設定などが必要になる場合があります。これらのタスクはすべて、アカウントアクセスを有効にする前後どちらでも実行できます。

ONTAP管理者アカウントへの公開鍵の関連付け

SSH 公開キー認証の場合、アカウントが SVM にアクセスする前に、公開キーを管理者アカウントに関連付ける必要があります。管理者アカウントにキーを関連付けるには、コマンドを使用し `security login publickey create`ます。

タスクの内容

パスワードとSSH公開鍵の両方を使用してSSH経由でアカウントを認証する場合、アカウントは最初に公開鍵で認証されます。

開始する前に

- SSHキーを生成しておく必要があります。
- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. 管理者アカウントに公開鍵を関連付けます。

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   の詳細については `security login publickey create`、を"ONTAPコマンド リファレンス"参照してください。

2. 公開鍵を表示して変更を確認します。

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   の詳細については `security login publickey show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドは、SVMの `engData1`SVM管理者アカウントに公開鍵を関連付け `svmadmin1`ます。公開鍵にはインデックス番号5が割り当てられます。

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

ONTAP管理者用の**SSH**公開鍵と**X.509**証明書を管理します。

管理者アカウントによるSSH認証のセキュリティを強化するために、一連のコマンドを使用して、SSH公開鍵とそのX.509証明書との関連付けを管理でき `security login publickey`ます。

公開鍵と**X.509**証明書を管理者アカウントに関連付ける

ONTAP 9 .13.1以降では、管理者アカウントに関連付けた公開鍵にX.509証明書を関連付けることができます。これにより、そのアカウントのSSHログイン時の証明書の有効期限または失効チェックのセキュリティが強化されます。

タスクの内容

SSH公開鍵とX.509証明書の両方を使用してSSH経由でアカウントを認証する場合、ONTAPは、SSH公開鍵を使用して認証する前にX.509証明書の有効性をチェックします。証明書の有効期限が切れているか失効している場合、SSHログインは拒否され、公開鍵は自動的に無効になります。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- SSHキーを生成しておく必要があります。
- X.509証明書の有効期限のみを確認する必要がある場合は、自己署名証明書を使用できます。
- X.509証明書の有効期限と失効を確認する必要がある場合は、次の手順を実行します。
  - 認証局（CA）から証明書を受け取っておく必要があります。
  - 証明書チェーン（中間およびルートのCA証明書）は、コマンドを使用してインストールする必要があります `security certificate install`。の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。
  - SSHに対してOCSPを有効にする必要があります。手順については、を参照してください "OCSPを使用してデジタル証明書が有効であることを確認する" 。

手順

1. 公開鍵とX.509証明書を管理者アカウントに関連付けます。

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   の詳細については `security login publickey create`、を"ONTAPコマンド リファレンス"参照してください。

2. 公開鍵を表示して変更を確認します。

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   の詳細については `security login publickey show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドは、公開鍵とX.509証明書をSVMの `engData2`SVM管理者アカウントに関連付け `svmadmin2` ます。公開鍵にはインデックス番号6が割り当てられます。

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

管理者アカウントの**SSH**公開鍵から証明書の関連付けを削除する

公開鍵を保持したまま、アカウントのSSH公開鍵から現在の証明書の関連付けを削除できます。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. 管理者アカウントからX.509証明書の関連付けを削除し、既存のSSH公開鍵を保持します。

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

   の詳細については `security login publickey modify`、を"ONTAPコマンド リファレンス"参照してください。

2. 公開鍵を表示して変更を確認します。

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

例

次のコマンドは、インデックス番号6のSVMのSVM `engData2`管理者アカウントからX.509証明書の関連付けを削除します `svmadmin2`。

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

管理者アカウントから公開鍵と証明書の関連付けを削除する

アカウントから現在の公開鍵と証明書の設定を削除できます。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. 管理者アカウントから公開鍵とX.509証明書の関連付けを削除します。

   `security login publickey delete -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   の詳細については `security login publickey delete`、を"ONTAPコマンド リファレンス"参照してください。

2. 公開鍵を表示して変更を確認します。

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

例

次のコマンドは、インデックス番号7のSVMの `engData3`SVM管理者アカウントから公開鍵とX.509証明書を削除します `svmadmin3`。

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

関連情報

- "セキュリティログイン公開鍵"

ONTAP SSHログイン用のCisco Duo 2FAの設定

ONTAP 9 14.1以降では、SSHログイン時に2要素認証（2FA）にCisco Duoを使用するようにONTAPを設定できます。Duoはクラスタレベルで設定し、デフォルトですべてのユーザアカウントに適用されます。また、Storage VM（旧称Vserver）のレベルでDuoを設定することもできます。その場合は、そのStorage VMのユーザにのみ適用されます。Duoを有効にして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

SSHログインでDuo認証を有効にした場合、ユーザは次回SSHを使用してログインするときにデバイスを登録する必要があります。登録情報については、Cisco Duoを参照して "登録に関するドキュメント"ください。

Cisco Duoでは、ONTAPコマンドラインインターフェイスを使用して次のタスクを実行できます。

- Cisco Duoの設定
- Cisco Duo設定の変更
- Cisco Duo設定の削除
- Cisco Duo設定の表示
- Duoグループの削除
- Duoグループの表示
- ユーザーのDuo認証をバイパスする

Cisco Duoの設定

コマンドを使用して、クラスタ全体または特定のStorage VM（ONTAP CLIではVserver）に対してCisco Duo構成を作成できます `security login duo create`。これにより、このクラスタまたはStorage VMのSSHログインでCisco Duoが有効になります。の詳細については `security login duo create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。
4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMに対してCisco Duo認証を有効にし、環境からの情報を角かっこ内の値に置き換えます。

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Cisco Duo設定の変更

Cisco Duoがユーザーを認証する方法を変更できます(たとえば、指定される認証プロンプトの数、使用されるHTTPプロキシなど)。Storage VM（ONTAP CLIではVserver）のCisco Duo設定を変更する必要がある場合は、コマンドを使用できます `security login duo modify`。の詳細については `security login duo modify`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。
4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMのCisco Duo設定を変更し、環境で更新された情報を角かっこ内の値に置き換えます。

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

Cisco Duo設定の削除

Cisco Duo設定を削除すると、ログイン時にSSHユーザがDuoを使用して認証する必要がなくなります。Storage VM（ONTAP CLIではVserverと表示されます）のCisco Duo設定を削除するには、コマンドを使用し `security login duo delete`ます。の詳細については `security login duo delete`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. このStorage VMのCisco Duo設定を削除し、Storage VM名をに置き換えて `<STORAGE_VM_NAME>`ください：

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

これにより、このStorage VMのCisco Duo設定が完全に削除されます。

Cisco Duo設定の表示

Storage VM（ONTAP CLIではVserverと表示されます）の既存のCisco Duo設定を表示するには、コマンドを使用し `security login duo show`ます。の詳細については `security login duo show`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. このStorage VMのCisco Duo設定を表示します。必要に応じて、パラメータを使用してStorage VMを指定できます `vserver`。Storage VM名はに置き換えてください。 `<STORAGE_VM_NAME>`

```
security login duo show -vserver <STORAGE_VM_NAME>
```

次のような出力が表示されます。

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Duoグループの作成

Cisco Duoでは、特定のActive Directory、LDAP、またはローカルユーザーグループのユーザーのみをDuo認証プロセスに含めるように設定できます。Duoグループを作成すると、そのグループ内のユーザーのみがDuo認証を求められます。Duoグループは、コマンドを使用して作成できます `security login duo group create`。グループを作成するときに、必要に応じて、そのグループ内の特定のユーザーをDuo認証プロセスから除外することができます。の詳細については `security login duo group create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループを作成し、環境の情報を括弧内の値に置き換えます。パラメータを省略する `-vserver`と、グループはクラスタレベルで作成されます。

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。オプションのパラメータで指定したユーザは `-excluded-users`、Duo認証プロセスに含まれません。

Duoグループの表示

既存のCisco Duoグループエントリを表示するには、コマンドを使用し `security login duo group show`ます。の詳細については `security login duo group show`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループのエントリを表示します。括弧内の値は、環境の情報に置き換えてください。パラメータを省略すると、 `-vserver`グループはクラスタレベルで表示されます。

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。オプションのパラメータで指定したユーザ `-excluded-users`は表示されません。

Duoグループの削除

Duoグループエントリを削除するには、コマンドを使用し `security login duo group delete`ます。グループを削除すると、そのグループのユーザはDuo認証プロセスに含まれなくなります。の詳細については `security login duo group delete`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループエントリを削除し、環境内の情報を括弧内の値に置き換えます。パラメータを省略すると、`-vserver`グループはクラスタレベルで削除されます。

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。

ユーザーのDuo認証をバイパスする

すべてのユーザーまたは特定のユーザーをDuo SSH認証プロセスから除外できます。

すべてのDuoユーザーを除外

すべてのユーザに対してCisco Duo SSH認証を無効にすることができます。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. SSHユーザのCisco Duo認証を無効にし、SVM名をに置き換え `<STORAGE_VM_NAME>`ます。

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Duoグループユーザーを除外

Duoグループの一部である特定のユーザーを、Duo SSH認証プロセスから除外できます。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. グループ内の特定のユーザーに対してCisco Duo認証を無効にします。括弧内の値は、除外するグループ名とユーザのリストに置き換えてください。

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。パラメータで指定したユーザは `-excluded-users`、Duo認証プロセスに含まれません。

の詳細については `security login duo group modify`、を"ONTAPコマンド リファレンス"参照してください。

ローカルDuoユーザを除外

Cisco Duo管理パネルを使用すると、特定のローカルユーザーをDuo認証の使用から除外できます。手順については、を参照して "Cisco Duoマニュアル"ください。

CA署名済みサーバ証明書を生成してONTAPにインストールする

本番用システムでは、クラスタまたは SVM を SSL サーバとして認証する際に使用する CA 署名デジタル証明書をインストールすることを推奨します。コマンドを使用してCertificate Signing Request（CSR；証明書署名要求）を生成し、 `security certificate install`コマンドを使用して認証局から返された証明書をインストールできます `security certificate generate-csr`。および `security certificate install`の詳細については `security certificate generate-

csr、を"ONTAPコマンド リファレンス"参照してください。

証明書署名要求を生成する

証明書署名要求（CSR）は、コマンドを使用して生成できます security certificate generate-csr。要求が処理されると、署名済みのデジタル証明書が認証局（CA）から送信されます。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. CSRを生成します。

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

次のコマンドは、ハッシュ関数で生成される2、048ビット秘密鍵を使用してCSRを作成します。この証明書 SHA256`は、米国カリフォルニア州のサニーベールにあるというカスタム共通名の企業の部門 `server1.companyname.com`内のグループ `IT`が使用します。 `Software`SVM担当者の管理者のEメールアドレスはです `web@example.com。出力にCSRと秘密鍵が表示されます。

CSRの作成例

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. CSR出力の証明書要求を電子形式（Eメールなど）で信頼できるサードパーティのCAに送信し、署名を求めます。

   要求が処理されると、署名済みのデジタル証明書がCAから送信されます。秘密鍵とCA署名デジタル証明書のコピーを保管しておく必要があります。

CA署名済みサーバ証明書のインストール

CA署名済みサーバ証明書は、コマンドを使用してSVMにインストールできます `security certificate install`。ONTAPでは、サーバ証明書の証明書チェーンを形成する認証局（CA）のルート証明書と中間証明書の入力を求められます。の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

ステップ

1. CA署名済みサーバ証明書をインストールします。

```
security certificate install -vserver SVM_name -type certificate_type
```

> ONTAPは、サーバ証明書の証明書チェーンを形成するCAルート証明書と中間証明書の入力を求めます。チェーンは、サーバ証明書を発行したCAの証明書から始まり、CAのルート証明書までの範囲があります。中間証明書が不足していると、サーバ証明書のインストールが失敗します。

次のコマンドは、CA署名済みサーバ証明書と中間証明書をSVMにインストールし `engData2`ます。

CA署名済みサーバ証明書中間証明書のインストール例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

関連情報

- "セキュリティ証明書のgenerate-csr"

System Managerを使用したONTAP証明書の管理

System.10.1以降では、ONTAP 9 Managerを使用して、信頼された認証局、クライアント/サーバ証明書、およびローカル（オンボード）の認証局を管理できます。

System Managerでは、他のアプリケーションから受け取った証明書を管理して、それらのアプリケーションからの通信を認証できます。また、他のアプリケーションに対してシステムを識別する独自の証明書を管理することもできます。

証明書情報の表示

System Managerでは、クラスタに格納されている信頼された認証局、クライアント/サーバ証明書、およびローカルの認証局を表示できます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. [* セキュリティ * （ * Security * ）] 領域までスクロールします。［ * 証明書 * ］ セクションには、次の詳細が表示されます。
   - 保存されている信頼された認証局の数。
   - 保存されているクライアント / サーバ証明書の数。
   - 保存されているローカル認証局の数。
3. 任意の数を選択して証明書のカテゴリの詳細を表示するか、 → すべてのカテゴリに関する情報を含む*証明書*ページを開きます。リストには、クラスタ全体の情報が表示されます。特定のStorage VMの情報のみを表示する場合は、次の手順を実行します。
   a. [ストレージ]>[Storage VM]*を選択します。
   b. Storage VMを選択します。
   c. [設定]タブに切り替えます。
   d. [証明書]セクションに表示されている番号を選択します。

次の手順

- [証明書]ページでは、次のことができます[証明書署名要求を生成する]。
- 証明書情報は、カテゴリごとに1つずつ、3つのタブに分かれています。各タブから次のタスクを実行できます。

タブ	実行できる手順
• 信頼された認証機関 *	• [install-trusted-cert] • [信頼された認証局を削除します。] • [信頼された認証局の更新]

• クライアント / サーバ証明書 *	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• ローカル認証局 *	• [新しいローカル認証局を作成します。] • [ローカル認証局を使用して証明書に署名する] • [ローカル認証局を削除します。] • [ローカル認証局の更新]

証明書署名要求を生成する

証明書署名要求（ CSR ）は、 Certificate * ページの任意のタブから System Manager で生成できます。秘密鍵と対応するCSRが生成され、認証局を使用して署名してパブリック証明書を生成できます。

手順

1. ［ * 証明書 * ］ ページを表示します。を参照して [証明書情報の表示]
2. [+ CSRの生成]*を選択します。
3. サブジェクト名の情報を入力します。
   a. * 共通名 * を入力します。
   b. * 国 * を選択します。
   c. * 組織 * を入力します。
   d. * 組織単位 * を入力します。
4. デフォルト値を上書きする場合は、 * その他のオプション * を選択して追加情報を指定します。

信頼された認証局のインストール（追加）

信頼された追加の認証局をSystem Managerにインストールできます。

手順

1. [**Trusted Certificate Authorities**] タブを表示します。を参照して [証明書情報の表示]
2. を選択します + Add 。
3. [Add Trusted Certificate Authority*] パネルで、次の手順を実行します。
   ◦ * 名 * を入力します。
   ◦ スコープ * には、 Storage VM を選択します。
   ◦ * 共通名 * を入力します。
   ◦ * タイプ * を選択します。
   ◦ 証明書の詳細を入力またはインポートします。 *

信頼された認証局を削除します。

System Managerでは、信頼された認証局を削除できます。

ONTAPがプリインストールされている信頼された認証局は削除できません。

手順

1. [**Trusted Certificate Authorities**] タブを表示します。を参照して [証明書情報の表示]
2. 信頼された認証局の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*[削除]*を選択します。

信頼された認証局の更新

System Managerでは、有効期限が切れている、または有効期限が近づいている信頼された認証局を更新できます。

手順

1. [**Trusted Certificate Authorities**] タブを表示します。を参照して [証明書情報の表示]
2. 信頼された認証局の名前を選択します。
3. 証明書名の横にあるを選択し、*更新*を選択します ⋮ 。

クライアント/サーバ証明書のインストール（追加）

System Managerでは、追加のクライアント/サーバ証明書をインストールできます。

手順

1. クライアント / サーバ証明書 * タブを表示します。を参照して [証明書情報の表示]
2. を選択します + Add 。
3. [Add Client/Server Certificate] パネルで、次の手順を実行します。
   - * 証明書名 * を入力します。
   - スコープ * には、 Storage VM を選択します。
   - * 共通名 * を入力します。
   - * タイプ * を選択します。
   - 証明書の詳細を入力またはインポートします。 *テキストファイルから証明書の詳細を入力またはコピーして貼り付けることも、 * Import * をクリックして証明書ファイルからテキストをインポートすることもできます。
   - 秘密鍵*を入力します。テキストファイルから秘密キーを入力するか、コピーして貼り付けるか、 * インポート * をクリックして秘密キーファイルからテキストをインポートすることができます。

自己署名クライアント/サーバ証明書を生成（追加）する

System Managerでは、追加の自己署名クライアント/サーバ証明書を生成できます。

手順

1. クライアント / サーバ証明書 * タブを表示します。を参照して [証明書情報の表示]
2. [+自己署名証明書の生成]*を選択します。
3. 自己署名証明書の生成 * パネルで、次の手順を実行します。
   - * 証明書名 * を入力します。
   - スコープ * には、 Storage VM を選択します。
   - * 共通名 * を入力します。
   - * タイプ * を選択します。
   - * ハッシュ関数 * を選択します。
   - * キーサイズ * を選択します。
   - Storage VM * を選択します。

クライアント/サーバ証明書を削除する

System Managerでは、クライアント/サーバ証明書を削除できます。

手順

1. クライアント / サーバ証明書 * タブを表示します。を参照して [証明書情報の表示]
2. クライアント/サーバ証明書の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*[削除]*をクリックします。

クライアント/サーバ証明書の更新

System Managerでは、期限切れまたはまもなく期限切れになるクライアント/サーバ証明書を更新できます。

手順

1. クライアント / サーバ証明書 * タブを表示します。を参照して [証明書情報の表示]
2. クライアント/サーバ証明書の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*更新*をクリックします。

新しいローカル認証局を作成します。

System Managerでは、新しいローカル認証局を作成できます。

手順

1. [ローカル証明機関 *] タブを表示します。を参照して [証明書情報の表示]
2. を選択します

。
3. [Add Local Certificate Authority*] パネルで、次の手順を実行します。
   - * 名 * を入力します。
   - スコープ * には、 Storage VM を選択します。
   - * 共通名 * を入力します。
4. デフォルト値を上書きする場合は、 * その他のオプション * を選択して追加情報を指定します。

ローカル認証局を使用して証明書に署名する

System Managerでは、ローカルの認証局を使用して証明書に署名できます。

手順

1. [ローカル証明機関 *] タブを表示します。を参照して [証明書情報の表示]
2. ローカル認証局の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、証明書に署名。
4. [証明書署名要求に署名する *] フォームに入力します。
   - 証明書署名のコンテンツを貼り付けるか、 * Import * をクリックして証明書署名要求ファイルをインポートできます。
   - 証明書が有効になる日数を指定します。

ローカル認証局を削除します。

System Managerでは、ローカル認証局を削除できます。

手順

1. [ローカル認証局] タブを表示します。を参照して [証明書情報の表示]
2. ローカル認証局の名前を選択します。
3. 名前の横にあるを選択し、*[削除]*を選択し ⋮ ます。

ローカル認証局の更新

System Managerでは、有効期限が切れている、または有効期限が近づいているローカル認証局を更新できます。

手順

1. [ローカル認証局] タブを表示します。を参照して [証明書情報の表示]
2. ローカル認証局の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*更新*をクリックします。

ONTAPでの**Active Directory**ドメインコントローラアクセスの設定

ADアカウントからSVMにアクセスするためには、ADドメインコントローラからクラスタまたはSVMへのアクセスを設定しておく必要があります。データ SVM 用に SMB サーバをすでに設定している場合は、クラスタへの AD アクセス用に SVM をゲートウェイまたは *tunnel* として設定できます。SMBサーバを設定していない場合は、ADドメインにSVMのコンピュータアカウントを作成できます。

ONTAPは、次のドメインコントローラ認証サービスをサポートしています。

- Kerberos
- LDAP
- Netlogon

- Local Security Authority（LSA）

ONTAPでは、セキュアなNetlogon接続を実現するために次のセッション キー アルゴリズムがサポートされます。

セッションキーアルゴリズム	使用可能なバージョン
HMAC-SHA256（Advanced Encryption Standard（AES）に基づく）クラスタでONTAP 9 .9.1以前を実行していて、ドメインコントローラでセキュアなネットログオンサービスにAESが適用されている場合は、接続が失敗します。この場合、代わりにONTAPとの強力なキー接続を受け入れるようにドメインコントローラを再設定する必要があります。	ONTAP 9 10.1
DESおよびHMAC-MD5（強力なキーが設定されている場合）	すべてのONTAP 9リリース

ネットログオンでのセキュアチャネルの確立中にAESセッションキーを使用する場合は、SVMでAESが有効になっていることを確認する必要があります。

- 14.1以降では、ONTAP 9の作成時にデフォルトでAESが有効になり、ネットログオンでのセキュアチャネルの確立時にAESセッションキーを使用するようにSVMのセキュリティ設定を変更する必要はありません。
- ONTAP 9 .10.1~9.13.1では、SVMの作成時にAESがデフォルトで無効になります。次のコマンドを使用してAESを有効にする必要があります。

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

ONTAP 9 .14.1以降にアップグレードした場合、以前のリリースのONTAPで作成された既存のSVMのAES設定は自動的には変更されません。これらのSVMでAESを有効にするには、引き続きこの設定の値を更新する必要があります。

認証トンネルの設定

データSVM用のSMBサーバがすでに設定されている場合は、コマンドを使用して、SVMをADによるクラスタアクセス用のゲートウェイ（*tunnel*）として設定でき `security login domain-tunnel create`ます。

ONTAP 9.16.1より前のバージョンでは、認証トンネルを使用してADでクラスタ管理者アカウントを管理する必要があります。

開始する前に

- データSVM用のSMBサーバを設定しておく必要があります。
- ADドメインのユーザ アカウントにクラスタの管理SVMへのアクセスを許可しておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

10.1以降では、**AD**アクセス用のゲートウェイ（ドメイントンネル）がある場合、**AD**ドメインで**ONTAP 9**を無効にしていれば、管理認証に**Kerberos**を使用できます。以前のリリースでは、**SVM**ゲートウェイの管理認証で**Kerberos**はサポートされていませんでした。この機能はデフォルトで使用できます。設定は必要ありません。

Kerberos認証は常に最初に試行されます。失敗した場合は、NTLM認証が試行されます。

手順

1. SMB対応のデータSVMをADドメインコントローラがクラスタにアクセスするための認証トンネルとして設定します。

```
security login domain-tunnel create -vserver <svm_name>
```

の詳細については `security login domain-tunnel create`、を"ONTAPコマンド リファレンス"参照してください。

ユーザを認証するには、SVMが実行されている必要があります。

次のコマンドは、SMB対応のデータSVMを認証トンネルとして設定し `engData`ます。

```
cluster1::>security login domain-tunnel create -vserver engData
```

ドメインに**SVM**コンピュータアカウントを作成する

データSVM用のSMBサーバを設定していない場合は、コマンドを使用して、ドメインにSVM用のコンピュータアカウントを作成できます `vserver active-directory create`。

タスクの内容

コマンドを入力すると `vserver active-directory create`、ドメイン内の指定した組織単位にコンピュータを追加するための十分なPrivilegesを持つADユーザアカウントのクレデンシャルを入力するように求められます。アカウントのパスワードを空にすることはできません。

ONTAP 9.16.1以降では、この手順を使用してADを使用してクラスタ管理者アカウントを管理できます。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. ADドメインにSVM用のコンピュータアカウントを作成します。

```
vserver active-directory create -vserver <SVM_name> -account-name
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

ONTAP 9.16.1以降では、この `-vserver`パラメータは管理SVMを指定できます。の詳細については `vserver active-directory create`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、SVMの `engData`ドメインに `example.com`という名前のコンピュータアカウントを作成します `ADSERVER1`。コマンドを入力すると、ADユーザアカウントのクレデンシャルの入力を求められます。

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

ONTAPでの**LDAP**または**NIS**サーバアクセスの設定

LDAPアカウントまたはNISアカウントからSVMにアクセスするためには、LDAPサーバまたはNISサーバからSVMへのアクセスを設定しておく必要があります。スイッチ機能を使用すると、LDAPまたはNISを代替ネームサービスソースとして使用できます。

LDAPサーバ アクセスの設定

LDAPアカウントがSVMにアクセスするためには、LDAPサーバからSVMへのアクセスを設定しておく必要があります。コマンドを使用すると、SVMにLDAPクライアント設定を作成できます `vserver services name-service ldap client create`。その後、コマンドを使用し `vserver services name-service ldap create`て、LDAPクライアント設定をSVMに関連付けます。

タスクの内容

ほとんどのLDAPサーバでは、ONTAPが提供するデフォルトスキーマを使用できます。

- MS-AD-BIS（Windows Server 2012以降のほとんどのADサーバで推奨されるスキーマ）
- AD-IDMU（Windows 2008、Windows 2016、およびそれ以降のADサーバ）
- AD-SFU（Windows 2003以前のADサーバ）
- RFC-2307（UNIX LDAPサーバ）

他のスキーマを使用する必要がないかぎり、デフォルトのスキーマを使用することを推奨します。その場合は、デフォルトのスキーマをコピーしてコピーを変更することで、独自のスキーマを作成できます。詳細については、次を参照してください。

- "NFSの設定"
- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"

開始する前に

- SVMにをインストールしておく必要があり"CA 署名済みサーバデジタル証明書"ます。

- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. SVMにLDAPクライアント設定を作成します。

```
vserver services name-service ldap client create -vserver <SVM_name> -client
-config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
-use-start-tls <true|false>
```

> Start TLSは、データSVMへのアクセスでのみサポートされます。管理SVMへのアクセスではサポートされません。

の詳細については `vserver services name-service ldap client create`、を"ONTAPコマンドリファレンス"参照してください。

次のコマンドは、SVMに `engData`という名前のLDAPクライアント設定を作成し `corp`ます。クライアントは、IPアドレスが172.160.0.100および172.16.0.101のLDAPサーバに匿名でバインドします。クライアントはRFC-2307スキーマを使用してLDAPクエリを実行します。クライアントとサーバ間の通信はStart TLSを使用して暗号化されます。

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

> 。 `-ldap-servers` LDAP サーバーのホスト名または IP アドレスを指定するフィールド。

2. LDAPクライアント設定をSVMに関連付けます。 `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

の詳細については `vserver services name-service ldap create`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、LDAPクライアント設定をSVMに `engData`関連付け `corp`、SVMでLDAPクライアントを有効にします。

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

> その `vserver services name-service ldap create`コマンドは自動構成検証を実行し、ONTAP がネーム サーバに接続できない場合はエラー メッセージを報告します。

3. vserver services name-service ldap checkコマンドを使用して、ネームサーバのステータスを検証します。

次のコマンドは、SVM vs0のLDAPサーバを検証します。

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                   |
```

使用することができます `name service check``ネームサーバーのステータスを検証するコマンド。

NISサーバ アクセスの設定

NISアカウントがSVMにアクセスするためには、NISサーバからSVMへのアクセスを設定しておく必要があります。SVMにNISドメイン設定を作成するには、コマンドを使用し `vserver services name-service nis-domain create`ます。

開始する前に

- SVMにNISドメインを設定するには、設定済みのすべてのサーバが使用可能でアクセス可能である必要があります。
- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

ステップ

1. SVMにNISドメイン設定を作成します。

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   の詳細については `vserver services name-service nis-domain create`、を"ONTAPコマンドリファレンス"参照してください。

   。 `-nis-servers` NIS サーバーのホスト名または IP アドレスを指定するフィールド。

   次のコマンドは、SVMにNISドメイン設定を作成し `engData`ます。`NIS`ドメインは `nisdomain`、IPアドレスを使用してNISサーバと通信し `192.0.2.180`ます。

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

ネームサービススイッチを作成する

ネームサービススイッチ機能を使用すると、LDAPまたはNISを代替ネームサービスソースとして使用できます。コマンドを使用すると、ネームサービスソースの参照順序を指定できます `vserver services name-service ns-switch modify`。

開始する前に

- LDAPサーバとNISサーバのアクセスを設定しておく必要があります。
- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

ステップ

1. ネームサービスソースの検索順序を指定します。

   ```
   vserver services name-service ns-switch modify -vserver <SVM_name> -database
   <name_service_switch_database> -sources <name_service_source_order>
   ```

   の詳細については `vserver services name-service ns-switch modify`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、SVM上のデータベース `engData`のLDAPおよびNISネームサービスソースの検索順序を指定します `passwd`。

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

ONTAP管理者パスワードを変更する

初期パスワードは、システムへの初回ログイン後すぐに変更してください。SVM管理者は、コマンドを使用して自分のパスワードを変更できます `security login password`。クラスタ管理者は、コマンドを使用して管理者のパスワードを変更できます `security login password`。

タスクの内容

新しいパスワードは次のルールに従う必要があります。

- ユーザ名を含めることはできません。
- 8文字以上である必要があります。
- 英文字と数字がそれぞれ1文字以上含まれている必要があります。
- 直近の6つのパスワードと同じパスワードは使用できません。

> コマンドを使用すると、指定したロールに関連付けられたアカウントのパスワードルールを変更できます `security login role config modify`。

開始する前に

- 自分のパスワードを変更するには、クラスタ管理者またはSVM管理者である必要があります。
- 他の管理者のパスワードを変更するには、クラスタ管理者である必要があります。

ステップ

1. 管理者パスワードを変更します。 `security login password -vserver` *`svm_name`* `-username` *`user_name`*

次のコマンドは、SVMのvs1.example.com管理者のパスワードを変更し `admin1`ます。プロンプトが表示されたら、現在のパスワードを入力し、新しいパスワードを入力して再入力します。

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

関連情報

- "security login role config modify"
- "セキュリティログインパスワード"

ONTAP管理者アカウントのロックとロック解除

コマンドを使用して管理者アカウントをロックし、 `security login unlock`コマンドを使用してアカウントのロックを解除でき `security login lock`ます。

開始する前に

これらのタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 管理者アカウントをロックします。

   `security login lock -vserver SVM_name -username user_name`

   次のコマンドは、SVMの管理者アカウントをロックし `admin1`vs1.example.comます。

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

   の詳細については `security login lock`、を"ONTAPコマンド リファレンス"参照してください。

2. 管理者アカウントのロックを解除します。

   `security login unlock -vserver SVM_name -username user_name`

   次のコマンドは、SVMの管理者アカウントのロックを解除し `admin1`vs1.example.comます。

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

   の詳細については `security login unlock`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "セキュリティログイン"

ONTAPでのログインの失敗を管理します。

ログイン試行が繰り返し失敗する場合、侵入者がストレージシステムへのアクセスを試みていることが疑われます。侵入を防ぐためにさまざまな対策を講じることができます。

失敗したログインを確認する方法

イベント管理システム（ EMS ）では 1 時間ごとに失敗したログイン試行を通知します。失敗したログインの記録はファイルで確認できます `audit.log`。

ログイン試行が繰り返し失敗する場合の対処方法

侵入を防ぐための短期的な対策としては、次のような方法があります。

- パスワードに大文字、小文字、特殊文字、数字を最低何文字か含めるように要求します
- ログインに失敗したあとに間隔を設定します
- 許容されるログイン失敗回数を制限し、指定した回数を超えたユーザをロックアウトします
- 指定した日数アクティブでないアカウントを期限切れにしてロックアウトします

これらのタスクは、コマンドを使用して実行できます `security login role config modify`。の詳細については `security login role config modify`、を"ONTAPコマンド リファレンス"参照してください。

長期的に見て、次の手順を実行することもできます。

- 新しく作成するすべてのSVMに対してログインの失敗回数を制限するには、コマンドを使用し `security ssh modify`ます。の詳細については `security ssh modify`、を"ONTAPコマンド リファレンス"参照してください。
- ユーザにパスワードの変更を求めることで、既存の MD5 アルゴリズムのアカウントをより安全な SHA-512 アルゴリズムに移行する。

ONTAP管理者アカウントのパスワードにSHA-2を適用する

ONTAP 9 .0より前に作成した管理者アカウントは、パスワードが手動で変更されるまで、アップグレード後も引き続きMD5パスワードを使用します。MD5はSHA-2より安全ではありません。そのため、アップグレード後は、MD5アカウントのユーザにパスワードを変更してデフォルトのSHA-512ハッシュ関数を使用するように指示する必要があります。

タスクの内容

パスワードハッシュ機能を使用すると、次の操作を実行できます。

- 指定したハッシュ関数に一致するユーザアカウントを表示します。
- 指定したハッシュ関数（MD5など）を使用するアカウントを期限切れにして、ユーザが次回ログイン時にパスワードを変更するように強制します。
- 指定したハッシュ関数を使用するパスワードが指定されたアカウントをロックする。

- ONTAP 9よりも前のリリースにリバートする場合は、クラスタ管理者のパスワードを以前のリリースでサポートされているハッシュ関数（MD5）と互換性があるパスワードにリセットします。

ONTAPは、NetApp Manageability SDKおよび `security-login-modify-password`を使用する場合にのみ、事前にハッシュされたSHA-2パスワードを受け入れ(`security-login-create`ます）。

手順

1. MD5管理者アカウントをSHA-512パスワードハッシュ関数に移行します。
   a. すべてのMD5管理者アカウントを期限切れにします。 `security login expire-password -vserver * -username * -hash-function md5`

      これにより、MD5アカウントユーザは次回ログイン時にパスワードを変更する必要があります。

   b. MD5アカウントのユーザに、コンソールまたはSSHセッションを使用してログインするように依頼します。

      アカウントの有効期限が切れていることが検出され、ユーザにパスワードの変更を求めるプロンプトが表示されます。変更されたパスワードには、デフォルトでSHA-512が使用されます。

2. 一定時間内にユーザがログインしてパスワードを変更しないMD5アカウントの場合は、アカウントを強制的に移行します。
   a. まだMD5ハッシュ関数を使用しているアカウントをロックします（advanced権限レベル）。 `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      で指定した日数が経過する `-lock-after`と、ユーザはMD5アカウントにアクセスできなくなります。

   b. ユーザがパスワードを変更する準備ができたら、アカウントのロックを解除します。 `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*
   c. ユーザに、コンソールまたはSSHセッションからアカウントにログインし、プロンプトが表示されたらパスワードを変更してもらいます。

関連情報

- "security login expire -パスワード"
- "セキュリティログインロック解除"

System Managerの**ONTAP**ファイルアクセスの問題を診断して修正する

ONTAP 9.8 以降では、ファイルアクセスに関する問題をトレースして確認できます。

手順

1. System Manager で、 * Storage > Storage VM* を選択します。
2. トレースを実行するStorage VMを選択します。
3. [詳細]*をクリックします ⋮ 。
4. ファイルアクセスのトレース * をクリックします。
5. ユーザー名とクライアントの IP アドレスを入力し、 * トレースを開始 * をクリックします。

トレース結果が表形式で表示されます。[* 理由] 列には、ファイルにアクセスできなかった理由が表示されます。

6. 結果テーブルの左側の列をクリック ⌄ すると、ファイルアクセス権限が表示されます。

マルチ管理者認証の管理

ONTAPのマルチ管理者認証の詳細

ONTAP 9.11.1以降では、Multi-Admin Verification（MAV；マルチ管理者認証）を使用して、ボリュームやスナップショットの削除などの特定の処理を、指定した管理者の承認後にのみ実行できるようにすることができます。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。

マルチ管理者検証の構成は次のとおりです。

- "1つ以上の管理者承認グループを作成します。"
- "マルチ管理者検証機能を有効にします。"
- "ルールを追加または変更する。"

初期設定後にこれらの要素を変更できるのは、MAV承認グループの管理者（MAV管理者）のみです。

マルチ管理者認証が有効な場合、保護対象処理を完了するには次の手順が必要です。

1. ユーザが処理を開始すると、 "要求が生成されます。"
2. 操作を実行する前に、少なくとも1つの"MAV管理者は承認する必要があります。"
3. 承認されると、ユーザーはプロンプトを表示して操作を完了します。

ⓘ MAV管理者の承認なしにマルチ管理者検証機能を無効にする必要がある場合は、 NetAppサポートに連絡して次のことを伝えてください。"NetAppナレッジベース: MAV 管理者が利用できない場合にマルチ管理者検証を無効にする方法" 。

複数管理者による検証は、高度な自動化を伴うボリュームやワークフローでは使用しません。自動化された各タスクは、処理を完了する前に承認が必要になるためです。自動化とMAVを一緒に使用する場合は、特定のMAV操作にクエリを使用することをお勧めします。たとえば、自動化が関係していないボリュームにのみMAVルールを適用し、特定の命名方式でそれらのボリュームを指定でき `volume delete`ます。

ⓘ Cloud Volumes ONTAPでは、マルチ管理者認証は使用できません。

マルチ管理者認証の仕組み

マルチ管理者認証は次の要素で構成されます。

- 承認権と拒否権を持つ1人以上の管理者のグループ。
- 保護された操作またはコマンドのセット（a_rules table_）
- a_rulesエンジン_保護されたオペレーションの実行を識別および制御します

MAVルールは、Role-Based Access Control（RBAC；ロールベースアクセス制御）ルールのあとに評価されます。したがって、保護された処理を実行または承認する管理者は、それらの処理に対して最低限必要なRBAC Privilegesをすでに所有している必要があります。"RBACの詳細については、こちらをご覧ください"です。

システム定義のルール

マルチ管理者検証を有効にすると、システム定義のルール（_guard-rale_rulesとも呼ばれます）によってMAV処理のセットが確立され、MAVプロセス自体が回避されるリスクが含まれます。これらの操作をルールテーブルから削除することはできません。MAVを有効にすると、アスタリスク（）で指定された操作は、実行前に**1**人以上の管理者による承認を必要とします。ただし、 show *コマンドは除きます。

- `security multi-admin-verify modify`操作 `*

  マルチ管理者検証機能の構成を制御します。

- `security multi-admin-verify approval-group`運用 `*

  マルチ管理者認証資格情報を使用して、管理者セットのメンバーシップを制御します。

- `security multi-admin-verify rule`運用 `*

  複数管理者による検証を必要とする一連のコマンドを制御します。

- `security multi-admin-verify request`運用

  承認プロセスを制御します。

ルール保護コマンド

システム定義の操作に加えて、マルチ管理者検証が有効になっている場合は次のコマンドがデフォルトで保護されますが、ルールを変更してこれらのコマンドの保護を削除できます。

- "セキュリティログインパスワード"
- "セキュリティログインロック解除"
- "設定"

各ONTAPバージョンでは、マルチ管理者認証ルールで保護できるコマンドが上記以外にも用意されています。保護可能なコマンドの全一覧を確認するには、お使いのONTAPリリースを選択してください。

9.17.1

- `cluster date modify`[3]
- `cluster log-forwarding create`[3]
- `cluster log-forwarding delete`[3]
- `cluster log-forwarding modify`[3]
- `cluster peer delete`
- `cluster time-service ntp server create`[3]
- `cluster time-service ntp server delete`[3]
- `cluster time-service ntp key create`[3]
- `cluster time-service ntp key delete`[3]
- `cluster time-service ntp key modify`[3]
- `cluster time-service ntp server modify`[3]
- `event config modify`
- `event config set-mail-server-password`[3]
- `lun delete`[3]
- `security anti-ransomware volume attack clear-suspect`[1]
- `security anti-ransomware volume disable`[1]
- `security anti-ransomware volume event-log modify`[2]
- `security anti-ransomware volume pause`[1]
- `security anti-ransomware vserver event-log modify`[2]
- `security audit modify`[3]
- `security ipsec config modify`[3]
- `security ipsec policy create`[3]
- `security ipsec policy delete`[3]
- `security ipsec policy modify`[3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase`[3]
- `security saml-sp create`[3]

- security saml-sp delete[3]
- security saml-sp modify[3]
- security webauthn credentials delete[4]
- snaplock legal-hold end[3]
- storage aggregate delete[3]
- storage aggregate offline[4]
- storage encryption disk destroy[3]
- storage encryption disk modify[3]
- storage encryption disk revert-to-original-state[3]
- storage encryption disk sanitize[3]
- system bridge run-cli[3]
- system controller flash-cache secure-erase run[3]
- system controller service-event delete[3]
- system health alert delete[3]
- system health alert modify[3]
- system health policy definition modify[3]
- system node autosupport modify[3]
- system node autosupport trigger modify[3]
- system node coredump delete[3]
- system node coredump delete-all[3]
- system node hardware nvram-encryption modify[3]
- system node run
- system node systemshell
- system script delete[3]
- system service-processor ssh add-allowed-addresses[3]
- system service-processor ssh remove-allowed-addresses[3]
- system smtape restore[3]
- system switch ethernet log disable-collection[3]
- system switch ethernet log modify[3]
- timezone[3]
- volume create[3]
- volume delete
- volume encryption conversion start[4]
- volume encryption rekey start[4]

- volume file privileged-delete[3]
- volume flexcache delete
- volume modify[3]
- volume rename [5]
- volume recovery-queue modify[2]
- volume recovery-queue purge[2]
- volume recovery-queue purge-all[2]
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot create[3]
- volume snapshot delete
- volume snapshot modify[3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename[3]
- volume snapshot restore
- vserver audit create[3]
- vserver audit delete[3]
- vserver audit disable[3]
- vserver audit modify[3]
- vserver audit rotate-log[3]
- vserver create[2]
- vserver consistency-group create[4]
- vserver consistency-group delete[4]
- vserver consistency-group modify[4]
- vserver consistency-group snapshot create[4]
- vserver consistency-group snapshot delete[4]
- vserver delete[3]
- vserver modify[2]
- vserver object-store-server audit create[3]

- vserver object-store-server audit delete[3]
- vserver object-store-server audit disable[3]
- vserver object-store-server audit modify[3]
- vserver object-store-server audit rotate-log[3]
- vserver object-store-server bucket cors-rule create[4]
- vserver object-store-server bucket cors-rule delete[4]
- vserver options[3]
- vserver peer delete
- vserver security file-directory apply[3]
- vserver security file-directory remove-slag[3]
- vserver stop[4]
- vserver vscan disable[3]
- vserver vscan on-access-policy create[3]
- vserver vscan on-access-policy delete[3]
- vserver vscan on-access-policy disable[3]
- vserver vscan on-access-policy modify[3]
- vserver vscan scanner-pool create[3]
- vserver vscan scanner-pool delete[3]
- vserver vscan scanner-pool modify[3]

9.16.1

- cluster date modify[3]
- cluster log-forwarding create[3]
- cluster log-forwarding delete[3]
- cluster log-forwarding modify[3]
- cluster peer delete
- cluster time-service ntp server create[3]
- cluster time-service ntp server delete[3]
- cluster time-service ntp key create[3]
- cluster time-service ntp key delete[3]
- cluster time-service ntp key modify[3]
- cluster time-service ntp server modify[3]
- event config modify
- event config set-mail-server-password [3]

- lun delete[3]
- security anti-ransomware volume attack clear-suspect[1]
- security anti-ransomware volume disable[1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause[1]
- security anti-ransomware vserver event-log modify[2]
- security audit modify[3]
- security ipsec config modify[3]
- security ipsec policy create[3]
- security ipsec policy delete[3]
- security ipsec policy modify[3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create[3]
- security saml-sp delete[3]
- security saml-sp modify[3]
- security webauthn credentials delete[4]
- snaplock legal-hold end[3]
- storage aggregate delete[3]
- storage aggregate offline[4]
- storage encryption disk destroy[3]
- storage encryption disk modify[3]
- storage encryption disk revert-to-original-state[3]
- storage encryption disk sanitize[3]
- system bridge run-cli[3]
- system controller flash-cache secure-erase run[3]
- system controller service-event delete[3]
- system health alert delete[3]
- system health alert modify[3]

- system health policy definition modify[3]
- system node autosupport modify[3]
- system node autosupport trigger modify[3]
- system node coredump delete[3]
- system node coredump delete-all[3]
- system node hardware nvram-encryption modify[3]
- system node run
- system node systemshell
- system script delete[3]
- system service-processor ssh add-allowed-addresses[3]
- system service-processor ssh remove-allowed-addresses[3]
- system smtape restore[3]
- system switch ethernet log disable-collection[3]
- system switch ethernet log modify[3]
- timezone[3]
- volume create[3]
- volume delete
- volume encryption conversion start[4]
- volume encryption rekey start[4]
- volume file privileged-delete[3]
- volume flexcache delete
- volume modify[3]
- volume recovery-queue modify[2]
- volume recovery-queue purge[2]
- volume recovery-queue purge-all[2]
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot create[3]
- volume snapshot delete
- volume snapshot modify[3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename[3]
- volume snapshot restore
- vserver audit create[3]
- vserver audit delete[3]
- vserver audit disable[3]
- vserver audit modify[3]
- vserver audit rotate-log[3]
- vserver create[2]
- vserver consistency-group create[4]
- vserver consistency-group delete[4]
- vserver consistency-group modify[4]
- vserver consistency-group snapshot create[4]
- vserver consistency-group snapshot delete[4]
- vserver delete[3]
- vserver modify[2]
- vserver object-store-server audit create[3]
- vserver object-store-server audit delete[3]
- vserver object-store-server audit disable[3]
- vserver object-store-server audit modify[3]
- vserver object-store-server audit rotate-log[3]
- vserver object-store-server bucket cors-rule create[4]
- vserver object-store-server bucket cors-rule delete[4]
- vserver options[3]
- vserver peer delete
- vserver security file-directory apply[3]
- vserver security file-directory remove-slag[3]
- vserver stop[4]
- vserver vscan disable[3]
- vserver vscan on-access-policy create[3]
- vserver vscan on-access-policy delete[3]
- vserver vscan on-access-policy disable[3]
- vserver vscan on-access-policy modify[3]

- vserver vscan scanner-pool create[3]
- vserver vscan scanner-pool delete[3]
- vserver vscan scanner-pool modify[3]

9.15.1

- cluster date modify[3]
- cluster log-forwarding create[3]
- cluster log-forwarding delete[3]
- cluster log-forwarding modify[3]
- cluster peer delete
- cluster time-service ntp server create[3]
- cluster time-service ntp server delete[3]
- cluster time-service ntp key create[3]
- cluster time-service ntp key delete[3]
- cluster time-service ntp key modify[3]
- cluster time-service ntp server modify[3]
- event config modify
- event config set-mail-server-password [3]
- lun delete[3]
- security anti-ransomware volume attack clear-suspect[1]
- security anti-ransomware volume disable[1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause[1]
- security anti-ransomware vserver event-log modify[2]
- security audit modify[3]
- security ipsec config modify[3]
- security ipsec policy create[3]
- security ipsec policy delete[3]
- security ipsec policy modify[3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create[3]
- security saml-sp delete[3]
- security saml-sp modify[3]
- snaplock legal-hold end[3]
- storage aggregate delete[3]
- storage encryption disk destroy[3]
- storage encryption disk modify[3]
- storage encryption disk revert-to-original-state[3]
- storage encryption disk sanitize[3]
- system bridge run-cli[3]
- system controller flash-cache secure-erase run[3]
- system controller service-event delete[3]
- system health alert delete[3]
- system health alert modify[3]
- system health policy definition modify[3]
- system node autosupport modify[3]
- system node autosupport trigger modify[3]
- system node coredump delete[3]
- system node coredump delete-all[3]
- system node hardware nvram-encryption modify[3]
- system node run
- system node systemshell
- system script delete[3]
- system service-processor ssh add-allowed-addresses[3]
- system service-processor ssh remove-allowed-addresses[3]
- system smtape restore[3]
- system switch ethernet log disable-collection[3]
- system switch ethernet log modify[3]
- timezone[3]
- volume create[3]
- volume delete
- volume file privileged-delete[3]

- volume flexcache delete
- volume modify[3]
- volume recovery-queue modify[2]
- volume recovery-queue purge[2]
- volume recovery-queue purge-all[2]
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot create[3]
- volume snapshot delete
- volume snapshot modify[3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename[3]
- volume snapshot restore
- vserver audit create[3]
- vserver audit delete[3]
- vserver audit disable[3]
- vserver audit modify[3]
- vserver audit rotate-log[3]
- vserver create[2]
- vserver delete[3]
- vserver modify[2]
- vserver object-store-server audit create[3]
- vserver object-store-server audit delete[3]
- vserver object-store-server audit disable[3]
- vserver object-store-server audit modify[3]
- vserver object-store-server audit rotate-log[3]
- vserver options[3]
- vserver peer delete
- vserver security file-directory apply[3]

- vserver security file-directory remove-slag[3]
- vserver vscan disable[3]
- vserver vscan on-access-policy create[3]
- vserver vscan on-access-policy delete[3]
- vserver vscan on-access-policy disable[3]
- vserver vscan on-access-policy modify[3]
- vserver vscan scanner-pool create[3]
- vserver vscan scanner-pool delete[3]
- vserver vscan scanner-pool modify[3]

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect[1]
- security anti-ransomware volume disable[1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause[1]
- security anti-ransomware vserver event-log modify[2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify[2]
- volume recovery-queue purge[2]
- volume recovery-queue purge-all[2]
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete*
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create[2]
- vserver modify[2]
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect[1]
- security anti-ransomware volume disable[1]
- security anti-ransomware volume pause[1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete*
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete*
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

1. 9.13.1の新しいrule-protectedコマンド
2. 9.14.1の新しいrule-protectedコマンド
3. 9.15.1の新しいrule-protectedコマンド
4. 9.16.1の新しいrule-protectedコマンド
5. 9.17.1で新規追加されたルール保護コマンド

*このコマンドはCLIでのみ使用でき、一部のリリースではSystem Managerでは使用できません。

MAVで保護されたクラスタで保護された操作が入力されると、指定されたMAV管理者グループに操作実行要求が送信されます。

次の設定が可能です。

- MAVグループ内の管理者の名前、連絡先情報、および数。

  MAV管理者には、クラスタ管理者権限のあるRBACロールが必要です。

- MAV管理者グループの数。
  - 保護対象処理ルールごとにMAVグループが割り当てられます。
  - MAVグループが複数ある場合は、どのMAVグループが特定のルールを承認するかを設定できます。
- 保護対象処理を実行するために必要なMAV承認者の数。
- MAV管理者が承認要求に応答する必要がある_承認の失効_期間。
- 要求元の管理者が処理を完了する必要がある_実行のexpiry_period。

これらのパラメータを設定したら、変更するにはMAV承認が必要です。

MAV管理者は、保護された操作の実行要求を自分で承認することはできません。そのため、

- MAVは、管理者が1人だけのクラスタでは有効にしないでください。
- MAVグループに1人しかいない場合、そのMAV管理者は保護された操作を開始できません。通常の管理者は保護された操作を開始する必要があり、MAV管理者は承認のみを実行できます。
- MAV管理者が保護された操作を実行できるようにするには、MAV管理者の数が必要な承認の数より1つ多い必要があります。たとえば、保護された操作に2つの承認が必要で、MAV管理者にそれらの承認を実行させる場合、MAV管理者グループには3人のユーザーが必要です。

MAV管理者は、電子メールアラートで承認リクエストを受信することも（EMSを使用して）、リクエストキューを照会することもできます。リクエストを受け取ると、次の3つのアクションのいずれかを実行できます。

- 承認
- 拒否（拒否）
- 無視（アクションなし）

次の場合、MAVルールに関連付けられたすべての承認者に電子メール通知が送信されます。

- リクエストが作成されます。
- リクエストが承認または拒否された場合。
- 承認されたリクエストが実行されました。

リクエスト者が操作の同じ承認グループに属している場合は、リクエストが承認されると電子メールが送信されます。

リクエスト者は、自分のリクエストが承認グループに含まれていても、自分のリクエストを承認することはできません（ただし、自分のリクエストの電子メール通知を受け取ることはできます）。承認グループに属していないリクエスト者（つまり、MAV管理者でないリクエスト者）は、電子メール通知を受信しません。

保護された処理の実行の仕組み

保護された操作の実行が承認されると、要求元のユーザーはプロンプトが表示されたときに操作を続行します。処理が拒否された場合、要求元ユーザは処理を続行する前に要求を削除する必要があります。

MAVルールはRBACの権限の後に評価されます。そのため、操作を実行するための十分なRBAC権限を持たないユーザーは、MAV要求プロセスを開始できません。

MAVルールは、保護された操作が実行される前に評価されます。つまり、ルールはシステムの現在の状態に基づいて適用されます。例えば、MAVルールが以下の目的で作成された場合、 `volume modify`クエリで `-size 5GB` 、使用 `volume modify` 5GB のボリュームを 2GB にサイズ変更するには MAV の承認が必要ですが、2GB のボリュームを 5GB にサイズ変更する場合は必要ありません。

関連情報

- "クラスタ"
- "LUN"
- "セキュリティ"
- "SnapLock リーガルホールドの終了"
- "ストレージアグリゲート"
- "ストレージ暗号化"
- "システム"

MAVの**ONTAP**管理者承認グループの管理

マルチ管理者認証（MAV）を有効にする前に、承認権限または拒否権限を付与する管理者を1人以上含む管理者承認グループを作成する必要があります。マルチ管理者認証を有効にすると、承認グループメンバーシップを変更するには、既存の資格管理者のいずれかによる承認が必要になります。

タスクの内容

既存の管理者をMAVグループに追加したり、新しい管理者を作成したりできます。

MAV機能では、既存のRole-Based Access Control（RBAC；ロールベースアクセス制御）設定が使用されます。潜在的なMAV管理者は、MAV管理者グループに追加する前に、保護された操作を実行するための十分な権限を持っている必要があります。"RBACの詳細については、こちらをご覧ください。"

承認リクエストが保留中であることをMAV管理者に通知するようにMAVを設定できます。そのためには、Eメール通知（特にパラメータと `Mail Server`パラメータ）を設定する必要があります `Mail From`。または、これらのパラメータをクリアして通知を無効にすることもできます。電子メールアラートがない場合、MAV管理者は承認キューを手動で確認する必要があります。

ONTAP 9.15.1 以降では、Active Directory (AD) ユーザーを MAV 管理者として設定できます。 ADユーザーは"ONTAP管理者として設定されている"。

System Managerの手順

MAV承認グループを初めて作成する場合は、次の手順を参照してください。"マルチ管理者検証を有効にします。"

既存の承認グループを変更する、または追加の承認グループを作成するには、次の手順を実行します。

1. マルチ管理者認証を受ける管理者を指定します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. [Users and Roles]の横にあるをクリックします → 。*
   c. [Users]の下にあるをクリックします ＋ Add 。*
   d. 必要に応じて名簿を変更します。

      詳細については、を参照してください。 "管理者アクセスの制御"
2. MAV承認グループを作成または変更します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. セクションの[マルチ管理者の承認]*の横にあるをクリックします → 。（MAVがまだ設定されていない場合はアイコンが表示され ⚙ ます）。
      - Name：グループ名を入力します。
      - Approvers：ユーザのリストから承認者を選択します。
      - Email address：Eメール アドレスを入力します。
      - Default group：グループを選択します。

MAVを有効にしたあとで既存の設定を編集するには、MAVの承認が必要です。

CLIの手順

1. パラメータと `Mail Server`パラメータに値が設定されていることを確認します `Mail From`。入力：

   ```
   event config show
   ```

   次のように表示されます。

   ```
   cluster01::> event config show
                              Mail From:  admin@localhost
                            Mail Server:  localhost
                              Proxy URL:  -
                             Proxy User:  -
    Publish/Subscribe Messaging Enabled:  true
   ```

   パラメータを設定するには、次のように入力します。

   ```
   event config modify -mail-from email_address -mail-server server_name
   ```

および `event config modify`の詳細については `event config show`、を"ONTAPコマンド リファレンス"参照してください。

2. 複数管理者による検証を受ける管理者の特定

実行する操作	入力するコマンド
現在の管理者を表示します	`security login show`
現在の管理者のクレデンシャルの変更	`security login modify <parameters>`
新しい管理者アカウントを作成します	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

`security login modify`、および `security login create`の詳細について `security login show`は、をlink:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["ONTAPコマンド リファレンス "^]参照してください。

3. MAV承認グループを作成します。

`security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2…] [[-email address1], address1…]`

- `-vserver`-このリリースでは管理SVMのみがサポートされます。
- `-name`- MAVグループ名（最大64文字）。
- `-approvers`- 1 人以上の承認者のリスト。 ADユーザーの場合は、次の形式を使用します。 `domain\user` 。例： `mydomain\pavan` 。
- `-email`-リクエストが作成、承認、拒否、または実行されたときに通知される1つ以上の電子メールアドレス。

  *例：*次のコマンドは、2つのメンバーと関連付けられたEメールアドレスを持つMAVグループを作成します。

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. グループの作成とメンバーシップを確認します。

`security multi-admin-verify approval-group show`

- 例：*

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name         Approvers         Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

MAVグループの初期設定を変更するには、次のコマンドを使用します。

*注意：*すべての場合、MAV管理者による承認が必要です。

実行する操作	入力するコマンド
グループの特性を変更するか、既存のメンバー情報を変更します	`security multi-admin-verify approval-group modify [parameters]`
メンバーを追加または削除します	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
グループを削除します	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

関連情報

- "セキュリティ マルチ管理者検証"

ONTAPでのマルチ管理者検証の有効化または無効化

Multi-admin Verification（MAV）は明示的にイネーブルにする必要があります。マルチ管理者認証を有効にすると、削除するにはMAV承認グループの管理者（MAV管理者）による承認が必要になります。

タスクの内容

MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。

MAV管理者の承認なしにマルチ管理者検証機能を無効にする必要がある場合は、 NetAppサポートに連絡して次のことを伝えてください。"NetAppナレッジベース: MAV 管理者が利用できない場合にマルチ管理者検証を無効にする方法" 。

MAVをイネーブルにすると、次のパラメータをグローバルに指定できます。

承認グループ

グローバル承認グループのリスト。MAV機能を有効にするには、少なくとも1つのグループが必要です。

MAVを自律型ランサムウェア対策（ARP）で使用している場合は、ARPの一時停止、無効化、疑わしい要求のクリアを承認する新規または既存の承認グループを定義します。

必須の承認者

保護された操作を実行するために必要な承認者の数。デフォルトの最小値は1です。

必要な承認者の数は、デフォルトの承認グループ内の一意の承認者の総数よりも少なくする必要があります。

承認の有効期限（時間、分、秒）

MAV管理者が承認要求に応答する必要がある期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。

実行の有効期限（時間、分、秒）

要求元の管理者が::operationを完了する必要がある期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。

これらのパラメータは、"操作ルール。"

System Managerの手順

1. マルチ管理者認証を受ける管理者を指定します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. [Users and Roles]の横にあるをクリックします → 。*
   c. [Users]の下にあるをクリックします + Add 。*
   d. 必要に応じて名簿を変更します。

      詳細については、を参照してください。 "管理者アクセスの制御"
2. 複数管理者による検証を有効にするには、少なくとも1つの承認グループを作成し、少なくとも1つのルールを追加します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. セクションの[マルチ管理者の承認]*の横にあるをクリックします ⚙ 。
   c. をクリックし + Add て、少なくとも1つの承認グループを追加します。
      - [名前]-グループ名を入力します。
      - 承認者–ユーザーのリストから承認者を選択します。
      - Eメールアドレス–Eメールアドレスを入力します。
      - デフォルトグループ–グループを選択します。
   d. ルールを少なくとも1つ追加してください。
      - 操作–リストからサポートされているコマンドを選択します。

- クエリ–必要なコマンドオプションと値を入力します。
- オプションのパラメータ。グローバル設定を適用する場合は空白のままにし、特定のルールに別の値を割り当ててグローバル設定を上書きします。
  - 必要な承認者数
  - 承認グループ

e. [詳細設定*]をクリックして、デフォルトを表示または変更します。

- 必要な承認者数（デフォルト：1）
- 実行要求の有効期限（デフォルト：1時間）
- 承認リクエストの有効期限（デフォルト：1時間）
- メールサーバ*
- 送信元Eメールアドレス*

  *これらは、「通知管理」で管理されている電子メール設定を更新します。まだ設定されていない場合は、設定を求めるプロンプトが表示されます。

f. Enable（有効）*をクリックしてMAV初期設定を完了します。

初期設定後、現在のMAVステータスが* Multi-Admin Approval *（マルチ管理者承認）タイルに表示されます。

- ステータス（有効または無効）
- 承認が必要なアクティブな処理
- 保留状態のオープン要求の数

をクリックすると、既存の構成を表示できます →。既存の構成を編集するには、MAVの承認が必要です。

マルチ管理者認証を無効にするには：

1. **[Cluster]>[Settings.]**をクリックします
2. セクションの[マルチ管理者の承認]*の横にあるをクリックします ⚙ 。
3. [Enabled]トグルボタンをクリックします。

   この操作を完了するにはMAVの承認が必要です。

CLIの手順

CLIでMAV機能を有効にする前に、少なくとも1つが"MAV管理者グループ"作成されている必要があります。

実行する操作	入力するコマンド

MAV機能を有効にします	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	例：次のコマンドは、MAVを1つの承認グループ、2つの必須承認者、およびデフォルトの有効期限で有効にします。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	少なくとも1つ追加して初期設定を完了する"操作ルール。"

MAV設定の変更（MAVの承認が必要）	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

MAV機能を確認します	`security multi-admin-verify show`
	
	• 例：*
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- --------- ----------`
	`true 2 1h 1h mav-grp1`

MAV機能を無効にする（MAVの承認が必要）	`security multi-admin-verify modify -enabled false`

関連情報

- "セキュリティ マルチ管理者検証"

ONTAPで保護されたオペレーションのマルチ管理者検証ルールを管理します

マルチ管理者認証（MAV）ルールを作成して、承認が必要な操作を指定します。操作が開始されるたびに、保護された操作が傍受され、承認要求が生成されます。

適切なRBAC機能を持つ管理者は、MAVを有効にする前にルールを作成できますが、MAVを有効にすると、ルールセットを変更するにはMAVの承認が必要になります。

1回の操作で作成できるMAVルールは1つだけです。たとえば、複数のルールを作成することはできません `volume-snapshot-delete`。必要なルール制約は1つのルール内に含める必要があります。

保護するルールを作成できます"これらのコマンド"。各コマンドは、コマンドの保護機能が最初に使用可能になったONTAPバージョン以降で保護できます。

MAV system-defaultコマンドのルールは `security multi-admin-verify` "コマンド"変更できません。

システム定義の操作に加えて、マルチ管理者検証が有効になっている場合は次のコマンドがデフォルトで保護されますが、ルールを変更してこれらのコマンドの保護を削除できます。

- "セキュリティログインパスワード"
- "セキュリティログインロック解除"
- "設定"

ルール制約

ルールを作成するときに、オプションを指定して要求をコマンド機能のサブセットに制限することもできます `-query`。 `-query`オプションを使用すると、SVM、ボリューム、Snapshot名などの設定要素を制限することもできます。

たとえば、 `volume snapshot delete`コマンドでを `-query`に設定すると `-snapshot !hourly*,!daily*,!weekly*`、hourly、daily、またはweeklyという属性のプレフィックスが付いたボリュームSnapshotがMAV保護の対象から除外されます。

```
smci-vsim20::> security multi-admin-verify rule show
                                                 Required  Approval
Vserver Operation                                Approvers Groups
------- ---------------------------------------- --------- -------------
vs01    volume snapshot delete                   -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

除外された構成要素はMAVによって保護されず、管理者はそれらを削除または名前変更できます。

デフォルトでは、ルールは、保護された操作が入力されたときに対応するコマンドが自動的に生成されるように指定します `security multi-admin-verify request create` *"protected_operation"*。このデフォルトを変更して、コマンドを個別に入力するように指定でき `request create`ます。

デフォルトでは、ルールには次のグローバルMAV設定が継承されますが、ルール固有の例外を指定することもできます。

- 必要な承認者数
- 承認グループ
- 承認の有効期限
- 実行有効期間

System Managerの手順

保護された処理ルールを初めて追加する場合は、System Managerの手順を参照してください。"マルチ管理者検証を有効にします。"

既存のルールセットを変更するには：

1. [* Cluster]>[Settings]（設定）*を選択します。
2. セクションの[マルチ管理者の承認]*の横にあるを選択します ⚙ 。
3. 少なくとも1つのルールを追加する場合に選択し ＋ Add ます。既存のルールを変更または削除することもできます。
   - 操作–リストからサポートされているコマンドを選択します。
   - クエリ–必要なコマンドオプションと値を入力します。
   - オプションのパラメータ–グローバル設定を適用する場合は空白のままにし、特定のルールに別の値を割り当ててグローバル設定を上書きします。
     - 必要な承認者数
     - 承認グループ

CLIの手順

ⓘ を除き、すべての `security multi-admin-verify rule`コマンドを実行する前にMAV管理者の承認が必要です。 `security multi-admin-verify rule show`

実行する操作	入力するコマンド
ルールの作成	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

現在の管理者のクレデンシャルの変更	`security login modify <parameters>`
	
	例：次のルールでは、ルートボリュームの削除が承認されている必要があります。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

実行する操作	入力するコマンド
ルールを変更します	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
ルールを削除します。	`security multi-admin-verify rule delete -operation "protected_operation"`
ルールを表示します	`security multi-admin-verify rule show`

関連情報

- "セキュリティ マルチ管理者検証ルール"
- "security login modify"

ONTAPで**MAV**保護された操作の実行を要求

Multi-Admin Verification（MAV）が有効になっているクラスタで保護された操作またはコマンドを開始すると、ONTAPは自動的に操作を代行受信し、MAV承認グループの1人以上の管理者（MAV管理者）が承認する必要がある要求の生成を要求します。または、ダイアログなしでMAVリクエストを作成することもできます。

承認された場合は、クエリに応答して、要求の有効期限内に処理を完了する必要があります。拒否された場合、要求数の上限を超えた場合、または有効期限を過ぎた場合は、要求を削除して再送信する必要があります。

MAV機能は、既存のRBAC設定を遵守します。つまり、MAVの設定に関係なく、管理者ロールには、保護対象処理を実行するための十分な権限が必要です。"RBACの詳細については、こちらをご覧ください"です。

MAV管理者の場合は、保護された操作を実行する要求もMAV管理者によって承認されている必要があります。

System Managerの手順

ユーザーがメニュー項目をクリックして操作を開始し、その操作が保護されると、承認要求が生成され、次のような通知がユーザーに送信されます。

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

[*Multi-Admin Requests]ウィンドウは、MAVが有効な場合に使用できます。このウィンドウには、ユーザのログインIDとMAVロール（承認者または未承認）に基づいて保留中のリクエストが表示されます。保留中の要求ごとに、次のフィールドが表示されます。

- 操作
- インデックス（数値）

- ステータス（[保留中]、[承認済み]、[却下済み]、[実行済み]、または[期限切れ]）

  1人の承認者によってリクエストが却下された場合、それ以上のアクションは実行できません。

- クエリ（要求された操作のパラメータまたは値）
- 要求しているユーザ
- リクエストの有効期限：
- （の数）保留中の承認者
- （数）潜在的承認者数

要求が承認されると、要求したユーザは有効期限内に操作を再試行できます。

ユーザーが承認せずに操作を再試行すると、次のような通知が表示されます。

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLIの手順

1. 保護された動作を直接入力するか、MAV requestコマンドを使用して入力します。

   例–ボリュームを削除するには、次のいずれかのコマンドを入力します。

   - `volume delete`

     ```
     cluster-1::*> volume delete -volume vol1 -vserver vs0

     Warning: This operation requires multi-admin verification. To create
     a
              verification request use "security multi-admin-verify
     request
              create".

              Would you like to create a request for this operation?
               {y|n}: y

     Error: command failed: The security multi-admin-verify request (index
     3) is
            auto-generated and requires approval.
     ```

   - `security multi-admin-verify request create "volume delete"`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. リクエストのステータスを確認し、MAV通知に応答します。

   a. 要求が承認されたら、CLIメッセージに応答して処理を完了します。

      ▪ 例：*

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. 要求が拒否された場合、または有効期限が過ぎた場合は、要求を削除し、再送信するかMAV管理者に連絡してください。

- 例：*

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

関連情報

- "セキュリティ マルチ管理者検証"

ONTAPで**MAV**保護された操作要求を管理します。

MAV 承認グループ内の管理者 (MAV 管理者) は、保留中の操作実行要求を通知された場合、一定時間 (承認の有効期限) 内に承認または拒否のメッセージで応答する必要があります。十分な数の承認を得られなかった場合、要求者は要求を削除して別の要求を作成する必要があります。

タスクの内容

承認リクエストはインデックス番号で識別され、電子メールメッセージやリクエストキューの表示に含まれます。

`multi-admin-verify`終了状態のリクエストは自動的に上書きまたは削除される場合があります。使用"監査ログ"以前のリクエストを確認します。

要求キューから次の情報を表示できます。

操作
: 要求が作成される保護された操作。

クエリ
: ユーザーが操作を適用するオブジェクト。

都道府県
: リクエストの現在の状態（保留中、承認済み、却下済み、期限切れ） 実行済み。1人の承認者によってリクエストが却下された場合、それ以上のアクションは実行できません。

必須の承認者
: リクエストを承認するために必要なMAV管理者の数。ユーザーは、操作ルールに必要な承認者パラメータを設定できます。ユーザーがルールに必須承認者を設定していない場合は、グローバル設定の必須承認者が適用されます。

保留中の承認者
: リクエストを承認済みとしてマークするためにリクエストを承認する必要があるMAV管理者の数。

承認の有効期限
: MAV管理者が承認要求に応答する必要がある期間。承認されたユーザーは誰でも、操作ルールの承認期限を設定できます。ルールにapproval-expiryが設定されていない場合は、グローバル設定のapproval-expiryが適用されます。

実行の有効期限
: 要求元の管理者が処理を完了する必要のある期間。許可されたユーザーは誰でも、操作ルールの実行期限を設定できます。ルールにexecution-expiryが設定されていない場合は、グローバル設定のexecution-expiryが適用されます。

ユーザーが承認しました
: リクエストを承認したMAV管理者。

ユーザが拒否しました
: リクエストを拒否したMAV管理者。

Storage VM（SVM）
: 要求が関連付けられているSVM。このリリースでは管理SVMのみがサポートされます。

ユーザが要求しました
: 要求を作成したユーザのユーザ名。

作成時刻
: リクエストが作成された時刻。

承認された時間

リクエストの状態が承認済みに変更された時刻。

コメント

リクエストに関連付けられているコメント。

ユーザが許可されました

リクエストが承認された保護された操作の実行を許可されているユーザーのリスト。が空の場合は `users-permitted`、適切な権限を持つすべてのユーザが処理を実行できます。

System Manager

MAV管理者は、承認要求の詳細、要求の有効期限、要求を承認または却下するためのリンクが記載されたEメール メッセージを受信します。承認ダイアログには、メール内のリンクをクリックするか、システム マネージャーの イベントとジョブ > リクエスト に移動してアクセスできます。

リクエスト ウィンドウは、マルチ管理者検証が有効になっている場合に使用でき、ユーザーのログイン ID と MAV ロール (承認者かどうか) に基づいて保留中のリクエストが表示されます。

- 操作
- インデックス（数値）
- ステータス（[保留中]、[承認済み]、[却下済み]、[実行済み]、または[期限切れ]）

  1人の承認者によってリクエストが却下された場合、それ以上のアクションは実行できません。

- クエリ（要求された操作のパラメータまたは値）
- 要求しているユーザ
- リクエストの有効期限：
- （の数）保留中の承認者
- （数）潜在的承認者数

MAV管理者は、このウィンドウで追加のコントロールを使用できます。個 々 の操作、または選択した操作グループを承認、却下、または削除できます。ただし、MAV管理者が要求ユーザである場合は、自分の要求を承認、拒否、または削除することはできません。

CLI

1. 保留中のリクエストが電子メールで通知された場合は、リクエストのインデックス番号と承認の有効期限を書き留めてください。インデックス番号は、以下に示す **show** または **show-pending** オプションを使用して表示することもできます。
2. 要求を承認または拒否します。

実行する操作	入力するコマンド
リクエストを承認します	`security multi-admin-verify request approve` *`nn`*
要求を拒否します	`security multi-admin-verify request veto` *`nn`*
すべての要求、保留中の要求、または単一の要求を表示します	`security multi-admin-verify request { show`

実行する操作	入力するコマンド
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  キュー内のすべての要求を表示することも、保留中の要求だけを表示することもできます。インデックス番号を入力すると、その要求の情報のみが表示されます。特定のフィールドに関する情報（パラメータを使用）またはすべてのフィールドに関する情報（パラメータを使用）を表示できます `-fields`、 `-instance`。
リクエストを削除します	`security multi-admin-verify request delete` *nn*

例：

次のシーケンスは、MAV管理者がインデックス番号3のリクエスト電子メールを受信した後、リクエストを承認します。インデックス番号3はすでに1つの承認を持っています。

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

例：

次のシーケンスでは、MAV管理者がインデックス番号3の要求電子メールを受信した後、要求が拒否されます。この電子メールにはすでに1つの承認が設定されています。

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State    Approvers Requestor
----- -------------- ----- -------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

関連情報

- "セキュリティ マルチ管理者検証"

動的許可の管理

ONTAP動的認証の詳細

ONTAP 9.15.1以降では、管理者は動的許可を設定し有効化することで、ONTAPへのリモート アクセス時のセキュリティを強化するとともに、悪意のあるユーザによる攻撃の被害を軽減できます。ONTAP 9.15.1の動的許可は初期段階のフレームワークであり、ユーザにセキュリティ スコアを割り当て、その行動が不審な場合に追加の許可チェックを実施するか、操作を完全に拒否できます。管理者はルールの作成、信頼スコアの割り当

て、コマンドの制限を行い、ユーザの特定の行動を許可または拒否するタイミングを指定できます。動的許可の有効化は、クラスタ全体または個別のStorage VMに対して行えます。

動的許可の仕組み

動的許可では、信頼スコア システムに基づき、許可ポリシーに応じた各種信頼レベルをユーザに割り当てます。ユーザの信頼レベルに応じて、その操作を許可または拒否するか、追加の認証を求めることができます。

"動的許可のカスタマイズ"基準スコアの重みおよびその他の動的認可属性の設定方法については、を参照してください。

信頼できるデバイス

動的認可が使用されている場合、信頼できるデバイスの定義は、ユーザが認証方式の1つとして公開鍵認証を使用してONTAPにログインするために使用するデバイスです。デバイスは、そのユーザだけが対応する秘密鍵を所有しているため、信頼されています。

動的許可の例

たとえば、3人のユーザがボリュームを削除しようとするとします。ユーザーが操作を実行しようとすると、各ユーザーのリスク評価が検査されます。

- 最初のユーザーが信頼できるデバイスからログインし、以前に認証エラーがほとんど発生しなかったため、リスクレーティングが低くなります。この操作は追加の認証なしで許可されます。
- 2番目のユーザーは、以前の認証失敗の割合が中程度で、信頼できるデバイスからログインします。これにより、リスク評価は中程度になります。操作が許可される前に、追加の認証を要求されます。
- 3番目のユーザーは、以前の認証失敗の割合が高い信頼されていないデバイスからログインします。これにより、リスクレーティングが高くなります。操作は許可されません。

次のステップ

- "動的許可の有効化または無効化"
- "動的許可のカスタマイズ"

ONTAPでの動的許可の有効化または無効化

ONTAP 9 .15.1以降では、管理者は、コンフィギュレーションをテストするモードでダイナミック認可を設定し、イネーブルにすることができます。また、コンフィギュレーションを `enforced`アクティブにするモードでは、SSH経由で接続するCLIユーザのコンフィギュレーションをアクティブにすることもできます `visibility`。動的認可が不要になった場合は、ディセーブルにすることができます。ダイナミック許可をディセーブルにしても、コンフィギュレーション設定は使用可能なままであり、後で再度イネーブルにする場合に使用できます。

の詳細については `security dynamic-authorization modify`、を"ONTAPコマンド リファレンス"参照してください。

テストの動的許可を有効にする

表示モードで動的許可を有効にすると、機能をテストして、ユーザが誤ってロックアウトされないようにすることができます。このモードでは、信頼スコアはすべての制限されたアクティビティでチェックされますが、強制はされません。ただし、拒否された、または追加の認証チャレンジの対象となるアクティビティはすべてログに記録されます。ベストプラクティスとして、強制する前に、このモードで目的の設定をテストすることを推奨します。

> この手順を実行すると、他のダイナミック認可設定をまだ設定していない場合でも、初めてダイナミック認可をイネーブルにできます。"動的許可のカスタマイズ"その他の動的認証設定を環境に合わせてカスタマイズする手順については、を参照してください。

手順

1. グローバル設定を設定し、機能の状態をに変更することにより、可視モードでダイナミック許可をイネーブルにし `visibility`ます。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。括弧<>の値を環境に合わせて更新します。太字のパラメータは必須です。

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. コマンドを使用してグローバル設定を表示し、結果を確認し `show`ます。

```
security dynamic-authorization show
```

強制モードでの動的許可の有効化

強制モードでダイナミック許可をイネーブルにできます。通常、このモードは、可視化モードでのテストを完了した後に使用します。このモードでは、すべての制限されたアクティビティで信頼スコアがチェックされ、制限条件が満たされるとアクティビティ制限が適用されます。抑制間隔も適用されるため、指定された間隔内での追加の認証チャレンジを防ぐことができます。

> この手順は、事前にモードでダイナミック許可を設定してイネーブルにしていることを前提としてい `visibility`ます。これを強く推奨します。

手順

1. ステートをに変更して、モード `enforced`でダイナミック認可をイネーブルにし `enforced`ます。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。括弧<>の値を環境に合わせて更新します。太字のパラメータは必須です。

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. コマンドを使用してグローバル設定を表示し、結果を確認し `show`ます。

```
security dynamic-authorization show
```

動的許可の無効化

追加した認証セキュリティが不要になった場合、動的許可を無効化できます。

手順

1. 動的認可をディセーブルにするには、そのステートをに変更し `disabled`ます。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。括弧<>の値を環境に合わせて更新します。太字のパラメータは必須です。

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. コマンドを使用してグローバル設定を表示し、結果を確認し `show`ます。

```
security dynamic-authorization show
```

の詳細については `security dynamic-authorization show`、を"ONTAPコマンド リファレンス"参照してください。

次のステップ

（任意）使用する環境に応じて、"動的許可のカスタマイズ"その他のダイナミック認可設定を構成するには、を参照してください。

ONTAPでの動的許可のカスタマイズ

管理者は、動的許可のさまざまな設定をカスタマイズして、自身がONTAPクラスタにリモートでSSH接続する際のセキュリティを高められます。

セキュリティのニーズに応じて、以下の動的許可設定をカスタマイズできます。

- [動的認証グローバル設定の構成]
- [動的認証信頼スコアコンポーネントの設定]

- [カスタム信頼スコアプロバイダの設定]
- [制限されたコマンドの設定]
- [動的許可グループの設定]

動的認証グローバル設定の構成

動的許可のグローバル設定を行うことができます。これには、セキュアなStorage VM、認証チャレンジの抑制間隔、信頼スコアの設定などが含まれます。

の詳細については `security login domain-tunnel create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. 動的認可のグローバル設定を構成します。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。かっこ<>の値を環境に合わせて更新します。

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 作成された構成を表示します。

```
security dynamic-authorization show
```

制限されたコマンドの設定

ダイナミック許可をイネーブルにすると、この機能には制限されたコマンドのデフォルトセットが含まれます。このリストは、必要に応じて変更できます。制限されたコマンドのデフォルトリストについては、を参照して"Multi-Admin Verification（MAV）ドキュメント"ください。

制限されたコマンドの追加

動的許可で制限されているコマンドのリストにコマンドを追加できます。

の詳細については `security dynamic-authorization rule create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを追加します。角かっこ（<>）内の値は環境に合わせて変更してください。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. 変更後の制限コマンド リストを確認します。

```
security dynamic-authorization rule show
```

制限コマンドの削除

動的許可で制限するコマンドのリストからコマンドを削除できます。

の詳細については `security dynamic-authorization rule delete`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを削除します。角かっこ（<>）内の値は環境に合わせて変更してください。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. 変更後の制限コマンド リストを確認します。

```
security dynamic-authorization rule show
```

動的許可グループの設定

デフォルトでは、動的許可を有効化すると、ただちにすべてのユーザとグループに適用されます。ただし、コマンドを使用してグループを作成すると `security dynamic-authorization group create`、動的認可が特定のユーザにのみ適用されるようになります。

動的認可グループを追加します。

ダイナミック認可グループを追加できます。

の詳細については `security dynamic-authorization group create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. グループを作成します。角かっこ（<>）内の値は環境に合わせて変更してください。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. 変更後の動的許可グループを確認します。

```
security dynamic-authorization group show
```

動的許可グループの削除

動的許可グループを削除できます。

の詳細については `security dynamic-authorization group delete`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. グループを削除します。角かっこ（<>）内の値は環境に合わせて変更してください。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. 変更後の動的許可グループを確認します。

```
security dynamic-authorization group show
```

動的認証信頼スコアコンポーネントの設定

スコアリング基準の優先度を変更したり、リスクスコアリングから特定の基準を削除したりするために、最大スコアウェイトを設定できます。

ベストプラクティスとして、デフォルトのスコアウェイト値はそのままにし、必要な場合にのみ調整することを推奨します。

の詳細については `security dynamic-authorization trust-score-component modify`、を"ONTAPコマンド リファレンス"参照してください。

変更可能なコンポーネントは、デフォルトのスコアとパーセンテージの重みとともに次のとおりです。

基準	コンポーネント名	デフォルトの未加工スコアの重み	デフォルトの重量パーセンテージ
信頼できるデバイス	`trusted-device`	20	50
ユーザのログイン認証履歴	`authentication-history`	20	50

手順

1. 信頼スコアコンポーネントを変更します。括弧<>の値を環境に合わせて更新します。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. 変更後の信頼スコア コンポーネント設定を確認します。

```
security dynamic-authorization trust-score-component show
```

ユーザの信頼スコアのリセット

ユーザがシステム ポリシーによりアクセスを拒否されたものの、その身元を証明可能な場合、管理者はそのユーザの信頼スコアをリセットできます。

の詳細については `security dynamic-authorization user-trust-score reset`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを追加します。リセット可能な信頼スコアコンポーネントのリストについては、を参照してください[動的認証信頼スコアコンポーネントの設定]。括弧<>の値を環境に合わせて更新します。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

信頼スコアの閲覧

ユーザは、ログイン セッションにおける自分の信頼スコアを閲覧できます。

手順

1. 信頼スコアを表示します。

```
security login whoami
```

次のような出力が表示されます。

```
User: admin
Role: admin
Trust Score: 50
```

の詳細については `security login whoami`、を"ONTAPコマンド リファレンス"参照してください。

カスタム信頼スコアプロバイダの設定

外部の信頼スコアプロバイダーからスコアリングメソッドをすでに受信している場合は、カスタムプロバイダーを動的認可設定に追加できます。

開始する前に

- カスタム信頼スコアプロバイダはJSON応答を返す必要があります。次の構文要件を満たす必要があります。
  - 信頼スコアを返すフィールドは、配列要素ではなくスカラーである必要があります。
  - 信頼スコアを返すフィールドは、のようにネストされたフィールドにすることができます `trust_score.value`。
  - JSON応答内に数値の信頼スコアを返すフィールドが必要です。これがネイティブで利用できない場合は、この値を返すラッパースクリプトを記述できます。
- 提供される値は、信頼スコアまたはリスクスコアのいずれかです。違いは、信頼スコアが昇順で、高いスコアが高い信頼レベルを示し、リスクスコアが降順であることです。たとえば、0～100のスコア範囲の信頼スコアが90の場合、そのスコアが非常に信頼性が高く、追加のチャレンジなしで「許可」になる可能性があることを示します。一方、0～100のスコア範囲のリスクスコアが90の場合は、リスクが高く、追加のチャレンジなしで「拒否」になる可能性があります。
- カスタム信頼スコアプロバイダには、ONTAP REST API経由でアクセスできる必要があります。
- カスタム信頼スコアプロバイダは、サポートされているパラメータのいずれかを使用して設定する必要があります。サポートされているパラメータリストにない設定を必要とするカスタム信頼スコアプロバイダはサポートされません。

  の詳細については `security dynamic-authorization trust-score-component create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. カスタム信頼スコアプロバイダを追加します。括弧<>の値を環境に合わせて更新します。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 変更後の信頼スコア プロバイダ設定を確認します。

```
security dynamic-authorization trust-score-component show
```

カスタム信頼スコア プロバイダ タグの設定

外部の信頼スコア プロバイダとの通信にタグを使用できます。こうすることで、機密情報を漏えいさせることなく、URLで信頼スコア プロバイダに情報を送信できます。

の詳細については `security dynamic-authorization trust-score-component create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. 信頼スコアプロバイダタグを有効にします。括弧<>の値を環境に合わせて更新します。パラメータを使用しない場合、 `-vserver`コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

例：

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

OAuth 2.0を使用した認証と許可

ONTAP OAuth 2.0実装の概要

ONTAP 9 .14以降では、Open Authorization (OAuth 2.0)フレームワークを使用してONTAPクラスタへのアクセスを制御するオプションが用意されています。この機能は、ONTAP CLI、System Manager、REST APIなど、ONTAP管理インターフェイスを使用して設定できます。ただし、OAuth 2.0の承認とアクセス制御の決定は、クライアントがREST APIを使用してONTAPにアクセスする場合にのみ適用できます。

OAuth 2.0のサポートは、ONTAP 9 .14.0で初めて導入されたため、使用しているONTAPリリースに依存します。詳細については、を参照してください "ONTAPリリースノート"。

機能とメリット

ONTAPでOAuth 2.0を使用する主な機能と利点を以下に説明します。

OAuth 2.0標準のサポート

OAuth 2.0は業界標準の認可フレームワークです。署名付きアクセストークンを使用して、保護されたリソースへのアクセスを制限および制御するために使用されます。OAuth 2.0を使用すると、次のような利点があります。

- 認証設定の多くのオプション
- パスワードを含むクライアントのクレデンシャルは絶対に公開しない
- トークンは構成に基づいて有効期限が切れるように設定できます
- REST APIでの使用に最適

一般的な認証サーバでテスト済み

ONTAP OAuth 2.0の実装は、次のようにONTAPリリースに基づいたいくつかの一般的なサーバーまたはサービスでテストされています。

- UUID.16.1（グループUUIDとネームマッピングおよび外部ロールのサポート）ONTAP 9：
  - MicrosoftエントラID
- OAuth .14.1（標準OAuth 2.0機能のサポートONTAP 9）
  - Auth0
  - Active Directoryフェデレーションサービス（ADFS）
  - キークローク

各ONTAPリリースで使用できる機能の詳細については、を参照してください"認証サーバとアクセストークン"。

複数の同時認証サーバのサポート

1つのONTAPクラスタに対して最大8つの許可サーバを定義できます。これにより、多様なセキュリティ環境のニーズに柔軟に対応できます。

RESTロールトノトウゴウ

ONTAP認証の決定は、最終的にはユーザまたはグループに割り当てられたRESTロールに基づいて行われます。これらのロールは、自己完結型スコープとしてアクセストークン内で伝送されるか、Active DirectoryまたはLDAPグループとともにローカルONTAP定義に基づいて伝送されます。

送信者に制約されたアクセストークンを使用するオプション

クライアント認証を強化するMutual Transport Layer Security（MTLS）を使用するようにONTAPおよび認可サーバを設定できます。これにより、OAuth 2.0アクセストークンが最初に発行されたクライアントによってのみ使用されることが保証されます。この機能は、FAPIやMITERによって確立されたものを含む、いくつかの一般的なセキュリティ推奨事項をサポートし、それらと一致しています。

実装と構成

大まかに言えば、OAuth 2.0の実装と構成にはいくつかの側面があり、開始時に考慮する必要があります。

ONTAP内のOAuth 2.0エンティティ

OAuth 2.0認証フレームワークは、データセンターまたはネットワーク内の実際の要素または仮想要素にマッピングできる複数のエンティティを定義します。OAuth 2.0エンティティとそのONTAPへの適応を以下の表に示します。

OAuth 2.0エンティティ	説明
リソース	内部ONTAPコマンドを使用してONTAPリソースへのアクセスを提供するREST APIエンドポイント。
リソース所有者	保護されたリソースを作成した、またはデフォルトでそのリソースを所有しているONTAPクラスタユーザ。
リソースサーバ	保護されているリソースのホスト（ONTAPクラスタ）。
クライアント	リソース所有者に代わって、または権限を持ってREST APIエンドポイントへのアクセスを要求するアプリケーション。
許可サーバ	通常、アクセストークンの発行と管理ポリシーの適用を担当する専用サーバです。

コアONTAP構成

OAuth 2.0を有効にして使用するようにONTAPクラスタを設定する必要があります。これには、認可サーバへの接続の確立と、必要なONTAP認可設定の定義が含まれます。この設定は、次のいずれかの管理インターフェイスを使用して実行できます。

- ONTAPコマンドラインインターフェイス
- System Manager
- ONTAP REST API

環境およびサポートサービス

ONTAP定義に加えて、認可サーバも設定する必要があります。グループとロールのマッピングを使用している場合は、Active Directoryグループまたは LDAPに相当するものも設定する必要があります。

サポートされるONTAPクライアント

ONTAP 9 .14以降では、REST APIクライアントからOAuth 2.0を使用してONTAPにアクセスできます。REST API呼び出しを実行する前に、認証サーバからアクセストークンを取得する必要があります。次に、クライア

ントは、HTTP認証要求ヘッダーを使用して、このトークンを_bearer token_としてONTAPクラスタに渡します。必要なセキュリティのレベルに応じて、クライアントで証明書を作成してインストールし、MTLSに基づいて送信者に制約されたトークンを使用することもできます。

選択した用語

ONTAPを使用したOAuth 2.0デプロイメントの検討を開始する際には、いくつかの用語について理解しておくと役立ちます。OAuth 2.0の詳細については、を参照してください"その他のリソース"。

アクセストークン

認証サーバーによって発行され、保護されたリソースへのアクセス要求を行うためにOAuth 2.0クライアントアプリケーションによって使用されるトークン。

JSON Webトークン

アクセストークンのフォーマットに使用される標準。JSONは、OAuth 2.0の要求を3つの主要セクションに配置したコンパクトな形式で表現するために使用されます。

送信者に制約されたアクセストークン

Mutual Transport Layer Security（MTLS）プロトコルに基づくオプションの機能。トークンで追加の確認要求を使用することで、アクセストークンが最初に発行されたクライアントによってのみ使用されるようになります。

JSON Webキーセット

JWKSは、ONTAPがクライアントから提示されたJWTトークンを検証するために使用する公開鍵の集まりです。キーセットは、通常、認証サーバで専用のURIを使用して使用できます。

適用範囲

スコープは、ONTAP REST APIなどの保護されたリソースへのアプリケーションのアクセスを制限または制御する手段を提供します。これらは、アクセストークン内の文字列として表されます。

ONTAP RESTロール

RESTロールはONTAP 9 .6で導入されたロールで、ONTAP RBACフレームワークの中核をなす要素です。これらのロールは、ONTAPで引き続きサポートされている以前の従来のロールとは異なります。ONTAPのOAuth 2.0実装では、RESTロールのみがサポートされています。

HTTP認証ヘッダー

REST API呼び出しの一部としてクライアントと関連する権限を識別するためのHTTP要求に含まれるヘッダー。認証と認可の実行方法に応じて、いくつかの種類または実装があります。OAuth 2.0アクセストークンをONTAPに提示する場合、トークンは_bearer token_として識別されます。

HTTPベーシック認証

初期のHTTP認証技術はまだONTAPでサポートされています。プレーンテキストのクレデンシャル（ユーザ名とパスワード）はコロンで連結され、base64でエンコードされます。文字列は認可要求ヘッダーに配置され、サーバに送信されます。

FAPI

OpenID Foundationのワーキンググループで、金融業界向けにプロトコル、データスキーマ、およびセキュリティに関する推奨事項を提供しています。このAPIは元 々 Financial Grade APIとして知られていた。

マイター

米国空軍と米国政府に技術的および安全保障上のガイダンスを提供する民間の非営利企業。

その他のリソース

いくつかの追加リソースを以下に示します。OAuth 2.0と関連規格の詳細については、これらのサイトを参照してください。

プロトコルと標準

- "RFC 6749: OAuth 2.0認可フレームワーク"
- "RFC 7519：JSON Webトークン（JWT）"
- "RFC 7523: OAuth 2.0クライアントの認証と承認のためのJSON Webトークン（JWT）プロファイル"
- "RFC 7662：『OAuth 2.0 Token Introspection』"
- "RFC 7800：『Proof-of-Possession Key for JWT』"
- "RFC 8705：『OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens』"

組織

- "OpenID基盤"
- "FAPIワーキンググループ"
- "マイター"
- "IANA-JWT"

製品とサービス

- "Auth0"
- "エントラID"
- "ADFSの概要"
- "キークローク"

その他のツールとユーティリティ

- "Auth0によるJWT"
- "OpenSSL"

NetAppのドキュメントとリソース

- "ONTAP自動化に関するドキュメント"

概念

ONTAPの**OAuth 2.0**認証サーバーとアクセストークン

認可サーバーは、OAuth 2.0 Authorizationフレームワーク内の中心的なコンポーネントとしていくつかの重要な機能を実行します。

OAuth 2.0認可サーバ

認証サーバは、主にアクセストークンの作成と署名を行います。これらのトークンには、クライアントアプリケーションが保護されたリソースに選択的にアクセスできるように、IDおよび承認情報が含まれています。これらのサーバは通常、相互に分離されており、スタンドアロンの専用サーバとして、またはより大きなIDおよびアクセス管理製品の一部として、いくつかの異なる方法で実装できます。

> OAuth 2.0の機能がより大きなIDおよびアクセス管理製品またはソリューション内にパッケージ化されている場合は特に、認可サーバーに異なる用語が使用されることがあります。たとえば、*アイデンティティプロバイダ（IdP）*という用語は、*認証サーバ*と同じ意味でよく使用されます。

管理

アクセストークンの発行に加えて、認可サーバーは一般的にWebユーザーインターフェイスを介して関連する管理サービスも提供します。たとえば、次の項目を定義および管理できます。

- ユーザおよびユーザ認証
- スコープ
- テナントとレルムによる管理の分離
- ポリシーの適用
- さまざまな外部サービスへの接続
- その他のIDプロトコル（SAMLなど）のサポート

ONTAPは、OAuth 2.0標準に準拠した認可サーバーと互換性があります。

ONTAPニテイキ

1つ以上の認可サーバをONTAPに定義する必要があります。ONTAPは、各サーバとセキュアに通信してトークンを検証し、クライアントアプリケーションをサポートするその他の関連タスクを実行します。

ONTAP構成の主な側面を以下に示します。詳細については、も参照してください"OAuth 2.0の導入シナリオ"。

アクセストークンの検証方法と検証場所

アクセストークンを検証するには、2つのオプションがあります。

- ローカル検証

  ONTAPは、トークンを発行した認可サーバーから提供された情報に基づいて、アクセストークンをローカルで検証できます。認証サーバから取得された情報はONTAPによってキャッシュされ、定期的に更新されます。

- リモートイントロスペクション

  リモートイントロスペクションを使用して、認証サーバーでトークンを検証することもできます。イントロスペクションは、許可された当事者がアクセストークンについて認可サーバーに問い合わせることを可能にするプロトコルです。ONTAPは、アクセストークンから特定のメタデータを抽出し、トークンを検証する方法を提供します。ONTAPは、パフォーマンス上の理由から一部のデータをキャッシュします。

ネットワークの場所

ONTAPはファイアウォールの背後にある可能性があります。この場合は、設定の一部としてプロキシを指定する必要があります。

許可サーバの定義方法

ONTAPに対する認証サーバは、CLI、System Manager、REST APIなどの任意の管理インターフェイスを使用して定義できます。たとえば、CLIではコマンドを使用し `security oauth2 client create`ます。

の詳細については `security oauth2 client create`、を"ONTAPコマンド リファレンス"参照してください。

認証サーバの数

1つのONTAPクラスタに対して最大8つの許可サーバを定義できます。発行者または発行者/オーディエンスの要求が一意である限り、同じ認証サーバを同じONTAPクラスタに複数回定義できます。たとえば、Keycloakでは、異なるレルムを使用する場合は常にこのようになります。

ONTAPでサポートされるOAuth 2.0機能

OAuth 2.0のサポートは、最初はONTAP 9 .14.1で利用可能でしたが、その後のリリースでも引き続き強化されています。ONTAPでサポートされているOAuth 2.0の機能を以下に説明します。

特定のONTAPリリースで導入された機能は、今後のリリースでも引き継がれます。

ONTAP 9 .16.1

ONTAP 9 .16.1では、標準のOAuth 2.0機能が拡張され、ネイティブのエントラIDグループ用のエントラID固有の拡張機能が含まれるようになりました。これには、名前の代わりにアクセストークンでGUIDを使用する必要があります。さらに、このリリースでは、アクセストークンの「roles」フィールドを使用してネイティブアイデンティティプロバイダのロールをONTAPのロールにマッピングするための外部ロールマッピングのサポートが追加されています。

ONTAP 9 .14.1

ONTAP 9 .14.1以降では、を使用するアプリケーションの次の標準OAuth 2.0機能を通じて、認証サーバがサポートされています。

- およびで説明されているように、「ISS」、「AUD」、および "RFC 7519：JSON Webトークン（JWT）"「exp」を含む標準フィールドを持つOAuth 2.0 "RFC6749: OAuth 2.0認可フレームワーク"。これには、「UPN」、「appid」、「sub」、「username」、「preferred_username」などのアクセストークンのフィールドを使用してユーザーを一意に識別するサポートも含まれます。
- 「group」フィールドを持つグループ名に対するADFSベンダー固有の拡張子。
- 「group」フィールドを持つグループUUIDに対するAzureベンダー固有の拡張機能。
- OAuth 2.0アクセストークンスコープ内の自己完結型および名前付きロールを使用した認証サポートのためのONTAP拡張。これには、「scope」フィールドと「scp」フィールド、およびスコープ内のグループ名が含まれます。

OAuth 2.0アクセストークンの使用

認証サーバによって発行されたOAuth 2.0アクセストークンはONTAPによって検証され、REST APIクライアント要求のロールベースアクセスの決定に使用されます。

アクセストークンの取得

REST APIを使用するONTAPクラスタに定義されている認証サーバからアクセストークンを取得する必要があります。トークンを取得するには、認可サーバーに直接問い合わせる必要があります。

> ONTAPは、アクセストークンを発行したり、クライアントから承認サーバに要求をリダイレクトしたりしません。

トークンの要求方法は、次のようないくつかの要因によって異なります。

- 認可サーバとその設定オプション
- OAuth 2.0認可タイプ
- 要求の発行に使用するクライアントまたはソフトウェアツール

付与タイプ

a_grant_は、OAuth 2.0アクセストークンの要求と受信に使用される、ネットワークフローのセットを含む明確に定義されたプロセスです。クライアント、環境、およびセキュリティの要件に応じて、いくつかの異なる権限付与タイプを使用できます。一般的な付与タイプの一覧を以下の表に示します。

付与タイプ	説明
クライアントクレデンシャル	クレデンシャル（IDや共有シークレットなど）のみを使用する一般的な付与タイプ。クライアントは、リソース所有者と密接な信頼関係を持っていると想定されます。
パスワード	リソース所有者パスワード資格情報付与タイプは、リソース所有者がクライアントとの信頼関係を確立している場合に使用できます。また、レガシーHTTPクライアントをOAuth 2.0に移行する場合にも役立ちます。
認証コード	これは機密クライアントにとって理想的な認可タイプであり、リダイレクトベースのフローに基づいています。アクセストークンとリフレッシュトークンの両方を取得するために使用できます。

JWTの内容

OAuth 2.0アクセストークンはJWT形式です。コンテンツは、設定に基づいて認可サーバによって作成されます。ただし、トークンはクライアントアプリケーションには不透明です。クライアントには、トークンを検査したり、コンテンツを認識したりする理由はありません。

各JWTアクセストークンには、クレームのセットが含まれています。クレームは、発行者の特性と認可サーバーでの管理定義に基づいた認可を記述します。この規格に登録されている請求の一部は、次の表に記載されています。すべての文字列で大文字と小文字が区別されます。

請求	キーワード	説明
発行者	ISS	トークンを発行したプリンシパルを識別します。請求処理はアプリケーション固有です。
件名	サブ	トークンのサブジェクトまたはユーザ。名前のスコープは、グローバルまたはローカルで一意になります。
対象読者	豪ドル	トークンの対象となる受信者。文字列の配列として実装されます。

請求	キーワード	説明
有効期限	有効期限	トークンが期限切れになり、拒否されるまでの時間。

詳細については、を参照してください "RFC 7519：JSON Webトークン" 。

クライアント許可

ONTAPクライアント許可の概要とオプション

ONTAP OAuth 2.0の実装は、柔軟性と堅牢性を考慮して設計されており、ONTAP環境を保護するために必要な機能を提供します。同時に指定できない設定オプションがいくつかあります。承認の決定は、最終的には、OAuth 2.0アクセストークンに含まれるか、OAuth 2.0アクセストークンから派生したONTAP RESTロールに基づいて行われます。

OAuth 2.0の認可を設定する場合にのみ使用でき"ONTAP RESTロール"ます。以前のONTAPの従来のロールはサポートされていません。

ONTAPは、設定に基づいて、最も適切な1つの許可オプションを適用します。ONTAPによるクライアントアクセスの決定方法の詳細については、を参照してください"ONTAPニヨルアクセスノケツテイホウホウ"。

OAuth 2.0の自己完結型スコープ

これらのスコープには、1つ以上のカスタムRESTロールが含まれており、それぞれがアクセストークン内の1つの文字列内にカプセル化されています。ONTAPロールの定義には依存しません。認可サーバでスコープ文字列を設定する必要があります。詳細については、を参照してください "自己完結型OAuth 2.0スコープ" 。

ローカル**ONTAP REST**ロール

組み込みまたはカスタムの名前付きRESTロールを1つ使用できます。指定したロールのscope構文は、* ontap-role-*<URL-encoded-ONTAP-role-name>です。たとえば、ONTAPロールがスコープ文字列の場合、`admin`はになります `ontap-role-admin`。

ユーザ

アプリケーション「http」へのアクセスで定義されたアクセストークン内のユーザー名を使用できます。ユーザは、定義された認証方式に基づいて、パスワード、ドメイン（Active Directory）、nsswitch（LDAP）の順にテストされます。

グループ

認可サーバは、認可にONTAPグループを使用するように設定できます。ローカルONTAPの定義を調べても、アクセスを決定できない場合は、Active Directory（「domain」）またはLDAP（「nsswitch」）グループが使用されます。グループ情報は、次の2つの方法のいずれかで指定できます。

- OAuth 2.0スコープ文字列

  グループメンバーシップを持つユーザがいない場合、クライアントのクレデンシャルフローを使用して機密アプリケーションをサポートします。スコープには* ontap-group-*<URL-encoded-ONTAP-group-name>という名前を付けます。たとえば、グループが「development」の場合、スコープ文字列は「ontap-group-development」になります。

- 「グループ」の主張

これは、リソース所有者(パスワード付与)フローを使用してADFSによって発行されるアクセストークンを対象としています。

見る"ONTAPでのOAuth 2.0またはSAML IdPグループの使用"詳細についてはこちらをご覧ください。

ONTAPにおける自己完結型OAuth 2.0スコープ

自己完結型スコープは、アクセストークンで伝送される文字列です。各ロールは完全なカスタムロール定義であり、アクセスを決定するためにONTAPが必要とするすべての機能が含まれています。スコープは、ONTAP内で定義されているRESTロールとは別のものです。

スコープ文字列の形式

基本レベルでは、スコープは連続した文字列として表され、コロンで区切られた6つの値で構成されます。スコープ文字列で使用されるパラメータについては、以下で説明します。

ONTAPリテラル

スコープは、小文字のリテラル値で始まる必要があります `ontap`。これにより、範囲がONTAPに固有であることが識別されます。

クラスタ

スコープを適用するONTAPクラスタを定義します。次の値を指定できます。

- クラスタUUID

  単一のクラスタを識別します。

- アスタリスク(*)

  スコープがすべてのクラスタに適用されることを示します。

クラスタのUUIDは、ONTAP CLIのコマンドを使用して表示できます `cluster identity show`。指定しない場合、範囲はすべてのクラスタに適用されます。の詳細については `cluster identity show`、を"ONTAPコマンド リファレンス"参照してください。

ロール

自己完結型スコープに含まれるRESTロールの名前。この値は、ONTAPで検証されたり、ONTAPに定義されている既存のRESTロールと照合されたりすることはありません。この名前はロギングに使用されます。

アクセスレベル

この値は、スコープ内でAPIエンドポイントを使用するときにクライアントアプリケーションに適用されるアクセスレベルを示します。次の表に示す6つの値があります。

アクセスレベル	説明
なし	指定したエンドポイントへのすべてのアクセスを拒否します。
読み取り専用	GETを使用した読み取りアクセスのみを許可します。
read_create	POSTを使用して、読み取りアクセスと新しいリソースインスタンスの作成を許可します。
read_modify	読み取りアクセスを許可し、PATCHを使用して既存のリソースを更新する機能を許可します。
read_create_modify	削除以外のすべてのアクセスを許可します。許可される処理は、GET（読み取り）、POST（作成）、およびPATCH（更新）です。
すべて	フルアクセスを許可します。

SVM

スコープが適用されるクラスタ内のSVMの名前。すべてのSVMを示すために、*（アスタリスク）を使用します。

この機能は、ONTAP 9.14.1では完全にはサポートされていません。SVMのパラメータは無視して、プレースホルダにアスタリスクを使用できます。で "ONTAPリリースノート"今後のSVMのサポートを確認します。

REST API URI

リソースまたは関連リソースのセットへの完全パスまたは部分パス。文字列はで始まる必要があります `/api`。値を指定しない場合、スコープはONTAPクラスタのすべてのAPIエンドポイントに適用されます。

範囲の例

自己完結型スコープの例を以下に示します。

ONTAP：：joes-role：read_create_modify：：/api/cluster

このロールを割り当てられたユーザに、エンドポイントへの読み取り、作成、および変更アクセスを許可します `/cluster`。

CLI管理ツール

自己完結型スコープの管理を容易にし、エラーが発生しにくくするために、ONTAPには、入力パラメータに基づいてスコープ文字列を生成するCLIコマンドが用意されて `security oauth2 scope`います。

コマンド `security oauth2 scope`には、入力内容に基づいて次の2つのユースケースがあります。

- 文字列をスコープするCLIパラメータ

  このバージョンのコマンドを使用すると、入力パラメータに基づいてスコープ文字列を生成できます。

- scope string to CLIパラメータ

  このバージョンのコマンドを使用すると、入力スコープ文字列に基づいてコマンドパラメータを生成できます。

例

次の例では、次のコマンド例のあとに出力が含まれたスコープ文字列を生成します。この定義はすべてのクラスタに適用されます。

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

の詳細については `security oauth2 scope`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPにおけるOAuth 2.0外部ロールマッピング

外部ロールは、ONTAPで使用するように設定されたIdentifyプロバイダで定義されます。ONTAP CLIを使用して、これらの外部ロールとONTAPロールのマッピング関係を作成および管理できます。

ONTAP REST APIを使用して外部ロールマッピング機能を設定することもできます。詳細については、を "ONTAP自動化に関するドキュメント"参照してください。

アクセストークンの外部ロール

これは、2つの外部ロールを含むJSONアクセストークンの一部です。

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

構成

外部ロールマッピング機能は、ONTAPコマンドラインインターフェイスを使用して管理できます。

作成

ロールマッピング設定は、コマンドを使用して定義できます `security login external-role-mapping create`。このコマンドおよび関連するオプションを実行するには、ONTAP * admin *権限レベルである必要があります。

パラメータ

グループマッピングの作成に使用するパラメータを次に示します。

パラメータ	説明
`external-role`	外部のアイデンティティプロバイダで定義されているロールの名前。
`provider`	アイデンティティプロバイダの名前。これはシステムの識別子である必要があります。
`ontap-role`	外部ロールがマッピングされている既存のONTAPロールを示します。

例

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

の詳細については `security login external-role-mapping create`、を"ONTAPコマンド リファレンス"参照してください。

その他の**CLI**処理

このコマンドでは、次のような追加の処理がサポートされます。

- - 表示
- 変更
- 削除

関連情報

- "ONTAPコマンド リファレンス"

ONTAPニヨルクライアントアクセスノケツテイホウホウ

OAuth 2.0を適切に設計および実装するには、ONTAPが許可設定を使用してクライアントのアクセスを決定する方法を理解する必要があります。アクセスを確認するために使用する主な手順は、ONTAPリリースに基づいて次のとおりです。

ONTAP 9 .15.1では、OAuth 2.0の重要なアップデートはありませんでした。9.15.1リリースを使用している場合は、ONTAP 9 .14.1の説明を参照してください。

関連情報

- "ONTAPでサポートされるOAuth 2.0機能"

ONTAP 9 .16.1

ONTAP 9 .16.1では、標準のOAuth 2.0のサポートが拡張され、ネイティブのエントラIDグループ用のMicrosoftエントラID固有の拡張機能と外部の役割マッピングが含まれるようになりました。

ONTAP 9のクライアントアクセスを確認します。**16.1**

ステップ**1**：自己完結型スコープ

アクセストークンに自己完結型のスコープが含まれている場合、ONTAPは最初にこれらのスコープを調べます。自己完結型スコープがない場合は、ステップ2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な*allow*または*deny*決定が行われるまで、各スコープを適用します。明示的な決定が行われた場合、処理は終了します。

ONTAPが明示的にアクセスを決定できない場合は、手順2に進みます。

手順**2**：ローカルロールフラグを確認する

ONTAPでは、ブーリアンパラメータが検証され `use-local-roles-if-present`ます。このフラグの値は、ONTAPに定義された認可サーバーごとに個別に設定されます。

- 値がの場合は、 `true`手順3に進みます。
- 値がの場合は `false`、処理が終了し、アクセスが拒否されます。

手順**3**：名前付き**ONTAP REST**ロール

アクセストークンに名前付きRESTロールがOR `scp`フィールドに含まれている場合、または要求として含まれている場合 `scope`、ONTAPはそのロールを使用してアクセスの決定を行います。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

名前付きRESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

手順**4**：ユーザ

アクセストークンからユーザ名を抽出し、アプリケーション「http」にアクセスできるユーザと照合します。ユーザは、認証方式に基づいて次の順序で検証されます。

- パスワード
- ドメイン（Active Directory）
- nsswitch（LDAP）

一致するユーザが見つかった場合、ONTAPはそのユーザに対して定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

ユーザが一致しない場合、またはアクセストークンにユーザ名がない場合は、手順5に進みます。

ステップ**5**：グループ

1つ以上のグループが含まれている場合は、その形式が検証されます。グループがUUIDとして表されている場合は、内部グループ マッピング テーブルが検索されます。一致するグループおよび関連付けられているロールがある場合、ONTAPは、そのグループに定義されたロールを使用してアクセスの可否を判定します。常に*ALLOW*または*DENY*の判定が行われ、処理は終了します。詳細については、"ONTAPでのOAuth 2.0またはSAML IdPグループの使用" 。

グループが名前で表され、ドメインまたはnsswitch許可が設定されている場合、ONTAPはそれらのグループをそれぞれActive DirectoryまたはLDAPグループと照合しようとします。一致するグループがある場合、ONTAPはそのグループに定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

一致するグループがない場合、またはアクセストークンにグループがない場合、アクセスは拒否され、処理は終了します。

ONTAP 9 .14.1

サポートされている初期のOAuth 2.0は、標準のOAuth 2.0機能に基づいて、ONTAP 9 .14.1で導入されました。

ONTAP 9のクライアントアクセスを確認します。**14.1**

ステップ**1**：自己完結型スコープ

アクセストークンに自己完結型のスコープが含まれている場合、ONTAPは最初にこれらのスコープを調べます。自己完結型スコープがない場合は、ステップ2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な*allow*または*deny*決定が行われるまで、各スコープを適用します。明示的な決定が行われた場合、処理は終了します。

ONTAPが明示的にアクセスを決定できない場合は、手順2に進みます。

手順**2**：ローカルロールフラグを確認する

ONTAPでは、ブーリアンパラメータが検証され `use-local-roles-if-present`ます。このフラグの値は、ONTAPに定義された認可サーバーごとに個別に設定されます。

- 値がの場合は、 `true`手順3に進みます。
- 値がの場合は `false`、処理が終了し、アクセスが拒否されます。

手順**3**：名前付き**ONTAP REST**ロール

アクセストークンのフィールドまたは `scp`フィールドに名前付き`REST`ロールが含まれている場合 `scope`、ONTAPはそのロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

名前付きRESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

手順**4**：ユーザ

アクセストークンからユーザ名を抽出し、アプリケーション「http」にアクセスできるユーザと照合します。ユーザは、認証方式に基づいて次の順序で検証されます。

- パスワード
- ドメイン（Active Directory）
- nsswitch（LDAP）

一致するユーザが見つかった場合、ONTAPはそのユーザに対して定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

ユーザが一致しない場合、またはアクセストークンにユーザ名がない場合は、手順5に進みます。

ステップ**5**：グループ

1つ以上のグループが含まれていて、ドメインまたはnsswitch認証が設定されている場合、ONTAPはそれらのグループをそれぞれActive DirectoryまたはLDAPグループと照合しようとします。

一致するグループがある場合、ONTAPはそのグループに定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

一致するグループがない場合、またはアクセストークンにグループがない場合、アクセスは拒否され、処理は終了します。

ONTAPに認可サーバーを定義するときに使用できる設定オプションはいくつかあります。これらのオプションに基づいて、いくつかの展開シナリオのいずれかを使用して、環境に適した承認サーバーを定義できます。

設定パラメータの概要

ONTAPに認可サーバーを定義する際には、いくつかの設定パラメータを使用できます。これらのパラメータは、一般にすべての管理インターフェイスでサポートされています。

> 個 々 のパラメータまたはフィールドに使用される名前は、ONTAP管理インターフェイスによって異なります。管理インターフェイスの違いに対応するために、テーブル内の各パラメータに1つの汎用名が使用されます。特定のインターフェイスで使用される正確な名前は、コンテキストに基づいて明確にする必要があります。

パラメータ	説明
名前	ONTAPで認識されている認可サーバの名前。
アプリケーション	定義が適用されるONTAP内部アプリケーション。これは* http *である必要があります。
発行者URI	トークンを発行するサイトまたは組織を識別するパスを持つFQDN。
プロバイダJWKS URI	ONTAPがアクセストークンの検証に使用するJSON Webキーセットを取得するパスとファイル名を含むFQDN。
JWKS更新間隔	ONTAPがプロバイダーJWKS URIから証明書情報を更新する頻度を決定する時間間隔。値はISO-8601形式で指定します。
イントロスペクションエンドポイント	ONTAPがイントロスペクションを通じてリモートトークン検証を実行するために使用するパスを持つFQDN。
クライアントID	認可サーバで定義されているクライアントの名前。この値が含まれている場合は、インターフェイスに基づいて関連付けられたクライアントシークレットも指定する必要があります。
発信プロキシ	これは、ONTAPがファイアウォールの背後にある場合に、認可サーバへのアクセスを提供するためです。URIはcurl形式で指定する必要があります。
ローカルロールがある場合は使用	ローカルONTAP定義が使用されているかどうかを判断するブーリアンフラグ（名前付きRESTロールとローカルユーザを含む）。
リモートユーザの要求	ONTAPがローカルユーザとの照合に使用する別名。アクセストークンのフィールドを使用して `sub`、ローカルユーザ名を照合します。
対象読者	このフィールドは、アクセストークンを使用できるエンドポイントを定義します。

導入シナリオ

いくつかの一般的な導入シナリオを次に示します。これらは、トークン検証がONTAPによってローカルで実行されるか、認証サーバによってリモートで実行されるかに基づいて編成されます。各シナリオには、必要な設定オプションのリストが含まれています。コンフィギュレーションコマンドの例については、を参照してください"ONTAPでのOAuth 2.0の導入"。

認可サーバを定義したら、ONTAP管理インターフェイスを使用してその設定を表示できます。たとえば、ONTAP CLIでコマンドを使用し `security oauth2 client show`ます。

ローカル検証

次の導入シナリオは、ローカルでトークン検証を実行するONTAPに基づいています。

プロキシなしで自己完結型スコープを使用する

これは、OAuth 2.0の自己完結型スコープのみを使用する最も単純な展開です。ローカルONTAP ID定義は使用されません。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- 発行者URI

また、認可サーバーでスコープを追加する必要があります。

プロキシで自己完結型スコープを使用する

この展開シナリオでは、OAuth 2.0の自己完結型スコープを使用します。ローカルONTAP ID定義は使用されません。ただし、認可サーバはファイアウォールの内側にあるため、プロキシを設定する必要があります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- 発信プロキシ
- 発行者URI
- 対象読者

また、認可サーバーでスコープを追加する必要があります。

ローカルユーザロールとデフォルトユーザ名のマッピングをプロキシで使用する

この導入シナリオでは、ローカルユーザロールとデフォルトのネームマッピングを使用します。リモートユーザ要求では、のデフォルト値が使用される `sub`ため、アクセストークンのこのフィールドはローカルユーザ名の照合に使用されます。ユーザ名は40文字以下にする必要があります。認証サーバはファイアウォールの内側にあるため、プロキシを設定する必要もあります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- 存在する場合はローカルロールを使用(`true`)
- 発信プロキシ
- 発行者

ローカルユーザがONTAPに定義されていることを確認する必要があります。

ローカルユーザロールと代替ユーザ名マッピングをプロキシで使用する

この導入シナリオでは、ローカルユーザロールと代替ユーザ名を使用して、ローカルONTAPユーザを照合します。認証サーバはファイアウォールの背後にあるため、プロキシを設定する必要があります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- 存在する場合はローカルロールを使用(`true`）
- リモートユーザの要求
- 発信プロキシ
- 発行者URI
- 対象読者

ローカルユーザがONTAPに定義されていることを確認する必要があります。

リモートイントロスペクション

次の展開構成は、イントロスペクションを介してリモートでトークン検証を実行するONTAPに基づいています。

プロキシなしで自己完結型スコープを使用する

これは、OAuth 2.0の自己完結型スコープを使用したシンプルな展開です。ONTAP ID定義は使用されません。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- イントロスペクションエンドポイント
- クライアントID
- 発行者URI

認可サーバーでは、スコープ、およびクライアントシークレットを定義する必要があります。

関連情報

- "セキュリティ OAuth2 クライアント 表示"

OAuth 2.0 相互 **TLS** を使用した**ONTAP**クライアント認証

セキュリティのニーズに応じて、オプションでMutual TLS（MTLS）を設定して強力なクライアント認証を実装できます。OAuth 2.0展開の一部としてONTAPで使用される場合、MTLSはアクセストークンが最初に発行されたクライアントによってのみ使用されることを保証します。

OAuth 2.0を使用した相互TLS

Transport Layer Security（TLS）は、2つのアプリケーション（通常はクライアントブラウザとWebサーバ）間にセキュアな通信チャネルを確立するために使用されます。相互TLSは、クライアント証明書を介してクライアントを強力に識別できるようにすることで、これを拡張します。OAuth 2.0を使用したONTAPクラスタで使用する場合、送信者に制約されたアクセストークンを作成して使用することで、基本的なMTLS機能が拡張されます。

送信者に制約されたアクセストークンは、最初に発行されたクライアントのみが使用できます。この機能をサポートするために、新しい確認要求が(`cnf`トークンに挿入されます。このフィールドには、アクセストークンの要求時に使用されるクライアント証明書のダイジェストを保持するプロパティが含まれ`x5t#S256`ます。この値は、トークンの検証の一環としてONTAPによって検証されます。送信者に制約されていない許可サーバーによって発行されたアクセストークンには、追加の確認要求は含まれません。

認可サーバごとにMTLSを個別に使用するようにONTAPを設定する必要があります。たとえば、CLIコマンド`security oauth2 client`には、次の表に示す3つの値に基づいてMTLS処理を制御するパラメータが含まれてい`use-mutual-tls`ます。

> 各構成で、ONTAPによって実行される結果とアクションは、構成パラメータの値、およびアクセストークンとクライアント証明書の内容によって異なります。テーブル内のパラメータは、最小から最も制限の厳しいものに分類されています。

パラメータ	説明
なし	OAuth 2.0相互TLS認証は、認可サーバーでは完全に無効になっています。ONTAPは、確認要求がトークンに含まれている場合やクライアント証明書がTLS接続で提供されている場合でも、MTLSクライアント証明書認証を実行しません。
リクエスト	OAuth 2.0相互TLS認証は、送信者に制約されたアクセストークンがクライアントによって提示された場合に適用されます。つまり、MTLSは、確認要求（with property）がアクセストークンに存在する場合にのみ適用され`x5t#S256`ます。これがデフォルト設定です。
必須	OAuth 2.0相互TLS認証は、認可サーバーによって発行されたすべてのアクセストークンに適用されます。したがって、すべてのアクセストークンは送信者に制約される必要があります。アクセストークンに確認要求がない場合、または無効なクライアント証明書がある場合、認証およびREST API要求は失敗します。

導入フローの概要

ONTAP環境でOAuth 2.0でMTLSを使用する場合の一般的な手順を以下に示します。詳細については、を参照してください "RFC 8705：『OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens』"。

手順1：クライアント証明書を作成してインストールする

クライアントIDの確立は、クライアントの秘密鍵に関する知識の証明に基づいています。対応する公開鍵は、クライアントから提示された署名付きX.509証明書に配置されます。クライアント証明書の作成手順の概要は次のとおりです。

1. 公開鍵と秘密鍵のペアを生成する
2. 証明書署名要求を作成する
3. CSRファイルを既知のCAに送信する

4. CAが要求を検証し、署名済み証明書を発行

通常、クライアント証明書はローカルのオペレーティングシステムにインストールするか、curlなどの一般的なユーティリティを使用して直接使用できます。

ステップ**2**：**MTLS**を使用するように**ONTAP**を設定する

MTLSを使用するようにONTAPを設定する必要があります。この設定は、認可サーバごとに個別に行われます。たとえば、CLIでは、オプションのパラメータを指定してコマンドを `security oauth2 client`使用し `use-mutual-tls`ます。詳細については、を参照してください "ONTAPでのOAuth 2.0の導入" 。

手順**3**：クライアントがアクセストークンを要求する

クライアントは、ONTAPに設定された認証サーバからアクセストークンを要求する必要があります。クライアントアプリケーションは、手順1で作成およびインストールした証明書でMTLSを使用する必要があります。

ステップ**4:**認証サーバーがアクセストークンを生成する

認可サーバはクライアント要求を検証し、アクセストークンを生成します。これの一部として、クライアント証明書のメッセージダイジェストを作成します。このダイジェストは、確認要求(フィールド)としてトークンに含まれ `cnf`ます。

手順**5**：クライアントアプリケーションが**ONTAP**にアクセストークンを提示する

クライアントアプリケーションは、ONTAPクラスタへのREST API呼び出しを実行し、アクセストークンを* bearerトークン*として承認要求ヘッダーに含めます。クライアントは、アクセストークンの要求に使用したのと同じ証明書を持つMTLSを使用する必要があります。

ステップ**6: ONTAP**はクライアントとトークンを検証します。

ONTAPは、HTTP要求でアクセストークンと、MTLS処理の一部として使用されるクライアント証明書を受信します。ONTAPは最初にアクセストークンの署名を検証します。設定に基づいて、ONTAPはクライアント証明書のメッセージダイジェストを生成し、トークン内の確認要求* cnf*と比較します。2つの値が一致する場合、ONTAPは、API要求を行うクライアントがアクセストークンが最初に発行されたクライアントと同じであることを確認しました。

関連情報

- "セキュリティ OAuth2 クライアント"

構成と導入

ONTAPを使用した**OAuth 2.0**の導入準備

ONTAP環境でOAuth 2.0を構成する前に、展開の準備をする必要があります。主なタスクと決定事項の概要を以下に示します。セクションの配置は、通常、従うべき順序に沿って配置されます。ただし、ほとんどの環境に適用できますが、必要に応じて環境に適応する必要があります。また、正式な導入計画の作成も検討する必要があります。

環境に応じて、ONTAPに定義されている認証サーバの設定を選択できます。これには、導入のタイプごとに指定する必要があるパラメータ値も含まれます。詳細については、を参照してください "OAuth 2.0の導入シナリオ" 。

リソースとクライアントアプリケーションを保護

OAuth 2.0は、保護されたリソースへのアクセスを制御するための承認フレームワークです。このため、導入の最初の重要なステップは、使用可能なリソースと、それらにアクセスする必要があるクライアントを特定することです。

クライアントアプリケーションを特定する

REST API呼び出しを発行するときにOAuth 2.0を使用するクライアントと、アクセスが必要なAPIエンドポイントを決定する必要があります。

既存の**ONTAP REST**ロールとローカルユーザの確認

RESTロールやローカルユーザなど、既存のONTAP IDの定義を確認する必要があります。OAuth 2.0の設定方法によっては、これらの定義を使用してアクセスを決定できます。

OAuth 2.0へのグローバルな移行

OAuth 2.0認証を段階的に実装することもできますが、各認証サーバーにグローバルフラグを設定することで、すべてのREST APIクライアントをOAuth 2.0にすぐに移動することもできます。これにより、自己完結型スコープを作成することなく、既存のONTAP構成に基づいてアクセスを決定できます。

認証サーバ

認証サーバーは、アクセストークンを発行し、管理ポリシーを適用することで、OAuth 2.0の展開において重要な役割を果たします。

認可サーバーを選択してインストールします。

1つ以上の認可サーバーを選択してインストールする必要があります。スコープの定義方法など、アイデンティティプロバイダの設定オプションと手順を理解することが重要です。Microsoft Entra IDを含む一部の承認サーバーは、名前ではなくUUIDを使用してグループを表します。

認証ルート**CA**証明書をインストールする必要があるかどうかを判断する

ONTAPでは、認証サーバの証明書を使用して、クライアントから提示された署名済みアクセストークンを検証します。これを行うには、ONTAPにルートCA証明書と中間証明書が必要です。ONTAPがプリインストールされている場合があります。そうでない場合は、インストールする必要があります。

ネットワークの場所と構成の評価

認証サーバがファイアウォールの背後にある場合は、プロキシサーバを使用するようにONTAPを設定する必要があります。

クライアント認証と許可

クライアントの認証と許可には、いくつかの側面を考慮する必要があります。

自己完結型スコープまたはローカル**ONTAP ID**定義

大まかに言えば、認可サーバーで定義された自己完結型スコープを定義することも、役割やユーザーを含む既存のローカルONTAP ID定義に依存することもできます。

ローカル**ONTAP**処理を使用するオプション

ONTAP ID定義を使用する場合は、適用するものを次のように決定する必要があります。

- ネームドRESTロール

- ローカルユーザの一致
- Active DirectoryまたはLDAPグループ

ローカル検証またはリモートイントロスペクション

アクセストークンがONTAPによってローカルで検証されるか、イントロスペクションによって認可サーバーで検証されるかを決定する必要があります。また、更新間隔など、いくつかの関連する値も考慮する必要があります。

送信者に制約されたアクセストークン

高度なセキュリティが必要な環境では、MTLSに基づいて送信制限付きアクセストークンを使用できます。これには、クライアントごとに証明書が必要です。

UUIDおよび**ID**マッピングとしてのグループ

UUIDを使用するグループを表す認証サーバを使用している場合は、これらをグループ名および場合によっては関連するロールにマッピングする方法を計画する必要があります。

管理インターフェイス

OAuth 2.0の管理は、次のいずれかのONTAPインターフェイスを使用して実行できます。

- コマンドラインインターフェイス
- System Manager
- REST API

クライアントニヨルアクセストークンノヨウキュウホウホウ

クライアントアプリケーションは、許可サーバからアクセストークンを直接要求する必要があります。許可の種類を含め、これをどのように行うかを決定する必要があります。

ONTAPの設定

ONTAPのいくつかの設定タスクを実行する必要があります。

RESTロールとローカルユーザを定義する

認証設定に基づいて、ローカルのONTAP識別処理を使用できます。この場合は、RESTロールとユーザ定義を確認して定義する必要があります。また、認証サーバによっては、UUID値に基づいたグループの管理も含まれる場合があります。

コア構成

コアONTAP構成の実行には、主に次の3つの手順が必要です。

- 必要に応じて、認証サーバの証明書に署名したCAのルート証明書（および中間証明書）をインストールします。
- 認可サーバを定義します。
- クラスタに対してOAuth 2.0の処理を有効にします。

ONTAPでの**OAuth 2.0**の導入

OAuth 2.0のコア機能の展開には、主に3つのステップがあります。

開始する前に

ONTAPを設定する前に、OAuth 2.0の展開を準備する必要があります。たとえば、証明書がどのように署名されたか、ファイアウォールの内側にあるかなど、承認サーバーを評価する必要があります。詳細については、を参照してください "ONTAPを使用したOAuth 2.0の導入準備" 。

手順**1**：認可サーバのルート**CA**証明書をインストールする

ONTAPには、多数のルートCA証明書が事前にインストールされています。そのため、多くの場合、認証サーバの証明書は追加の設定なしでONTAPによってすぐに認識されます。ただし、許可サーバ証明書の署名方法によっては、ルートCA証明書と中間証明書のインストールが必要になる場合があります。

必要に応じて、次の手順に従って証明書をインストールします。必要な証明書はすべてクラスタレベルでインストールする必要があります。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。

例 **26.** 手順

System Manager

1. System Managerで、**[**クラスタ**]>***[設定]*を選択します。
2. [セキュリティ]*セクションまで下にスクロールします。
3. の横にある→*をクリックします。
4. タブで[追加]*をクリックします。
5. [インポート]*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて設定パラメータを設定します。
7. [追加]*をクリックします。

CLI

1. インストールを開始します。

   ```
   security certificate install -type server-ca
   ```

2. 次のコンソール メッセージを探します。

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. テキスト エディタで証明書ファイルを開きます。
4. 次の行を含めて、証明書全体をコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. コマンド プロンプトの末尾に証明書を貼り付けます。
6. Enter*キーを押してインストールを完了します。
7. 次のいずれかを使用して証明書がインストールされていることを確認します。

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

手順**2**：認証サーバを設定する

ONTAPに対する認可サーバーを少なくとも1つ定義する必要があります。設定と導入計画に基づいてパラメータ値を選択する必要があります。を参照し"OAuth2導入シナリオ"て、構成に必要な正確なパラメータを特定します。

認可サーバー定義を変更するには、既存の定義を削除して新しい定義を作成します。

次の例は、の最初の単純な導入シナリオに基づいて"ローカル検証"います。自己完結型スコープはプロキシなしで使用されます。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。CLIの手順では、コマンドを実行する前に置き換える必要があるシンボリック変数を使用します。

例 **27.** 手順

System Manager

1. System Managerで、**[**クラスタ**]**>*[設定]*を選択します。
2. [セキュリティ]*セクションまで下にスクロールします。
3. * OAuth 2.0 authorization の横にある+*をクリックします。
4. [その他のオプション]*を選択します。
5. 導入に必要な値を次のように指定します。
   - 名前
   - アプリケーション（http）
   - プロバイダJWKS URI
   - 発行者URI
6. [追加]*をクリックします。

CLI

1. 定義を再作成します。

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

例：

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

の詳細については `security oauth2 client create`、を"ONTAPコマンド リファレンス"参照してください。

手順**3**：**OAuth 2.0**を有効にする

最後のステップは、OAuth 2.0を有効にすることです。これはONTAPクラスタのグローバル設定です。

ONTAP、認可サーバー、およびサポートサービスがすべて正しく設定されていることを確認するまで、OAuth 2.0の処理を有効にしないでください。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。

例 **28.** 手順

System Manager

1. System Managerで、**[**クラスタ**]>***[設定]*を選択します。
2. [セキュリティ]セクション*まで下にスクロールします。
3. * OAuth 2.0 authorization の横にある→*をクリックします。
4. * OAuth 2.0認証*を有効にします。

CLI

1. OAuth 2.0を有効にします。

```
security oauth2 modify -enabled true
```

2. OAuth 2.0が有効になっていることを確認します。

```
security oauth2 show
Is OAuth 2.0 Enabled: true
```

関連情報

- "セキュリティ証明書のインストール"
- "security certificate show"
- "セキュリティ OAuth2 変更"
- "セキュリティ OAuth2 表示"

OAuth 2.0を使用して**ONTAP REST API**呼び出しを発行する

ONTAPのOAuth 2.0実装では、REST APIクライアントアプリケーションがサポートされています。curlを使用して簡単なREST API呼び出しを発行し、OAuth 2.0の使用を開始できます。次の例は、ONTAPクラスタのバージョンを取得します。

開始する前に

ONTAPクラスタに対してOAuth 2.0機能を設定して有効にする必要があります。これには、認可サーバーの定義が含まれます。

ステップ**1**：アクセストークンを取得する

REST API呼び出しで使用するアクセストークンを取得する必要があります。トークン要求はONTAPの外部で実行され、正確な手順は認可サーバとその設定によって異なります。Webブラウザ、curlコマンド、またはプ

ログラミング言語を使用してトークンを要求できます。

説明のために、curlを使用してKeycloakからアクセストークンを要求する方法の例を以下に示します。

キークロークの例

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

返されたトークンをコピーして保存する必要があります。

手順**2**：**REST API**呼び出しを問題する

有効なアクセストークンを取得したら、curlコマンドにアクセストークンを指定してREST API呼び出しを実行できます。

パラメータと変数

curlの例の2つの変数について、次の表で説明します。

変数	説明
$FQDN_IP	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレス。
$access_token	認可サーバーによって発行されたOAuth 2.0アクセストークン。

curlの例を発行する前に、まずBashシェル環境でこれらの変数を設定する必要があります。たとえば、Linux CLIで次のコマンドを入力して、FQDN変数を設定および表示します。

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

両方の変数をローカルのBashシェルで定義したら、curlコマンドをコピーしてCLIに貼り付けることができます。Enter *を押して変数を置き換え、コマンドを問題します。

カールの例

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

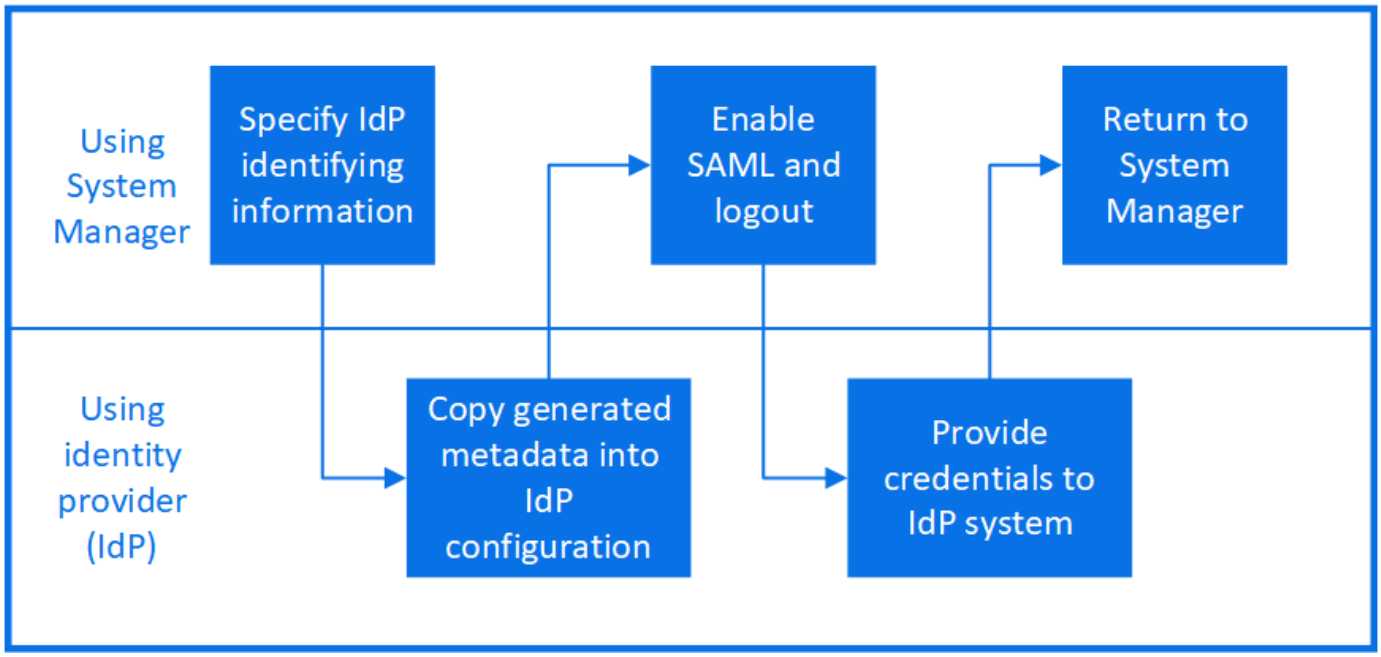
リモートONTAPユーザーの SAML 認証を構成する

ONTAP 9.3以降では、WebサービスにSecurity Assertion Markup Language（SAML）認証を設定できます。SAML認証を設定して有効にすると、Active DirectoryやLDAPなどのディレクトリ サービス プロバイダではなく、外部のアイデンティティ プロバイダ（IdP）によってユーザが認証されます。SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダが認証に使用されます。

SAML認証を有効にする

System ManagerまたはCLIを使用してSAML認証を有効にするには、次の手順を実行します。クラスタでONTAP 9.7以前が実行されている場合は、System Managerで実行する手順が異なります。使用しているシステムで利用可能なSystem Managerのオンライン ヘルプを参照してください。

SAML 認証を有効にすると、SAML 認証用に設定されたリモート ユーザーのみが System Manager GUI にアクセスできるようになります。ローカル ユーザはSystem ManagerのGUIにアクセスできません。



タスクの内容

- SAML認証はONTAPにのみ適用されます `http`そして `ontapi`アプリケーション。

その `http`そして `ontapi`アプリケーションは、サービス プロセッサ インフラストラクチャ、 ONTAP API、および System Manager などの Web サービスによって使用されます。

- SAML認証は、管理SVMへのアクセスでのみ使用できます。
- ONTAP 9.17.1以降では、IdPが提供するグループ情報をONTAPロールにマッピングできるようになりました。これにより、IdPで定義されたグループに基づいてユーザにロールを割り当てることができます。詳細については、以下を参照してください。 "ONTAPでのOAuth 2.0またはSAML IdPグループの使用" 。

次のIdPがSystem Managerで検証されました。

- Microsoft Entra ID（ ONTAP 9.17.1以降で検証済み）
- Active Directoryフェデレーションサービス
- Cisco Duo (次のONTAPバージョンで検証済み)
  - 9.7P21以降の9.7リリース（を参照 "System Managerのクラシックドキュメント"）
  - 9.8P17以降の9.8パッチリリース
  - 9.9.1P13 以降の 9.9.1 パッチリリース
  - 9.10.1P9 以降の 9.10.1 パッチリリース
  - 9.11.1P4 以降の 9.11.1 パッチリリース
  - 9.12.1以降のリリース
- Shibboleth

開始する前に

- リモート認証に使用するIdPは、以下のものでなければなりません構成された。IdPのURIが必要です。ONTAP が認証要求を送信し、応答を受信する Web アドレスです。
- ONTAPクラスタと IdP の間でポート 443 が開いている必要があります。
- ONTAPクラスタとIdPは、互いの完全修飾ドメイン名にpingを実行できる必要があります。DNSが正しく設定され、クラスタ証明書の有効期限が切れていないことを確認してください。
- て、IdPの信頼できる認証局（CA）をONTAPに追加します。あなたは "System ManagerでONTAP証明書を管理する"。IdP でONTAPクラスタ証明書を設定する必要がある場合があります
- ONTAPクラスタの"サービス プロセッサ（SP）"コンソール。SAMLが正しく構成されていない場合は、SPコンソールから無効にする必要があります。
- Entra ID（ ONTAP 9.17.1以降で検証済み）をご利用の場合は、 ONTAP SAML設定を作成する前に、ONTAPメタデータでEntra IDを設定する必要があります。EntraIDは、 ONTAPメタデータが設定されるまでIdP URIを提供しません。ONTAPONTAP設定を作成するには、IdP URIが必要です。
  - System Managerを使用してSAMLを設定する場合は、System ManagerからONTAPメタデータが提供されるまで、IdP URIフィールドを空白のままにしておきます。ONTAPONTAPデータを使用してEntra IDを設定し、SAML設定を有効にする前にIdP URIをSystem Managerにコピーしてください。
  - ONTAP CLIを使用してSAMLを設定する場合は、 ONTAP SAML設定を有効にする前にONTAPメタデータを生成する必要があります。ONTAPONTAPデータファイルは、以下のコマンドで生成できます。

```
security saml-sp default-metadata create -sp-host <ontap_host_name>
```

`ontap_host_name` SAMLサービスプロバイダホスト（この場合はONTAPシステム）のホスト名またはIPアドレスです。デフォルトでは、クラスタ管理IPアドレスが使用されます。必要に応じて、ONTAPサーバ証明書の情報を指定できます。デフォルトでは、ONTAP Webサーバ証明書の情報が使用されます。

提供されたメタデータを使用してEntra IDを設定します。ONTAPONTAP設定を作成する前に、Entra IDを設定する必要があります。Entraの設定が完了したら、以下のCLI手順に進みます。

- クラスタ内のすべてのノードがバージョン 9.17.1 になるまで、Entra ID のONTAPメタデータを生成することはできません。

手順

環境に応じて、次の手順を実行します。

System Manager

1. [クラスタ]>[設定]*をクリックします。
2. [SAML認証]*の横にあるをクリックします ⚙。
3. SAML 認証を有効にする * チェックボックスがオンになっていることを確認します。
4. IdP URIのURLを入力します（ "https://" ）。EntraID を使用している場合は、この手順をスキップしてください。
5. 必要に応じて、ホスト システムのアドレスを変更します。これは、認証後にIdPが接続するアドレスです。デフォルトはクラスタ管理IPアドレスです。
6. 正しい証明書が使用されていることを確認します。
   - システムに「サーバ」タイプの証明書が1つだけ適用されている場合、その証明書はデフォルトとみなされ、画面には表示されません。
   - システムに「サーバ」タイプの証明書が複数適用されている場合は、そのうちの1つが表示されます。別の証明書を選択するには、 * Change * をクリックします。
7. [保存（ Save ）] をクリックします。確認ウィンドウにメタデータ情報が表示され、クリップボードに自動的にコピーされます。
8. 指定したIdPシステムに移動し、クリップボードからメタデータをコピーしてシステムのメタデータを更新します。Entra ID を使用している場合は、システム メタデータを使用して Entra ID を設定した後、IdP URI をONTAPにコピーします。
9. 確認ウィンドウ（ System Manager ）に戻り、チェックボックスをオンにします。 * ホスト URI またはメタデータで IdP を設定しました。 *
10. Logout * をクリックして、 SAML ベースの認証を有効にします。IdPシステムに認証画面が表示されます。
11. IdP サインオン ページで、SAML ベースの資格情報を入力します。クレデンシャルが確認されると、System Managerのホーム ページが表示されます。

CLI

1. SAML設定を作成して、ONTAPからIdPメタデータにアクセスできるようにします。

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   `idp_uri`は、IdPメタデータのダウンロード元のIdPホストのFTPアドレスまたはHTTPアドレスです。

   > ⓘ 一部のURLには疑問符（？）が含まれています。疑問符はONTAPコマンドラインのアクティブヘルプを起動します。クエスチョンマーク付きのURLを入力するには、まず、以下のコマンドでアクティブ・ヘルプを無効にする必要がある `set -active -help false`。アクティブ・ヘルプは、後でコマンド `set -active-help true` 。"ONTAPコマンド リファレンス" 。

   `ontap_host_name`は、SAMLサービスプロバイダホスト（ここではONTAPシステム）のホスト名またはIPアドレスです。デフォルトでは、クラスタ管理LIFのIPアドレスが使用されます。

   必要に応じて、ONTAPサーバ証明書の情報を指定できます。デフォルトでは、ONTAP Webサーバ証明書情報が使用されます。

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

ONTAPホストメタデータにアクセスするためのURLが表示されます。

2. IdPホストから、 IdPを設定する ONTAPホストメタデータを使用します。EntraIDを使用している場合は、この手順はすでに完了しています。
3. IdP が設定されたら、SAML 設定を有効にします。

   ```
   security saml-sp modify -is-enabled true
   ```

   または `ontapi`アプリケーションにアクセスする既存のユーザには `http`、SAML認証が自動的に設定されます。

4. ユーザーを作成したい場合は、 `http`または `ontapi` SAMLの設定後にアプリケーションにログインする場合は、新規ユーザーの認証方法としてSAMLを指定します。ONTAP9.17.1より前のバージョンでは、既存のユーザーに対してSAMLログインが自動的に作成されます。 `http`または `ontapi` SAMLが有効な場合、新しいユーザーはSAML用に設定される必要があります。ONTAP9.17.1以降、SAMLで作成されONTAPすべてのユーザーは `password` 、 `domain` 、 または `nsswitch` SAMLが有効になっている場合、認証方法は IdP に対して自動的に認証されます。

   a. を使用した新規ユーザー用のログイン方法を作成します。 `user_name` IdP で設定されたユーザー名と一致する必要があります。

      ⓘ `user_name`値では大文字と小文字が区別されます。ユーザ名だけを含め、ドメインの一部は含めないでください。

      ```
      security login create -user-or-group-name <user_name> -application [http
      | ontapi] -authentication-method saml -vserver <svm_name>
      ```

      例：

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver cluster_12
      ```

b. ユーザエントリが作成されたことを確認します。

```
security login show
```

例：

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
--------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
admin1          http        saml          backup           -
none
```

+
の詳細については `security login show`、を"ONTAPコマンド リファレンス"参照してください。

SAML認証の無効化

外部IDプロバイダー（IdP）によるリモートSystem Managerユーザーの認証を停止したい場合は、SAML認証を無効にすることができます。SAML認証を無効にすると、ローカルユーザー認証、またはActive DirectoryやLDAPなどの設定済みディレクトリサービスプロバイダーがユーザー認証に使用されます。

環境に応じて、次の手順を実行します。

例 **29.** 手順

System Manager

1. [クラスタ]>[設定]*をクリックします。
2. [* SAML Authentication* （ SAML 認証）] で、 [* Enabled *（有効 * ）] トグルボタンをクリックします。
3. オプション：**[SAML**認証**]***の横にあるをクリックし、[SAML認証を有効にする]*チェックボックスをオフにすることもできます 。

CLI

1. SAML認証を無効にします。

```
security saml-sp modify -is-enabled false
```

2. SAML認証を使用する必要がなくなった場合やIdPを変更する場合は、SAMLの設定を削除します。

```
security saml-sp delete
```

サードパーティの**IdP**を構成する

タスクの内容

ONTAPで認証するには、IdP の設定を変更する必要がある場合があります。以下のセクションでは、サポートされている IdP の設定情報について説明します。

エントラ**ID**

Entra IDを設定する際は、新しいアプリケーションを作成し、 ONTAPが提供するメタデータを使用してSAMLサインオンを設定します。アプリケーションの作成後、アプリケーションのSAML設定の「属性とクレーム」セクションを以下の内容に合わせて編集します。

設定	値
名前	urn:oid:0.9.2342.19200300.100.1.1
ネームスペース	空白のまま
名前の形式	URI
ソース	属性
ソース属性	ユーザー.ユーザープリンシパル名

Entra ID でグループを使用する場合は、次の設定でグループ要求を追加します。

設定	値
名前	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
ネームスペース	空白のまま
ソース属性	グループID

Entra IDはUUID形式でグループ情報を提供します。EntraIDでグループを使用する方法の詳細については、以下を参照してください。 "UUIDを使用したグループの管理" 。

アプリケーション SAML 設定の「SAML 証明書」セクションで提供される *App Federation Metadata URL* は、 ONTAPに入力する IdP URI です。

Entra ID多要素認証の設定方法については、以下を参照してください。 "Microsoft Entra 多要素認証の展開を計画する" 。

詳細については、 "Entra ID文書" 。

Active Directoryフェデレーションサービス

Active Directory Federation Services（AD FS）を設定する際には、 ONTAPが提供するサービスプロバイダメタデータを使用して、新しいクレーム対応証明書利用者信頼を追加する必要があります。証明書利用者信頼を作成したら、「LDAP属性をクレームとして送信」テンプレートを使用して、証明書利用者信頼のクレーム発行ポリシーに以下のクレームルールを追加します。

属性ストア	**LDAP**属性	送信クレームタイプ
Active Directory	SAM-account-name	Name ID
Active Directory	SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Active Directory	名前の形式	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory	トークングループ - ドメイン名で修飾	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAMAccountName	urn:oid:1.2.840.113556.1.4.221

AD FSはグループ情報を名前形式で提供します。ADFSでのグループの使用の詳細については、以下を参照してください。 "名前付きのグループを管理します。" 。

詳細については、 "AD FS ドキュメント" 。

Cisco Duo

参照"Cisco Duoマニュアル"構成情報については。

Shibboleth

Shibboleth IdP を構成する前に、LDAP サーバーを構成する必要があります。

ONTAPでSAMLを有効にする場合は、提供されたホストメタデータXMLを保存します。Shibbolethがインストールされているホストで、 `metadata/sp-metadata.xml` Shibboleth IdP ホーム ディレクトリ内のホスト メタデータ XML を使用します。

詳細については、 "Shibboleth" 。

SAMLの設定に関する問題のトラブルシューティング

Security Assertion Markup Language（SAML）認証の設定に失敗した場合は、SAMLの設定に失敗した各ノードを手動で修復して、障害からリカバリできます。修復プロセス中にWebサーバが再起動され、アクティブなHTTP接続またはHTTPS接続が中断されます。

タスクの内容

SAML認証を設定すると、ONTAPはSAMLの設定をノード単位で適用します。SAML認証を有効にすると、設定に問題がある場合、ONTAPは自動的に各ノードを修復しようとします。いずれかのノードでSAMLの設定に問題がある場合は、SAML認証を無効にしてから再度有効にすることができます。SAML認証を再度有効にしたあとも、1つ以上のノードにSAMLの設定を適用できない場合があります。SAMLの設定に失敗したノードを特定し、そのノードを手動で修復できます。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. SAMLの設定に失敗したノードを特定します。

   ```
   security saml-sp status show -instance
   ```

   例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

の詳細については `security saml-sp status show`、を"ONTAPコマンド リファレンス"参照してください。

3. 障害が発生したノードでSAMLの設定を修復します。

   `security saml-sp repair -node <node_name>`

   例：

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Webサーバが再起動され、アクティブなHTTP接続またはHTTPS接続が中断されます。

   の詳細については `security saml-sp repair`、を"ONTAPコマンド リファレンス"参照してください。

4. すべてのノードでSAMLが正しく設定されていることを確認します。

   `security saml-sp status show -instance`

例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                  Update Status: config-success
                 Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                  Update Status: config-success
                 Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

の詳細については `security saml-sp status show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "ONTAPコマンド リファレンス"
- "セキュリティSAML - SP"
- "security login create"

ONTAPでのOAuth 2.0またはSAML IdPグループの使用

ONTAP には、OAuth 2.0 認証サーバーまたは SAML ID プロバイダー (IdP) に基づいてグループを構成するためのいくつかのオプションが用意されています。グループを、ONTAPがアクセス制御に使用するロールにマッピングできます。

ONTAP 9.17.1以降では、SAML IdPが提供するグループ情報をONTAPロールにマッピングできるようになりました。これにより、IdPで定義されたグループに基づいてユーザーにロールを割り当てることができます。詳しくは"SAML認証の設定"。ONTAP 9.14.1以降、 ONTAPはOAuth 2.0のグループ名認証をサポートします。ONTAP9.16.1以降、 ONTAPはONTAP 2.0のグループUUID認証とロールマッピングをサポートします。"ONTAP OAuth 2.0実装の概要" 。

グループの識別方法

認可サーバまたはSAML IdPでグループを設定すると、名前またはUUIDを使用してOAuth 2.0アクセストークンまたはSAMLアサーションでグループが識別され、送信されます。ONTAPを設定する前に、認可サーバまた

はSAML IdPがグループをどのように処理するかを把握しておく必要があります。

アクセストークンに複数のグループが含まれている場合、ONTAPは一致するまで各グループを使用しようとします。

グループ名

Active Directory Federation Service（ADFS）などの多くの認可サーバーやSAML IdPは、グループを名前で識別・表現します。は、ADFSによって生成された、複数のグループを含むJSON OAuth 2.0アクセストークンの一部です。[名前付きのグループを管理します。]詳細についてはこちらをご覧ください。

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

グループ**UUID**

Microsoft Entra IDのような一部の認可サーバーとSAML IdPは、UUIDを使用してグループを識別・表現します。は、Entra IDによって生成された、複数のグループを含むOAuth 2.0アクセストークンの一部です。UUIDを使用したグループの管理詳細についてはこちらをご覧ください。

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

名前付きのグループを管理します。

認証サーバーまたは SAML IdP が名前を使用してグループを識別する場合は、各グループがONTAPクラスターに対して定義されていることを確認する必要があります。セキュリティ環境によっては、グループがすでに定義されている場合があります。

ONTAPグループを定義するCLIコマンドの例を以下に示します。サンプルアクセストークンから取得した名前付きグループを使用していることに注意してください。このコマンドを実行するには、 ONTAPの*admin*権限レベルが必要です。

例

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

使用 `-authentication-method domain`または `nsswitch` SAML IdP および OAuth 2.0 認証サーバーグループ用。

この機能は、ONTAP REST APIを使用して設定することもできます。詳細はこちら "ONTAP自動化に関するドキュメント" 。

UUIDを使用したグループの管理

認可サーバまたはSAML IdPがUUID値を使用してグループを表す場合、グループを使用する前に2段階の設定を行う必要があります。ONTAP9.16.1以降では、 2つのマッピング機能が利用可能になり、Entra IDでテストされています。OAuth2.0用のEntra IDはONTAP 9.16.1以降、SAML用のEntra IDはONTAP 9.17.1以降でサポートされています。CLIコマンドを実行するには、 ONTAPの*admin*権限レベルが必要です。

これらの機能は、ONTAP REST APIを使用して設定することもできます。詳細については、を"ONTAP自動化に関するドキュメント"参照してください。

グループ**UUID**をグループ名にマッピングする

UUID 値を使用してグループを表す認証サーバーまたは SAML IdP を使用している場合は、グループ UUID をグループ名にマッピングする必要があります。以下では、主なONTAP CLI処理について説明します。

作成

新しいグループマッピング設定を定義するには、 `security login group create`コマンド。グループのUUIDと名前は、認可サーバーまたはSAML IdPの設定と一致する必要があります。詳細については、 `security login group create`の中で"ONTAPコマンド リファレンス" 。

パラメータ

グループマッピングの作成に使用するパラメータを次に示します。

パラメータ	説明
`vserver`	必要に応じて、グループを関連付けるSVM（SVM）の名前を指定します。省略すると、グループはONTAPクラスタに関連付けられます。
`name`	ONTAPが使用するグループの一意の名前。
`type`	この値は、グループの発信元のアイデンティティプロバイダを示します。
`uuid`	認可サーバーまたは SAML IdP によって提供されるグループのユニバーサル一意識別子を指定します。

ONTAPのグループを定義する CLI コマンドの例を以下に示します。サンプルアクセストークンの UUID グループを使用していることに注意してください。

例

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

グループを作成すると、グループに対して一意の読み取り専用整数識別子が生成されます。

その他のCLI処理

このコマンドでは、次のような追加の処理がサポートされます。

- - 表示
- 変更
- 削除

オプションを使用すると、グループに対して生成された一意のグループIDを取得できます `show`。の詳細については `show`、を"ONTAPコマンド リファレンス"参照してください。

グループUUIDをロールにマッピングする

UUID値を使用してグループを表す認可サーバまたはSAML IdPを使用している場合は、グループをロールにマッピングできます。ONTAPONTAP役割ベースのアクセス制御の詳細については、以下を参照してください"ONTAPアクセス制御ロールの管理について"。 以下では、主なONTAP CLI処理について説明します。コマンドを発行するには、 ONTAP **admin** 権限レベルである必要があります

> まず最初にグループUUIDをグループ名にマッピングするグループに対して生成された一意の整数 ID を取得します。グループをロールにマッピングするには、IDが必要です。

作成

新しいロールマッピングを定義するには、 `security login group role-mapping create`コマンド。詳細はこちら `security login group role-mapping create`の中で"ONTAPコマンド リファレンス" 。

パラメータ

グループをロールにマッピングするために使用されるパラメータを次に示します。

パラメータ	説明
`group-id`	コマンドを使用して、グループに対して生成される一意のIDを指定します `security login group create`。
`role`	グループのマッピング先のONTAPロールの名前。

例

```
security login group role-mapping create -group-id 1 -role admin
```

その他のCLI処理

このコマンドでは、次のような追加の処理がサポートされます。

- - 表示
- 変更
- 削除

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

関連情報

- "外部ロールのマッピング"

WebAuthn MFAを使用した認証と許可

ONTAP System Managerユーザー向けのWebAuthn多要素認証について学ぶ

ONTAP 9 .16.1以降では、管理者がにログインするユーザに対してWebAuthn多要素認証（MFA）を有効にすることができます。これにより、2つ目の認証形式としてFIDO2キー（YubiKeyなど）を使用したSystem Managerログインが有効になります。デフォルトでは、新規および既存のONTAPユーザに対してWebAuthn MFAは無効になっています。

WebAuthn MFAは、最初の認証方式に次のタイプの認証を使用するユーザおよびグループでサポートされます。

- ユーザ：パスワード、ドメイン、またはnsswitch
- グループ:ドメインまたはnsswitch

ユーザの2つ目の認証方式としてWebAuthn MFAを有効にすると、System Managerにログインしたときにハードウェア認証サーバを登録するように求められます。登録後、秘密鍵はオーセンティケータに格納され、公開鍵はONTAPに格納されます。

ONTAPは、ユーザごとに1つのWebAuthnクレデンシャルをサポートします。ユーザがオーセンティケータを失い、オーセンティケータを交換する必要がある場合、ONTAP管理者はそのユーザのWebAuthnクレデンシャルを削除して、ユーザが次回のログイン時に新しいオーセンティケータを登録できるようにする必要があります。

> 2つ目の認証方式としてWebAuthn MFAを有効にしているユーザは"https://myontap.example.com"、IPアドレス（など"https://192.168.100.200"）ではなくFQDN（など）を使用してSystem Managerにアクセスする必要があります。WebAuthn MFAが有効なユーザの場合、IPアドレスを使用してSystem Managerにログインしようとすると拒否されます。

ONTAP System Managerのユーザまたはグループに対して**WebAuthn MFA**を有効にする

ONTAP管理者は、[WebAuthn MFA]オプションを有効にして新しいユーザまたはグループを追加するか、既存のユーザまたはグループに対してオプションを有効にすることで、System Managerのユーザまたはグループに対してWebAuthn MFAを有効にできます。

> ユーザまたはグループの2番目の認証方式としてWebAuthn MFAを有効にすると、System Managerに次回ログインしたときに、ユーザ（またはそのグループ内のすべてのユーザ）にハードウェアFIDO2デバイスの登録が求められます。この登録はユーザーのローカルオペレーティングシステムによって処理され、通常はセキュリティキーの挿入、パスキーの作成、セキュリティキーのタッチ（サポートされている場合）で構成されます。

新しいユーザまたはグループの作成時に**WebAuthn MFA**を有効にする

System ManagerまたはONTAP CLIを使用して、WebAuthn MFAを有効にして新しいユーザまたはグループを作成できます。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. [Users]*で[Add]*を選択します。
4. ユーザまたはグループの名前を指定し、* Role *のドロップダウンメニューでロールを選択します。
5. ユーザまたはグループのログイン方法とパスワードを指定します。

   WebAuthn MFAは、ユーザに対しては「password」、「domain」、または「nsswitch」、グループに対しては「domain」または「nsswitch」のログイン方法をサポートしています。
6. [MFA for HTTP]列で、*[Enabled]*を選択します。
7. [保存（ Save ）] を選択します。

CLI

1. WebAuthn MFAを有効にして新しいユーザまたはグループを作成します。

   次の例では、2番目の認証方式として「publickey」を選択してWebAuthn MFAを有効にしています。

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

既存のユーザまたはグループに対して**WebAuthn MFA**を有効にする

既存のユーザまたはグループに対してWebAuthn MFAを有効にすることができます。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループのオプションメニューを選択します。

   WebAuthn MFAは、ユーザに対しては「password」、「domain」、または「nsswitch」、グループに対しては「domain」または「nsswitch」のログイン方法をサポートしています。
4. そのユーザの* MFA for HTTP 列で Enabled *を選択します。
5. [保存（ Save ）] を選択します。

CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループに対してWebAuthn MFAを有効にします。

   次の例では、2番目の認証方式として「publickey」を選択してWebAuthn MFAを有効にしています。

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

   の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP System ManagerユーザのWebAuthn MFAを無効にする

ONTAP管理者は、System ManagerまたはONTAP CLIでユーザまたはグループを編集することで、ユーザまたはグループのWebAuthn MFAを無効にできます。

既存のユーザまたはグループに対して**WebAuthn MFA**を無効にする

既存のユーザまたはグループのWebAuthn MFAはいつでも無効にできます。

> ⓘ 登録済みクレデンシャルを無効にしても、クレデンシャルは保持されます。今後クレデンシャルを再度有効にすると、同じクレデンシャルが使用されるため、ユーザがログイン時に再登録する必要はありません。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループを選択します。
4. そのユーザの* MFA for HTTP 列で Disabled *を選択します。
5. [保存（ Save ）] を選択します。

CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループのWebAuthn MFAを無効にします。

   次の例では、2番目の認証方式として「none」を選択してWebAuthn MFAを無効にしています。

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

   の詳細については `security login modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP WebAuthn MFA設定の表示とクレデンシャルの管理

ONTAP管理者は、クラスタ全体のWebAuthn MFA設定を表示し、WebAuthn MFAのユーザおよびグループのクレデンシャルを管理できます。

WebAuthn MFAのクラスタ設定を表示します。

ONTAP CLIを使用して、WebAuthn MFAのクラスタ設定を表示できます。

手順

1. WebAuthn MFAのクラスタ設定を表示します。必要に応じて、引数を使用してStorage VMを指定できます `vserver`。

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   の詳細については `security webauthn show`、を"ONTAPコマンド リファレンス"参照してください。

サポートされている公開鍵**WebAuthn MFA**アルゴリズムの表示

Storage VMまたはクラスタのWebAuthn MFAでサポートされている公開鍵アルゴリズムを表示できます。

手順

1. サポートされている公開鍵WebAuthn MFAアルゴリズムを列挙します。必要に応じて、引数を使用してStorage VMを指定できます `vserver`。

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

の詳細については `security webauthn supported-algorithms show`、を"ONTAPコマンド リファレンス"参照してください。

登録済み**WebAuthn MFA**クレデンシャルの表示

ONTAP管理者は、すべてのユーザの登録済みWebAuthnクレデンシャルを表示できます。この手順を使用する管理者以外のユーザは、自分の登録済みWebAuthnクレデンシャルのみを表示できます。

手順

1. 登録されたWebAuthn MFAクレデンシャルを表示します。

```
security webauthn credentials show
```

の詳細については `security webauthn credentials show`、を"ONTAPコマンド リファレンス"参照してください。

登録済み**WebAuthn MFA**クレデンシャルの削除

登録済みのWebAuthn MFAクレデンシャルを削除できます。これは、ユーザーのハードウェアキーが紛失したり、盗まれたり、使用されなくなったりした場合に便利です。ユーザーが元のハードウェアオーセンティケータを持っていて、新しいものに置き換えたい場合は、登録されたクレデンシャルを削除することもできます。クレデンシャルを削除すると、ユーザは交換用オーセンティケータを登録するように求められます。

ユーザの登録済みクレデンシャルを削除しても、そのユーザのWebAuthn MFAは無効になりません。ユーザがハードウェアオーセンティケータを紛失し、交換する前にログインする必要がある場合は、次の手順とユーザの手順を使用してクレデンシャルを削除する"WebAuthn MFAを無効にする"必要があります。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、クレデンシャルを削除するユーザまたはグループのオプションメニューを選択します。
4. [HTTPクレデンシャルのMFAを削除する]*を選択します。
5. 「 * 削除」を選択します。

CLI

1. 登録済みクレデンシャルを削除します。次の点に注意してください。
   - 必要に応じて、ユーザのStorage VMを指定できます。省略すると、クラスタレベルでクレデンシャルが削除されます。
   - 必要に応じて、クレデンシャルを削除するユーザのユーザ名を指定できます。省略すると、現在のユーザのクレデンシャルが削除されます。

   ```
   security webauthn credentials delete -vserver <storage_vm_name>
   -username <username>
   ```

   の詳細については `security webauthn credentials delete`、を"ONTAPコマンド リファレンス"参照してください。

Webサービスを管理します。

Webサービスの管理の概要

クラスタまたは Storage Virtual Machine （ SVM ）の Web サービスを有効または無効にしたり、 Web サービスの設定を表示したり、ロールのユーザが Web サービスにアクセスできるかどうかを管理したりできます。

クラスタまたはSVMのWebサービスは次の方法で管理できます。

- 特定のWebサービスの有効化と無効化
- Webサービスへのアクセスを暗号化されたHTTP（SSL）のみに制限するかどうかの指定
- Webサービスの可用性の表示
- あるロールのユーザに対するWebサービスへのアクセスの許可と禁止
- Webサービスへのアクセスが許可されているロールを表示する

ユーザがWebサービスにアクセスするには、次の条件がすべて満たされている必要があります。

- ユーザが認証されている必要があります。

たとえば、Webサービスからユーザ名とパスワードの入力を求められる場合があります。ユーザーの応答は有効なアカウントと一致する必要があります。

- ユーザに正しいアクセス方法が設定されていること。

  認証が成功するのは、指定されたWebサービスに対する正しいアクセス方法を持つユーザだけです。ONTAP API Webサービス `ontapi`の場合）、ユーザにアクセス方法が必要です `ontapi`。それ以外のすべてのWebサービスでは、ユーザにアクセス方法が設定されている必要があります `http`。

  ユーザのアクセス方法と認証方法を管理するには、コマンドを使用し `security login`ます。

- ユーザのアクセス制御ロールを許可するようにWebサービスが設定されている必要があります。

  ロールのWebサービスへのアクセスを制御するには、コマンドを使用し `vserver services web access`ます。

ファイアウォールが有効になっている場合は、Webサービスに使用するLIFのファイアウォールポリシーを設定して、HTTPまたはHTTPSを許可する必要があります。

Web サービスアクセスに HTTPS を使用する場合は、 Web サービスを提供するクラスタまたは SVM の SSL を有効にし、そのクラスタまたは SVM のデジタル証明書を提供する必要もあります。

ONTAP Webサービスへのアクセスを管理する

Webサービスは、ユーザがHTTPまたはHTTPSを使用してアクセスできるアプリケーションです。クラスタ管理者は、Webプロトコルエンジンをセットアップし、SSLを設定し、Webサービスを有効にし、ロールのユーザがWebサービスにアクセスできるようにすることができます。

ONTAP 9 .6以降では、次のWebサービスがサポートされます。

- サービスプロセッサインフラ(`spi`）

  このサービスにより、ノードのログファイル、コアダンプファイル、およびMIBファイルに、クラスタ管理LIFまたはノード管理LIFからHTTPまたはHTTPSでアクセスできるようになります。デフォルト設定はです `enabled`。

  ノードのログファイルまたはコアダンプファイルへのアクセス要求があると、 `spi` Web サービスは、ファイルが存在する別のノードのルート ボリュームへのマウント ポイントをノードから自動的に作成します。マウント ポイントを手動で作成する必要はありません。

- ONTAP (`ontapi`API）

  このサービスでは、ONTAP APIを実行して、リモートプログラムで管理機能を実行できます。デフォルト設定はです `enabled`。

  一部の外部管理ツールでは、このサービスが必要になる場合があります。たとえば、System Managerを使用する場合は、このサービスを有効なままにしておく必要があります。

- Data ONTAP検出(`disco`）

このサービスを使用すると、外部管理アプリケーションがネットワーク内のクラスタを検出できるようになります。デフォルト設定はです `enabled`。

- サポート診断(`supdiag`)

  このサービスは、問題の分析と解決を支援するために、システム上の特権環境へのアクセスを制御します。デフォルト設定はです `disabled`。このサービスは、テクニカルサポートから指示があった場合にのみ有効にしてください。

- System (`sysmgr`Manager)

  このサービスは、ONTAPに含まれるSystem Managerの可用性を管理します。デフォルト設定はです `enabled`。このサービスはクラスタでのみサポートされます。

- ファームウェアベースボード管理コントローラ（BMC）のアップデート(`FW_BMC`

  このサービスでは、BMCファームウェアファイルをダウンロードできます。デフォルト設定はです `enabled`。

- ONTAPのマニュアル(`docs`を参照)

  このサービスでは、ONTAPのドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ONTAP RESTful API(`docs_api`)

  このサービスでは、ONTAP RESTful APIのドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ファイルのアップロードとダウンロード(`fud`)

  このサービスは、ファイルのアップロードとダウンロードを提供します。デフォルト設定はです `enabled`。

- ONTAPメッセージング(`ontapmsg`)

  このサービスは、イベントをサブスクライブできるパブリッシュおよびサブスクライブインターフェイスをサポートしています。デフォルト設定はです `enabled`。

- ONTAPポータル(`portal`)

  このサービスは、ゲートウェイを仮想サーバに実装します。デフォルト設定はです `enabled`。

- ONTAP RESTfulインターフェイス(`rest`)

  このサービスは、RESTfulインターフェイスをサポートしています。このインターフェイスを使用して、クラスタインフラのすべての要素をリモートで管理できます。デフォルト設定はです `enabled`。

- Security Assertion Markup Language（SAML）サービスプロバイダのサポート(`saml`)

  このサービスは、SAMLサービスプロバイダをサポートするためのリソースを提供します。デフォルト設定はです `enabled`。

- SAMLサービスプロバイダ(saml-sp)

  このサービスは、SPメタデータやアサーションコンシューマサービスなどのサービスをサービスプロバイダに提供します。デフォルト設定はです enabled。

ONTAP 9 .7以降では、次の追加サービスがサポートされます。

- 構成バックアップファイル(backups)

  このサービスでは、構成バックアップファイルをダウンロードできます。デフォルト設定はです enabled。

- ONTAPセキュリティ(security)

  このサービスは、認証を強化するためのCSRFトークン管理をサポートします。デフォルト設定はです enabled。

ONTAPでWebプロトコルエンジンを管理します。

クラスタ上でWebプロトコルエンジンを設定して、Webアクセスを許可するかどうか、およびどのSSLバージョンを使用できるかを制御できます。Webプロトコルエンジンの設定を表示することもできます。

Webプロトコルエンジンは、次の方法でクラスタレベルで管理できます。

- コマンドでパラメータを指定する -external`と、リモートクライアントがHTTPまたはHTTPSを使用してWebサービスコンテンツにアクセスできるかどうかを指定できます `system services web modify。
- コマンドでパラメータを指定する -supported-protocol`と、セキュアなWebアクセスにSSLv3を使用するかどうかを指定できます `security config modify。デフォルトでは、SSLv3は無効になっています。Transport Layer Security 1.0（TLSv1.0）が有効になっており、必要に応じて無効にすることができます。

  の詳細については security config modify、を"ONTAPコマンド リファレンス"参照してください。

- クラスタ全体のコントロールプレーンWebサービスインターフェイスに対して、Federal Information Processing Standard（FIPS）140-2準拠モードを有効にすることができます。

  デフォルトでは、FIPS 140-2準拠モードは無効になっています。

  - * FIPS 140-2準拠モードが無効になっている場合*コマンドの security config modify`パラメータをに `true`設定し、コマンドを使用して `security config show`オンラインステータスを確認することで、FIPS 140-2準拠モードを有効にできます `is-fips-enabled。
  - * FIPS 140-2 準拠モードが有効な場合 *
    - ONTAP 9.11.1以降では、TLSv1、TLSv1.1、およびSSLv3は無効になり、TSLv1.2とTSLv1.3のみが引き続き有効になります。ONTAP 9の内部および外部にある他のシステムおよび通信に影響します。FIPS 140-2準拠モードを有効にしたあとに無効にした場合、TLSv1、TLSv1.1、およびSSLv3は無効なままになります。以前の設定に応じて、TLSv1.2またはTLSv1.3のいずれかが有

効なままになります。

- 9.11.1より前のバージョンのONTAP では、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAPでは、FIPS 140-2準拠モードが有効な場合、TLSv1とSSLv3の両方を有効にすることはできません。FIPS 140-2準拠モードを有効にしたあとに無効にした場合、TLSv1とSSLv3は無効なままですが、以前の設定に応じてTLSv1.2またはTLSv1.1とTLSv1.2の両方が有効になります。

- コマンドを使用すると、クラスタ全体のセキュリティの設定を表示できます `system security config show`。

  の詳細については `security config show`、を"ONTAPコマンド リファレンス"参照してください。

ファイアウォールが有効になっている場合は、Webサービスに使用する論理インターフェイス（LIF）のファイアウォールポリシーを設定して、HTTPまたはHTTPSアクセスを許可する必要があります。

WebサービスアクセスにHTTPSを使用する場合は、Webサービスを提供するクラスタまたはStorage Virtual Machine（SVM）のSSLを有効にし、そのクラスタまたはSVMのデジタル証明書を提供する必要もあります。

MetroCluster構成では、クラスタ上のWebプロトコルエンジンの設定変更はパートナークラスタにレプリケートされません。

Webプロトコルエンジンを管理するためのONTAPコマンド

Webプロトコルエンジンを管理するには、コマンドを使用し `system services web`ます。Webアクセス要求がファイアウォールを通過できるようにするには、コマンドと `network interface modify`コマンドを使用し `system services firewall policy create`ます。

状況	使用するコマンド
クラスタレベルで Web プロトコルエンジンを設定します。 • クラスタの Web プロトコルエンジンを有効または無効にします • クラスタの SSLv3 を有効または無効にします • セキュアな Web サービス（ HTTPS ）に対する FIPS 140-2 準拠を有効または無効にする	`system services web modify`
クラスタレベルの Web プロトコルエンジンの設定を表示し、 Web プロトコルがクラスタ全体で機能しているかどうかを確認し、 FIPS 140-2 準拠が有効でオンラインになっているかどうかを表示します	`system services web show`
ノードレベルの Web プロトコルエンジンの設定と、クラスタ内のノードに対する Web サービス処理のアクティビティを表示します	`system services web node show`

状況	使用するコマンド
ファイアウォールポリシーを作成するか、既存のファイアウォールポリシーに HTTP または HTTPS プロトコルサービスを追加して、 Web アクセス要求がファイアウォールを通過できるようにします	`system services firewall policy create` パラメータをまたは `https`に `http`設定する `-service`と、Webアクセス要求がファイアウォールを通過できるようになります。
ファイアウォールポリシーを LIF と関連付ける	`network interface modify` パラメータを使用すると、LIFのファイアウォールポリシーを変更できます `-firewall-policy`。

関連情報

- "network interface modify"

ONTAP Webサービスへのアクセスを構成する

Web サービスへのアクセスを設定することで、許可されたユーザが、 HTTP または HTTPS を使用してクラスタまたは Storage Virtual Machine （ SVM ）のサービスコンテンツにアクセスできるようになります。

手順

1. ファイアウォールが有効になっている場合は、 Web サービスで使用される LIF のファイアウォールポリシーで HTTP または HTTPS のアクセスがセットアップされていることを確認してください。

   ファイアウォールが有効になっているかどうかを確認するには、コマンドを使用し `system services firewall show`ます。

   a. ファイアウォールポリシーでHTTPまたはHTTPSが設定されていることを確認するには、コマンドを使用し `system services firewall policy show`ます。

      ポリシーでWebアクセスをサポートするには、コマンドのパラメータを `system services firewall policy create`または `https`に `http`設定し `-service`ます。

   b. HTTPまたはHTTPSをサポートしているファイアウォールポリシーが、Webサービスを提供するLIFに関連付けられていることを確認するには、パラメータを指定してコマンドを `-firewall-policy`使用し `network interface show`ます。

      の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

      LIFに対してファイアウォールポリシーを有効にするには、コマンドで `-firewall-policy`パラメータを使用し `network interface modify`ます。

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

2. クラスタレベルのWebプロトコルエンジンを設定してWebサービスのコンテンツにアクセスできるようにするには、コマンドを使用し `system services web modify`ます。

3. セキュアなWebサービス（HTTPS）を使用する場合は、コマンドを使用してSSLを有効にし、クラスタまたはSVMのデジタル証明書情報を入力します `security ssl modify`。

   の詳細については `security ssl modify`、を"ONTAPコマンド リファレンス"参照してください。

4. クラスタまたはSVMでWebサービスを有効にするには、コマンドを使用し `vserver services web modify` ます。

   この手順は、クラスタまたは SVM に対して有効にする各サービスについて繰り返す必要があります。

5. 特定のロールにクラスタまたはSVMのWebサービスへのアクセスを許可するには、コマンドを使用し `vserver services web access create` ます。

   アクセスを許可するロールはすでに存在している必要があります。既存のロールを表示する `security login role show` にはコマンドを使用します。新しいロールを作成するにはコマンドを使用します `security login role create`。

   および `security login role create` の詳細については `security login role show`、を"ONTAPコマンド リファレンス"参照してください。

6. Webサービスへのアクセスが許可されているロールについては、コマンドの出力を確認して、ユーザにも正しいアクセス方法が設定されていることを確認して `security login show` ください。

   ONTAP API Webサービスにアクセスするには `ontapi`）、ユーザにアクセス方法が設定されている必要があります `ontapi`。他のすべてのWebサービスにアクセスするには、ユーザにアクセス方法が設定されている必要があり `http` ます。

   の詳細については `security login show`、を"ONTAPコマンド リファレンス"参照してください。

> ユーザのアクセス方法を追加するには、コマンドを使用し `security login create` ます。の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

Webサービスを管理するためのONTAPコマンド

クラスタまたはStorage Virtual Machine（SVM）でのWebサービスの使用を管理するには、コマンドを使用し `vserver services web` ます。ロールのWebサービスへのアクセスを制御するには、コマンドを使用し `vserver services web access` ます。

状況	使用するコマンド
クラスタまたはSVMのWebサービスを設定します。 • Webサービスを有効または無効にする • WebサービスへのアクセスにHTTPSのみを使用できるかどうかを指定する	`vserver services web modify`
クラスタまたはSVMのWebサービスの設定と可用性を表示する	`vserver services web show`

状況	使用するコマンド
特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを許可する	`vserver services web access create`
クラスタまたはSVMのWebサービスへのアクセスが許可されているロールを表示する	`vserver services web access show`
特定のロールがクラスタまたはSVMのWebサービスにアクセスできないようにする	`vserver services web access delete`

関連情報

"ONTAPコマンド リファレンス"

ONTAPノード上のマウントポイントを管理するためのコマンド

Webサービスは `spi`、ノードのログファイルまたはコアファイルへのアクセス要求に応じて、1つのノードから別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で管理する必要はありませんが、コマンドを使用して管理できます `system node root-mount`。

状況	使用するコマンド
あるノードから別のノードのルートボリュームへのマウントポイントを手動で作成する	`system node root-mount create`ノード間で作成できるマウントポイントは1つだけです。
クラスタ内のノード上の既存のマウントポイントを、マウントポイントが作成された時刻と現在の状態を含めて表示する	`system node root-mount show`
ノードから別のノードのルートボリュームへのマウントポイントを削除し、そのマウントポイントへの接続を強制的に終了する	`system node root-mount delete`

関連情報

"ONTAPコマンド リファレンス"

ONTAPでSSLを管理する

コマンドを使用して `security ssl`、クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理します。SSLプロトコルは、デジタル証明書を使用してWebサーバとブラウザ間の暗号化された接続を確立することで、Webアクセスのセキュリティを向上させます。

クラスタまたはStorage Virtual Machine（SVM）のSSLは次の方法で管理できます。

- SSLの有効化
- デジタル証明書を生成してインストールし、クラスタまたはSVMと関連付ける
- SSL設定を表示してSSLが有効になっているかどうかを確認し、可能な場合はSSL証明書名を表示します。
- クラスタまたはSVMのファイアウォールポリシーを設定し、Webアクセス要求が通過できるようにする
- 使用できるSSLのバージョンの定義
- WebサービスのHTTPS要求のみにアクセスを制限する

SSLの管理用コマンド

クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理するには、コマンドを使用し`security ssl`ます。

状況	使用するコマンド
クラスタまたはSVMのSSLを有効にし、デジタル証明書を関連付ける	`security ssl modify`
クラスタまたはSVMのSSL設定と証明書の名前を表示する	`security ssl show`

および`security ssl show`の詳細については`security ssl modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP WebサービスにHSTSを使用する

HTTP Strict Transport Security（HSTS）は、プロトコルダウングレード攻撃やCookieハイジャックといった中間者攻撃からウェブサイトを保護するためのWebセキュリティポリシーメカニズムです。HSTSはHTTPSの使用を強制することで、ユーザーのブラウザとサーバ間のすべての通信が暗号化されることを保証します。ONTAP9.17.1以降、ONTAPはONTAP Webサービスに対してHTTPS接続を強制できるようになりました。

HSTSは、 ONTAPとの最初のセキュアなHTTPS接続が確立された後にのみ、Webブラウザによって適用されます。ブラウザが最初のセキュアな接続を確立しない場合、HSTSは適用されません。HSTSの管理については、ブラウザのドキュメントを参照してください。

タスクの内容

- 9.17.1以降では、新規にインストールされたONTAPクラスタではHSTSがデフォルトで有効になっています。9.17.1にアップグレードすると、HSTSはデフォルトで有効になりません。アップグレード後にHSTSを有効にする必要があります。
- HSTSはすべてサポートされています"ONTAP Webサービス" 。

開始する前に

- 次のタスクには高度な権限が必要です。

HSTS構成を表示

現在の HSTS 構成を表示して、有効になっているかどうかを確認し、最大経過時間の設定を表示できます。

手順

1. 使用 `system services web show` HSTS 設定を含む現在の Web サービス構成を表示するコマンド:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                             HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

HSTSを有効にして最大年齢を設定する

ONTAP 9.17.1以降、新しいONTAPクラスタではHSTSがデフォルトで有効になっています。既存のクラスタを9.17.1以降にアップグレードする場合は、クラスタでHSTSを手動で有効にして、HTTPSの使用を強制する必要があります。HSTSを有効にして最大有効期間を設定できます。HSTSが有効になっている場合は、いつでも最大有効期間を変更できます。HSTSを有効にすると、ブラウザは最初のセキュア接続が確立された後にのみ、セキュア接続の強制を開始します。

手順

1. 使用 `system services web modify` HSTS を有効にするか、最大経過時間を変更するコマンド:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age`ブラウザがHTTPSの適用を記憶する期間（秒数）を指定します。デフォルト値は63072000秒（2年）です。

HSTSを無効にする

ブラウザは接続ごとにHSTSの最大有効期間設定を保存し、 ONTAPでHSTSが無効になっている場合でも、接続中はHSTSを継続的に適用します。ブラウザがHSTSの適用を停止するまでには、設定された最大有効期間

までかかります。この期間中に安全な接続が不可能になった場合、HSTSを適用しているブラウザは、問題が解決されるかブラウザの最大有効期間が切れるまで、 ONTAP Webサービスへのアクセスを許可しません。

手順

1. HSTSを無効にするには、 `system services web modify`指示：

```
system services web modify -hsts-enabled false
```

関連情報

"RFC 6797 - HTTP 厳格なトランスポート セキュリティ (HSTS)"

ONTAP Webサービスアクセスの問題のトラブルシューティング

設定エラー原因 Web サービスへのアクセスに関する問題が発生します。このエラーに対応するには、 LIF 、ファイアウォールポリシー、 Web プロトコルエンジン、 Web サービス、デジタル証明書、 すべてのユーザアクセス許可が正しく設定されていることを確認します。

次の表は、 Web サービスの設定エラーを特定して対処する際に役立ちます。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
Webサービスにアクセスしようとすると、Webブラウザからまたは `failure to establish a connection`エラーが返されます `unable to connect。	LIF が正しく設定されていない可能性があります。	Web サービスを配信する LIF に ping を送信できることを確認します。 LIFにpingを送信するには、コマンドを使用し `network ping`ます。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
ファイアウォールが正しく設定されていない可能性があります。	HTTP または HTTPS をサポートするようにファイアウォールポリシーが設定されていて、ポリシーが Web サービスを配信する LIF に割り当てられていることを確認します。 ファイアウォールポリシーを管理するには、コマンドを使用し `system services firewall policy`ます。ポリシーとLIFを関連付けるには、コマンドと `-firewall-policy`パラメータを使用し `network interface modify`ます。	Web プロトコルエンジンが無効になっている可能性があります。
Web プロトコルエンジンが有効になっていて、 Web サービスがアクセス可能であることを確認します。 クラスタのWebプロトコルエンジンを管理するには、コマンドを使用し `system services web`ます。	Webサービスにアクセスしようとすると、Webブラウザからエラーが返され `not found`ます。	Web サービスが無効になっている可能性があります。
アクセスを許可する各 Web サービスが個別に有効になっていることを確認します。 Webサービスへのアクセスを有効にするには、コマンドを使用し `vserver services web modify`ます。	Web ブラウザで、ユーザのアカウント名とパスワードを使用して Web サービスにログインできない。	ユーザを認証できない、アクセス方法が正しくない、またはユーザに Web サービスへのアクセスが許可されていない

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
ユーザアカウントが存在し、正しいアクセス方法と認証方法が設定されていることを確認します。また、ユーザのロールに Web サービスへのアクセスが許可されていることを確認します。 ユーザアカウント、そのアクセス方法および認証方法を管理するには、コマンドを使用し `security login`ます。ONTAP API Webサービスにアクセスするには、アクセス方法が必要 `ontapi`です。他のすべてのWebサービスにアクセスするには、アクセス方法が必要 `http`です。Webサービスへのロールのアクセスを管理するには、コマンドを使用し `vserver services web access`ます。	HTTPS を使用して Web サービスに接続すると、接続が中断されたことが Web ブラウザに表示されます。	Web サービスを配信するクラスタまたは Storage Virtual Machine （ SVM ）で SSL が有効になっていない可能性がある
クラスタまたは SVM で SSL が有効になっていて、デジタル証明書が有効であることを確認します。 HTTPサーバのSSL設定を管理するにはコマンドを使用し、デジタル証明書情報を表示するにはコマンドを `security certificate show`使用し `security ssl`ます。	HTTPS を使用して Web サービスに接続すると、信頼されていない接続であると Web ブラウザに表示されます。	自己署名デジタル証明書を使用している可能性があります。

関連情報

- "ONTAPのネットワーク構成のベストプラクティスは何ですか?"
- "ネットワークping"
- "network interface modify"
- "セキュリティ証明書のgenerate-csr"

- "セキュリティ証明書のインストール"
- "security certificate show"
- "セキュリティSSL"

証明書を使用してリモートサーバのIDを確認する

ONTAPの証明書を使用してリモート サーバーの ID を検証する方法について説明します。

ONTAP は、リモートサーバの ID を検証するセキュリティ証明書機能をサポートしています。

ONTAP ソフトウェアでは、次のデジタル証明書機能とプロトコルを使用して安全に接続できます。

- Online Certificate Status Protocol （ OCSP ）は、 SSL 接続と Transport Layer Security （ TLS ）接続を使用して、 ONTAP サービスからのデジタル証明書要求のステータスを検証します。この機能はデフォルトでは無効になっています。
- ONTAP ソフトウェアには、信頼されたルート証明書のデフォルトセットが付属しています。
- Key Management Interoperability Protocol （ KMIP ）の証明書を使用して、クラスタと KMIP サーバの相互認証を有効にできます。

ONTAPのOCSPを使用してデジタル証明書が有効であることを確認する

Online Certificate Status Protocol（OCSP）を使用すると、トランスポート層セキュリティ（TLS）通信を使用するONTAPアプリケーションは、OCSPが有効になっている場合にデジタル証明書ステータスを受信できます。特定のアプリケーションに対するOCSP証明書ステータスチェックは、いつでも有効または無効にできます。デフォルトでは、OCSP証明書ステータスチェックは無効になっています。

開始する前に

このタスクを実行するには、advanced権限レベルのアクセス権が必要です。

タスクの内容

OCSPは次のアプリケーションをサポートしています。

- AutoSupport
- Event Management System（EMS；イベント管理システム）
- LDAP over TLS
- Key Management Interoperability Protocol（KMIP）
- 監査ログ
- FabricPool
- SSH（ONTAP 9.13.1以降）

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 特定のONTAPアプリケーションでOCSPによる証明書のステータスチェックを有効または無効にするには、該当するコマンドを使用します。

一部のアプリケーションで **OCSP** による証明書のステータスチェックを有効または無効にする場合	使用するコマンド
有効	`security config ocsp enable -app app name`
無効にする	`security config ocsp disable -app app name`

次のコマンドは、AutoSupportおよびEMSのOCSPサポートを有効にします。

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSPが有効な場合、アプリケーションは次のいずれかの応答を受信します。

- Good - 証明書は有効で、通信可能な状態です。
- Revoked - 証明書は発行元の認証局によって永続的に信頼できないと判断されており、通信不可能な状態です。
- Unknown - サーバが証明書に関するステータス情報を持っていないため、通信不可能な状態です。
- OCSP server information is missing in the certificate -サーバはOCSPが無効になっているかのように動作し、TLS通信を続行しますが、ステータスチェックは行われません。
- No response from OCSP server - アプリケーションを実行できない状態です。

3. TLS通信を使用するすべてのアプリケーションでOCSPによる証明書のステータスチェックを有効または無効にするには、該当するコマンドを使用します。

すべてのアプリケーションで **OCSP** による証明書のステータスチェックを有効または無効にする場合	使用するコマンド
有効	`security config ocsp enable -app all`
無効にする	`security config ocsp disable -app all`

有効にすると、すべてのアプリケーションが、指定された証明書が有効、失効、または不明であることを示す署名付き応答を受信します。証明書が失効している場合は、アプリケーションを続行できません。アプリケーションがOCSPサーバからの応答を受信できない場合、またはサーバに到達できない場合、アプリケーションは続行できません。

4. OCSPをサポートするすべてのアプリケーションとそのサポートステータスを表示するには、コマンドを使用し `security config ocsp show`ます。

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true
         ssh                             true

         8 entries were displayed.
```

関連情報

- "security config ocsp enableコマンドを実行します"
- "security config ocsp disableを指定します"
- "security config ocsp showの出力を確認します"

ONTAPで TLS ベースのアプリケーションのデフォルト証明書を表示する

ONTAP は、トランスポート層セキュリティ (TLS) を使用するONTAPアプリケーションに、信頼できるルート証明書のデフォルト セットを提供します。

開始する前に

デフォルトの証明書は、管理 SVM の作成時またはアップグレード時にのみ管理 SVM にインストールされます。

タスクの内容

現在クライアントとして機能し、証明書の検証が必要なアプリケーションは、 AutoSupport 、 EMS 、 LDAP 、監査ログ、 FabricPool 、 および KMIP を使用できます。

証明書の有効期限が切れると、ユーザに証明書を削除するよう要求する EMS メッセージが起動します。デフォルトの証明書は、 advanced 権限レベルでのみ削除できます。

デフォルトの証明書を削除すると、一部の ONTAP アプリケーションが正常に機能しなくなる場合があります（ AutoSupport 、監査ログなど）。

ステップ

1. 管理SVMにインストールされているデフォルトの証明書を表示するには、security certificate showコマンドを使用します。

security certificate show -vserver –type server-ca

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

の詳細については `security certificate show`、を"ONTAPコマンド リファレンス"参照してください。

クラスタとKMIPサーバの相互認証

ONTAPクラスタとKMIPサーバの相互認証の概要

Key Management Interoperability Protocol （ KMIP ）サーバなど、クラスタと外部キー管理ツールを相互認証することで、キー管理ツールが SSL を介した KMIP を使用してクラスタと通信できるようになります。この設定は、特定のアプリケーションや機能（ストレージ暗号化機能など）で、セキュアなデータアクセスを提供するためにセキュアなキーが必要な場合に使用します。

ONTAPでクラスタの証明書署名要求を生成する

Certificate Signing Request（CSR；証明書署名要求）を生成するには、security certificateコマンドを使用し `generate-csr`ます。要求が処理されると、署名済みのデジタル証明書が認証局（CA）から送信されます。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. CSRを生成します。

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

の詳細については `security certificate generate-csr`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、SHA256ハッシュ関数で生成される2、048ビット秘密鍵を使用してCSRを作成します。この証明書は、米国カリフォルニア州のサニーベールにある企業（カスタム共通名server1.companyname.com）のIT部門のソフトウェアグループが使用します。SVM担当管理者のEメールアドレスは\ web@example.comです。出力にCSRと秘密鍵が表示されます。

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. CSR出力の証明書要求を電子形式（Eメールなど）で信頼できるサードパーティのCAに送信し、署名を求めます。

   要求が処理されると、署名済みのデジタル証明書がCAから送信されます。秘密鍵とCA署名デジタル証明書のコピーを保管しておく必要があります。

ONTAPクラスタ用のCA署名サーバ証明書をインストールする

SSL サーバでクラスタまたは Storage Virtual Machine （ SVM ）を SSL クライアントとして認証するためには、 client タイプのデジタル証明書をクラスタまたは SVM にインストールします。次に、 client-ca 証明書をその SSL サーバの管理者に渡してインストールしてもらいます。

開始する前に

SSLサーバのルート証明書を、証明書タイプのクラスタまたはSVMにインストールしておく必要があります `server-ca`。

手順

1. クライアント認証に自己署名デジタル証明書を使用するには、 `security certificate create`コマンドでパラメータを指定し `type client`ます。

   の詳細については `security certificate create`、を"ONTAPコマンド リファレンス"参照してください。

2. クライアント認証に CA 署名デジタル証明書を使用するには、次の手順を実行します。

   a. security certificateコマンドを使用して、デジタル証明書署名要求（CSR）を生成します `generate-csr`。

      証明書要求と秘密鍵を含む CSR 出力が表示され、今後の参照用にファイルにコピーするよう求められます。 ONTAP

   b. CSR 出力の証明書要求をデジタル形式（ E メールなど）で信頼できる CA に送信し、署名を求めます。

      秘密鍵と CA 署名証明書のコピーは今後の参照用として保管しておいてください。

   要求が処理されると、署名済みのデジタル証明書がCAから送信されます。

   a. コマンドでパラメータを指定して `-type client`、CA署名証明書をインストールし `security certificate install`ます。
   b. プロンプトが表示されたら証明書と秘密鍵を入力し、 * Enter * キーを押します。
   c. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、 * Enter * キーを押します。

      信頼できるルート CA から発行された SSL 証明書に至る証明書チェーンに中間証明書がない場合は、クラスタまたは SVM に中間証明書をインストールします。中間証明書は、問題のエンドエンティティのサーバ証明書専用に信頼できるルートから発行される、副次的な証明書です。この結果、信頼できるルート CA から始まり、中間証明書を経て、発行された SSL 証明書で終わる証明書チェーンが形成されます。

3. クラスタまたはSVMの証明書をSSLサーバの管理者に渡してインストールしてもらいます `client-ca`。

   security certificate showコマンドと `-type client-ca`パラメータを指定して実行すると、 `-instance`証明書の情報が表示されます `client-ca`。

関連情報

- "セキュリティ証明書のインストール"
- "security certificate show"

ONTAPのKMIPサーバ用のCA署名付きクライアント証明書をインストールする

Key Management Interoperability Protocol （ KMIP ）の証明書サブタイプ（ -subtype kmip-cert パラメータ）は、 client および server-ca のタイプと組み合わせて適用され、クラスタと外部キー管理ツール（ KMIP サーバなど）の相互認証に使用される証明書であることを示します。

タスクの内容

KMIP サーバをクラスタに対して SSL サーバとして認証する KMIP 証明書をインストールします。

手順

1. コマンドでパラメータと `-subtype kmip-cert`パラメータを指定して `-type server-ca`、`security certificate install`KMIPサーバのKMIP証明書をインストールします。

2. プロンプトが表示されたら、証明書を入力して Enter キーを押します。

   今後の参照用として証明書のコピーを保管するように ONTAP から求められます。

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

関連情報

- "セキュリティ証明書のインストール"

セキュリティとデータ暗号化

自律型ランサムウェア対策

ONTAP自律型ランサムウェア対策の詳細

ONTAP 9.10.1以降、 ONTAP管理者はAutonomous Ransomware Protection（ARP）を有効にしてNAS（NFSおよびSMB）環境でワークロード分析を実行し、ランサムウェア攻撃の兆候となる可能性のある異常なアクティビティをプロアクティブに検出して警告することができます。ONTAPONTAP 9.17.1 以降、ARP は、LUN または NVMe 名前空間を含む SAN ボリューム、または VMware、Hyper-V、KVM などのハイパーバイザーからの仮想ディスクを含む NAS ボリュームなどのブロック デバイス ボリュームもサポートします。

ARPはONTAPに直接組み込まれており、ONTAPの他の機能との統合的な制御と連携を実現します。ARPはリアルタイムで動作し、ファイルシステムへの書き込みやファイルシステムからの読み取り時にデータを処理し、潜在的なランサムウェア攻撃を迅速に検出して対応します。

ARPは、保護を強化するために、スケジュールされたスナップショットに加え、定期的にロックされたスナップショットを作成します。スナップショットの保存期間をスマートに管理します。異常なアクティビティが検出されない場合、スナップショットはすぐに再利用されます。ただし、攻撃が検出された場合は、攻撃開始前に作成されたスナップショットが長期間保持されます。

ライセンスとイネーブルメント

ARPのサポートは "ONTAP 1ライセンス"。ONTAP One ライセンスをお持ちでない場合は、 ONTAPのバージョンに応じて異なる他のライセンスを ARP に使用できます

ONTAP リリース	ライセンス
ONTAP 9.11.1以降	`Anti_ransomware`
ONTAP 9 10.1	`MT_EK_MGMT` （マルチテナントキー管理）

- ONTAP 9.10.1からONTAP 9.11.1以降にアップグレードする場合、システムでARPがすでに設定されている場合は、新しいものをインストールする必要はありません。 `Anti-ransomware`ライセンス。新しくARPを設定する場合は、ライセンスが必要です。
- ONTAP 9.11.1 以降からONTAP 9.10.1 に復元する場合、Anti_ransomware ライセンスで ARP を有効にしていると、警告メッセージが表示され、ARP の再設定が必要になることがあります。"ARPのリバートについて説明します" 。

"既存のボリュームで自律ランサムウェア保護（ARP）を有効にするか、新しいボリュームを作成してARPを有効にすることができます。" 。

ONTAPランサムウェア対策戦略

ランサムウェアを効果的に検出するには、複数の保護レイヤが必要です。例として、自動車の安全機能を考え

てみましょう。シートベルトなどの1つの機能だけでは、事故から完全に身を守ることはできません。エアバッグ、アンチロックブレーキ、前方衝突警告は、総合的に見てより良い結果につながる安全機能です。ランサムウェア対策についても同じことが言えます。

ONTAPには、ランサムウェアからの保護に役立つ FPolicy、スナップショット、 SnapLock、 Active IQ Digital Advisor （ Digital Advisorとも呼ばれる）などの機能が含まれていますが、次の情報は機械学習機能を備えた ARP 機能に重点を置いています。

ランサムウェアから保護するNetAppポートフォリオのその他の機能の詳細については、以下を参照してください。 "ランサムウェアとNetAppの保護ポートフォリオ" 。

ARPが検出する内容

ONTAP ARPは、身代金が支払われるまで攻撃者がデータを保持し続けるサービス拒否攻撃から保護するように設計されています。ARPは、以下の情報に基づいてリアルタイムのランサムウェア検出を提供します。

- 受信データが暗号化されているかプレーンテキストであるかを識別します。
- 以下を検出する分析：
  - エントロピー: (NASおよびSANで使用) ファイル内のデータのランダム性の評価
  - ファイル拡張子の種類: (NASでのみ使用) 想定される拡張子の種類に準拠していないファイル拡張子
  - ファイル**IOPS**: (ONTAP 9.11.1以降のNASでのみ使用) データ暗号化による異常なボリュームアクティビティの急増

ARP は、少数のファイルが暗号化されただけでほとんどのランサムウェア攻撃の拡散を検出し、自動的に応答してデータを保護して、疑わしい攻撃が発生していることを警告します。

ランサムウェア検出システムでは完全な安全性を保証することはできません。 ARP は、ウイルス対策ソフトウェアが侵入を検出できなかった場合に、追加の防御層を提供します。

ARPモードについて学ぶ

ボリュームに対して ARP が有効になると、ベースラインを確立するための学習期間に入ります。 ARP は、アクティブ検出モードに移行する前にシステム メトリックを分析してアラート プロファイルを作成します。アクティブ モードでは、ARP は異常なアクティビティを監視し、異常な動作を検出すると保護アクションを実行し、アラートを生成します。

ARP の場合、学習モードとアクティブ モードの動作は、 ONTAP のバージョン、ボリューム タイプ、およびプロトコル (NAS または SAN) によって異なります。

NAS環境とモードの種類

NAS環境では学習モードとアクティブモードが使用されます。 ARP/AI ONTAP 9.16.1 以降の NAS 環境で実行されている場合、 FlexVolボリュームで ARP が使用されるときに学習期間はありません。

次の表は、NAS 環境におけるONTAP 9.10.1 以降のバージョンの違いをまとめたものです。

モード	説明	ボリュームの種類とバージョン
学ぶ	ONTAP 9.15.1～9.10.1では、ARPを有効にすると自動的に学習モードに設定されます。ARP学習モードでは、ONTAPシステムにより、分析対象（エントロピー、ファイルの拡張子タイプ、ファイルのIOPS）に基づくアラート プロファイルが作成されます。を学習モードのまま30日間維持することをお勧めします。ONTAPONTAP 9.13.1 以降、ARP は最適な学習間隔を自動的に決定し、切り替えを自動化します。切り替えは 30 日前に実行される可能性があります。ONTAPより前のバージョンでは、手動で切り替えることができます。 "学習モードからアクティブモードへの切り替えについて詳しくは、こちらをご覧ください。" 。 コマンドは `security anti-ransomware volume workload-behavior show`、ボリュームで検出されたファイル拡張子を表示します。このコマンドをラーニングモードの早い段階で実行し、ファイルタイプが正確に表示される場合は、ONTAPが他のメトリックを収集しているため、このデータをアクティブモードに移行する際のベースとして使用しないでください。の詳細については `security anti-ransomware volume workload-behavior show`、を"ONTAPコマンド リファレンス"参照してください。	• ONTAP 9.15.1～9.10.1のFlexVolボリューム • ONTAP 9.13.1以降のFlexGroupボリューム
アクティブ	学習モードでワークロードの特性を評価するのに十分な期間ARPを実行したら、アクティブ モードに切り替えてデータの保護を開始します。ONTAP 9.13.1 以降、ARP は最適な学習間隔を自動的に決定し、切り替えを自動化します。切り替えは 30 日前に実行される可能性があります。 ONTAP 9.15.1 ～ 9.10.1 では、最適な学習期間が完了すると ARP はアクティブ モードに切り替わります。ARPをアクティブ モードに切り替えると、ONTAPによって、脅威が検出された場合にデータを保護するためのARP Snapshotが作成されます。 アクティブ モードでは、ファイル拡張子に異常のフラグが立てられている場合は、アラートを評価する必要があります。アラートに応じてデータを保護するための措置を講じることも、アラートを誤検知としてマークすることもできます。アラートを誤検出としてマークすると、そのプロファイルが更新されます。例えば、新しいファイル拡張子によってアラートがトリガーされ、それを誤検知としてマークした場合、次回そのファイル拡張子が検出されたときにはアラートは表示されなくなります。	サポートされているすべてのONTAPバージョンとFlexVolおよびFlexGroupボリューム

SAN環境とモードの種類

SAN環境では、自動的にアクティブ検出に移行する前に、評価期間（NAS環境の学習モードに類似）が設けられます。次の表は、評価モードとアクティブモードの概要です。

モード	説明	ボリュームの種類とバージョン
評価	暗号化のベースライン動作を決定するために、2～4週間の評価期間が設けられます。評価期間が完了したかどうかを確認するには、 `security anti-ransomware volume show`コマンドとチェック `Block device detection status`。 "SANボリュームとエントロピー評価期間の詳細" 。	• ONTAP 9.17.1以降のFlexVolボリューム
アクティブ	評価期間終了後、ARP SAN保護がアクティブかどうかを確認するには、`security anti-ransomware volume show`コマンドとチェック `Block device detection status`の状態 `Active_suitable_workload`評価されたエントロピー量が正常に監視できることを示します。ARPは、評価中に確認されたデータに応じて適応しきい値を自動的に調整します。	• ONTAP 9.17.1以降のFlexVolボリューム

脅威評価と**ARP**スナップショット

ARPは、学習済みの分析結果に基づいて測定された受信データに基づいて脅威の確率を評価します。ARPが異常を検出すると、測定値が割り当てられます。スナップショットは、検出時または定期的に割り当てられます。

ARPしきい値

- 低：ボリュームの異常をいち早く検出したもの（たとえば、新しいファイル拡張子がボリュームに検出された場合など）。このレベルの検出は、ARP/AIを搭載していないONTAP 9 .16.1より前のバージョンでのみ使用できます。
  - ONTAP 9.11.1以降では、 "ARPの検出パラメータをカスタマイズする" 。
  - ONTAP 9.10.1では、中程度へのエスカレーションのしきい値は100個以上です。
- 中：高いエントロピーが検出されるか、または同じ未知のファイル拡張子を持つ複数のファイルが検出された場合。これは、ARP/AI機能を備えたONTAP 9.16.1以降のベースライン検出レベルです。

ONTAPによって、異常がランサムウェアのプロファイルと一致しているかを判断する分析レポートが実行されると、脅威は「Moderate」に格上げされます。攻撃の可能性がModerateの場合、ONTAPによって、脅威の評価を求めるEMS通知が生成されます。しかし、ONTAP9.14.1以降では、以下のことが可能です"デフォルトのアラート設定を変更する"。"異常な活動への対応" 。

中程度の脅威に関する情報は、System Managerの*[イベント]セクションまたはコマンドを使用して確認できます `security anti-ransomware volume show`。脅威が低いイベントは、ARP / AIがないONTAP 9.16.1より前のバージョンでコマンドを使用して表示することもできます `security anti-ransomware volume show`。の詳細については `security anti-ransomware volume show`、を"ONTAPコマンド リファレンス"参照してください。

ARPスナップショット

ARP は、攻撃の初期兆候が検出されるとスナップショットを作成します。その後、詳細な分析が行われ、潜在的な攻撃の有無が判断されます。ARP ARP スナップショットは、攻撃が完全に確認される前でも積極的に作成されるため、特定の正当なアプリケーションに対しては定期的に生成されることもあります。これらのスナップショットの存在は異常とはみなされません。攻撃が確認された場合、攻撃確率は `Moderate`攻撃通知

が生成されます。

ONTAP 9.17.1 以降では、NAS ボリュームと SAN ボリュームの両方に対して、また検出された異常に応じて、ARP スナップショットが定期的に生成されます。は、ARPスナップショットに識別しやすい名前を付けます。

ONTAP 9.11.1以降では、保持設定を変更できます。詳細については、 "スナップショットのオプションを変更します。" 。

次の表は、バージョン別の ARP スナップショットの違いをまとめたものです。

機能	**ONTAP 9.17.1**以降	**ONTAP 9.16.1**以前
作成トリガー	• スナップショットは、特定のトリガーに関係なく、固定の4時間間隔で作成されます。 • 攻撃の確認 トリガー タイプに基づいて、「定期的」または「攻撃」スナップショットが作成されます。	• 高エントロピーが検出されました • 新しいファイル拡張子が検出されました (9.15.1 以前) • ファイル操作の急増が検出されました (9.15.1 以前) スナップショットの作成間隔はトリガー タイプによって異なります。
先頭に付ける名前の規則	「ランサムウェア対策定期バックアップ」「ランサムウェア攻撃対策バックアップ」	「ランサムウェア対策バックアップ」
削除動作	ARPスナップショットはロックされており、管理者は削除できません	ARPスナップショットはロックされており、管理者は削除できません
最大スナップショット数	"スナップショットの設定可能な制限は6つ"	"スナップショットの設定可能な制限は6つ"
保持期間	スナップショットは通常 12 時間保持されます。 • NAS ボリューム: ファイル分析によって攻撃が確認された場合、管理者が攻撃を真または誤検知 (明らかに疑わしい) としてマークするまで、攻撃前に作成されたスナップショットは保持されます。 • SAN ボリュームまたは VM データストア: ブロックエントロピー分析によって攻撃が確認された場合、攻撃前に作成されたスナップショットは 10 日間保持されます (構成可能)。	• トリガー条件に基づいて決定されます（固定ではありません） • 攻撃前に作成されたスナップショットは、管理者が攻撃を真または誤検知（明らかに疑わしい）としてマークするまで保持されます。

機能	**ONTAP 9.17.1**以降	**ONTAP 9.16.1**以前
明らかに疑わしい行為	管理者は、確認に基づいて保持を設定する明確な疑いのあるアクションを実行できます。 • 偽陽性の保持期間は24時間 • 真陽性保持期間は7日間	管理者は、確認に基づいて保持を設定する明確な疑いのあるアクションを実行できます。 • 偽陽性の保持期間は24時間 • 真陽性保持期間は7日間 この予防的保持動作は、 ONTAP 9.16.1より前には存在しません。
有効期限	すべてのスナップショットに有効期限が設定されます	なし

ランサムウェア攻撃後に**ONTAP**でデータをリカバリする方法

ARPは、実績のあるONTAPのデータ保護およびディザスタリカバリテクノロジーを基盤として、ランサムウェア攻撃に対応します。ARPARP は、攻撃の初期兆候が検出されると、ロックされたスナップショットを作成します。まず、攻撃が実際のものか誤検知なのかを確認する必要があります。攻撃が確認されれば、ARPスナップショットを使用してボリュームを復元できます。

ロックされたSnapshotは通常の方法では削除できません。ただし、後で攻撃を誤検知としてマークすることにした場合、 ONTAP はロックされたコピーを削除します。

ボリューム全体を元に戻す代わりに、選択したスナップショットから影響を受けたファイルを回復できます。

攻撃への対応とデータの回復の詳細については、次のトピックを参照してください。

- "異常な活動への対応"
- "ARPスナップショットからデータを回復する"
- "ONTAPスナップショットからのリカバリ"
- "スマートなランサムウェアリカバリ"

ARPのマルチ管理検証保護

ONTAP 9.13.1以降では、Autonomous Ransomware Protection（ARP；自律ランサムウェア対策）設定に複数の認証済みユーザ管理者が必要になるように、Multi-admin Verification（MAV；マルチ管理者検証）を有効にすることを推奨します。詳細については、を参照してください "マルチ管理者検証を有効にします"。

人工知能（**ARP / AI**）による自律型ランサムウェア対策

ONTAP 9.16.1以降、ARPはランサムウェア対策分析用の機械学習モデルを採用することでサイバーレジリエンス（回復力）を向上させます。ARPの機械学習モデルは、シミュレーションされたランサムウェア攻撃の前後両方の大規模なファイル データセットで事前にトレーニングされています。このモデルは、NAS環境で常に進化するランサムウェアを99%の精度で検出します。このリソース集約型のトレーニングは、オープンソースのフォレンジック調査データセットを用いてONTAPの外部で行われます。モデリングパイプライン全体で顧客データは使用されないため、プライバシーの問題は発生しません。このトレーニングから得られる事前トレーニング済みモデルは、 ONTAPに同梱されています。このモデルは、 ONTAP CLIまたはONTAP APIからアクセスしたり変更したりすることはできません。

FlexVolボリュームを使用した**ARP / AI**のアクティブな保護に即座に移行

ARP/AIとFlexVolボリュームでは、次のようなことはありません学習期間。ARP/AI は、インストール後または 9.16 にアップグレードするとすぐに有効化され、アクティブになりますクラスタをONTAP 9.16.1にアップグレードすると、既存および新規のFlexVolでARPがすでに有効になっている場合、それらのボリュームでARP/AIが自動的に有効になります。

"ARP/AIの有効化の詳細"

ARP/AIノシトウコウシン

最新のランサムウェアの脅威に対する保護を最新の状態に保つために、ARP/AIでは、ONTAPの通常のアップグレードやリリースのサイクルとは別に頻繁に自動更新を提供しています。もしあなたが"自動更新を有効にした"セキュリティファイルの自動更新を選択すると、ARP/AIの自動セキュリティ更新も受信できるようになります。また、 "これらの更新を手動で行う"更新が行われるタイミングを制御します。

System.16.1以降では、システムおよびファームウェアの更新に加えて、ONTAP 9 Managerを使用してARP/AIのセキュリティ更新を利用できます。

"ARP / AIの更新に関する詳細はこちら"

関連情報

- "ONTAPコマンド リファレンス"

ONTAP自律型ランサムウェア対策のユースケースと考慮事項

Autonomous Ransomware Protection (ARP) は、 ONTAP 9.10.1 以降の NAS ワークロードとONTAP 9.17.1 以降の SAN ワークロードで利用できます。ARPを導入する前に、推奨される使用方法、サポートされる構成、パフォーマンスへの影響について理解しておく必要があります。

サポートされる構成とされない構成

ARPの使用を決定する際には、ボリュームのワークロードがARPに適していること、および必要なシステム構成を満たしていることを確認することが重要です。

最適なワークロード

ARP は次のタイプのワークロードに適しています。

- NFSまたはSANストレージ上のデータベース
- WindowsまたはLinuxのホームディレクトリ

  ARP/AIが存在しない環境では、学習期間中に検出されない拡張子を持つファイルをユーザーが作成する可能性があります。そのため、このワークロードでは誤検知の可能性が高くなります。

- 画像とビデオ

  たとえば、医療記録やEDA（Electronic Design Automation）データなどです。

適していないワークロード：

ARP は次のタイプのワークロードには適していません。

- ファイルの作成または削除操作の頻度が高いワークロード (数秒で数十万のファイル、たとえばテスト/開発ワークロード)。
- ARP の脅威検出は、ファイルの作成、名前の変更、または削除操作の異常な急増を認識する能力に依存します。アプリケーション自体がファイル アクティビティのソースである場合、ランサムウェアのアクティビティと効果的に区別することができません。
- アプリケーションやホストがデータを暗号化するワークロード

  ARPでは、受信データが暗号化されているかどうかを区別する機能を使用します。アプリケーション自体がデータを暗号化している場合、機能の有効性が低下します。ただし、ARP は、ファイル アクティビティ (削除、上書き、作成、または新しいファイル拡張子による作成または名前変更) とファイル タイプに基づいて引き続き機能します。

サポートされている構成

ONTAP 9.10.1以降、NAS NFSおよびSMB FlexVolボリュームでARPが利用可能になりました。9.17.1以降では、SANストレージを備えたiSCSI、FC、NVMeのSAN FlexVolボリュームでもARPが利用可能になりました。

その他の構成とボリューム タイプのサポート状況は、ONTAPのバージョン別に次の表に示します。

	ONTAP 9.17.1	ONTAP 9 .16.1	ONTAP 9 .15.1	ONTAP 9 .14.1	ONTAP 9 .13.1	ONTAP 9 12.1	ONTAP 9 .11.1	ONTAP 9 10.1
SnapMirror非同期で保護されているボリューム	✓	✓	✓	✓	✓	✓		
SnapMirror非同期（SVMディザスタリカバリ）で保護されるSVM	✓	✓	✓	✓	✓	✓		
SVMデータ移動 (`vserver migrate`)	✓	✓	✓	✓	✓	✓		
FlexGroupボリューム[1]	✓	✓	✓	✓	✓			
マルチ管理者認証	✓	✓	✓	✓	✓			

	ONTAP 9.17.1	ONTAP 9 .16.1	ONTAP 9 .15.1	ONTAP 9 .14.1	ONTAP 9 .13.1	ONTAP 9 12.1	ONTAP 9 .11.1	ONTAP 9 10.1
自動更新機能を備えたARP / AI	✓	✓						

[1] ARP/AIはFlexGroupボリュームをサポートしていません。ONTAP9.16.1へのアップグレード後も、ARPが有効になっているFlexGroupボリュームは、ARP/AIの導入前と同じARPモデルで引き続き動作しONTAP。

SnapMirrorと**ARP**の相互運用性

ONTAP 9.12.1以降では、SnapMirror非同期デスティネーション ボリュームでARPがサポートされます。ARPは、 SnapMirror同期またはSnapMirrorアクティブ同期ではサポートされません。

SnapMirrorソースボリュームがARP対応の場合、 SnapMirrorデスティネーションボリュームは自動的にARP設定状態（ `dry-run`または `enabled`）、ARP トレーニング データ、およびソース ボリュームの ARP によって作成されたスナップショットが含まれます。あらためて有効にする必要はありません。

宛先ボリュームは読み取り専用（RO）スナップショットで構成されていますが、そのデータに対してARP処理は行われません。ただし、SnapMirrorデスティネーション ボリュームが読み書き可能（RW）に変換されると、そのボリュームでARPが自動的に有効になります。宛先ボリュームでは、ソースボリュームに既に記録されている情報以外に、追加の学習手順は必要ありません。

ONTAP 9.10.1および9.11.1では、ソース ボリュームからデスティネーション ボリュームへのARPの設定、トレーニング データ、Snapshotの転送は行われません。このため、 SnapMirror の宛先ボリュームを RW に変換する場合は、変換後に宛先ボリューム上の ARP を学習モードで明示的に有効にする必要があります。

ARPと仮想マシン

ARPは仮想マシン（VM）でサポートされています。ARPの検出動作は、VMの内部と外部の変更で異なります。ARP は、VM 内に高度に圧縮されたファイル (7z や ZIP など) や暗号化されたファイル (パスワードで保護された PDF、DOC、ZIP など) が多数含まれるワークロードには推奨されません。

VMの外部での変更

ARP は、新しい拡張子が暗号化された状態でボリュームに入力された場合、またはファイル拡張子が変更された場合に、VM 外部の NFS ボリューム上のファイル拡張子の変更を検出できます。

VMの内部での変更

ランサムウェア攻撃によって仮想マシン内のファイルが変更され、仮想マシン外部には変更が加えられなかった場合、仮想マシンのデフォルトのエントロピーが低い場合（.txt、.docx、.mp4ファイルなど）、ARPは脅威を検出しONTAP以前では、このシナリオでARPは保護スナップショットを作成しますが、仮想マシン外部のファイル拡張子は改ざんされていないため、脅威アラートは生成されません。ONTAP9.17.1のSANONTAP以降では、ARPは仮想マシン内部でエントロピー異常を検出した場合にも脅威アラートを生成します。

デフォルトでは、ファイルのエントロピーが高い場合 (たとえば、.gzip またはパスワードで保護されたファイル)、ARP の検出機能は制限されます。ARPはこの場合でもプロアクティブにSnapshotを作成できますが、ファイル拡張子が外部から改ざんされていない場合、アラートはトリガーされません。

SAN の場合、ARP はボリューム レベルでエントロピー統計を分析し、エントロピーの異常が見つかったときに検出をトリガーします。

サポートされない構成

ARP はONTAP S3 環境ではサポートされていません。

ARPでは、次のボリューム構成はサポートされません。

- FlexGroupボリューム（ ONTAP 9.10.1～9.12.1）。ONTAPONTAP以降ではFlexGroupボリュームがサポートされますが、ARP/AIより前のARPモデルに限定されます。
- FlexCacheボリューム（元のFlexVolではサポートされますが、キャッシュ ボリュームではサポートされません）
- オフライン ボリューム
- SnapLockボリューム
- SnapMirrorアクティブ同期
- SnapMirror同期
- SnapMirror非同期（ ONTAP 9.10.1および9.11.1）。SnapMirror非同期は、ONTAP 9.12.1以降でサポートされています。詳細については、 SnapMirror 。
- 制限されたボリューム
- Storage VMのルートボリューム
- 停止しているStorage VMのボリューム

ARPのパフォーマンスと周波数に関する考慮事項

ARPは、スループットとピークIOPSで測定されるシステム パフォーマンスへの影響はほとんどありません。ARP 機能の影響は、特定のボリュームのワークロードによって異なります。一般的なワークロードでは、以下の構成の制限が推奨されます。

ワークロードの特性	ノードあたりの最大ボリューム数（推奨値）	ノードあたりのボリューム制限を超えるとパフォーマンスが低下します [1]
読み取り集中型またはデータを圧縮できる	150	最大IOPSの4%
書き込みが多く、データを圧縮できない	60	• NAS: ONTAP 9.15.1 以前の場合、最大 IOPS の 10% • NAS: ONTAP 9.16.1 以降では最大 IOPS の 4% • SAN: ONTAP 9.17.1 以降では最大 IOPS の 5%

[1] 推奨制限を超えて追加されたボリュームの数に関係なく、システム パフォーマンスはこれらのパーセンテージを超えて低下しません。

ARP 分析は優先順位に従って実行されるため、保護されているボリュームの数が増えると、各ボリュームでの分析の実行頻度は低くなります。

ARPで保護されたボリュームを使用したマルチ管理者検証

ONTAP 9 .13.1以降では、マルチ管理者検証（MAV）をイネーブルにして、ARPによるセキュリティを強化できます。MAVを使用すると、少なくとも2人以上の認証された管理者が、保護されたボリュームでARPをオフにしたり、ARPを一時停止したり、疑わしい攻撃をfalse positiveとしてマークしたりする必要があります。方法をご確認ください"ARPで保護されたボリュームのMAVを有効にします"。

MAVグループの管理者を定義し、保護する、、 `security anti-ransomware volume pause`および `security anti-ransomware volume attack clear-suspect`ARPコマンドのMAVルールを作成する必要があり `security anti-ransomware volume disable`ます。MAVグループの各管理者は、MAV設定内の新しいルール要求を承認する必要があります"MAVルールを再度追加します"。

> `security anti-ransomware volume pause`、および `security anti-ransomware volume attack clear-suspect`の詳細について `security anti-ransomware volume disable`は、をlink:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+anti-ransomware+volume["ONTAPコマンドリファレンス"^]参照してください。

ONTAP 9.14.1以降では、ARPに、ARP Snapshotの作成と新しいファイル拡張子の監視に関するアラート機能が搭載されています。これらのイベントに関するアラートは、デフォルトでは無効になっています。アラートは、ボリューム レベルまたはSVMレベルで設定できます。アラートを有効にするには `security anti-ransomware vserver event-log modify`または音量レベルで `security anti-ransomware volume event-log modify`。

および `security anti-ransomware volume event-log modify`の詳細については `security anti-ransomware vserver event-log modify`、を"ONTAPコマンド リファレンス"参照してください。

次のステップ

- "自律型ランサムウェア対策を有効にする"
- "ARPで保護されたボリュームのMAVを有効にする"

ONTAP自律型ランサムウェア対策を有効にする

ONTAP 9 .10.1以降では、既存のボリュームで自律型ランサムウェア対策（ARP）を有効にするか、新しいボリュームを作成してARPを最初から有効にすることができます。

すべての新しいボリュームがAutonomous Ransomware Protection（ARP）でデフォルトで有効になるようにONTAPクラスタを設定する場合は、こちらを参照してください"関連するARP手順"。

タスクの内容

- **(NAS環境のみ) ONTAP 9.10.1～9.15.1**または**FlexGroup**ボリュームの**ARP**の場合 これらのバージョンのONTAPでは、常に最初にARPを有効にする必要があります。 "ラーニングモード" （または「ドライラン」状態）。最初に学習モードでARPを有効にすると、システムがワークロードを分析して正常な動作を特定します。最初からアクティブ モードにすると、誤検出レポートが大量に生成される可能性があります。

  ARP を学習モードで少なくとも 30 日間実行することをお勧めします。ONTAP 9.13.1以降では、ARPによって最適な学習期間が自動的に決定され、30日が経過しなくても自動的に切り替えが行われる場合があ

ります。

- **(NAS 環境のみ) FlexVol**ボリュームを備えた**ONTAP 9.16.1** 以降の場合 System Manager または CLI を使用して ARP を有効にすると、ARP/AI 保護が有効になり、すぐにアクティブになります。学習期間は必要ありません。
- （**SAN**環境のみ） **FlexVol**を備えた**ONTAP 9.17.1**以降の場合 System ManagerまたはCLIを使用してARPを有効にすると、ARP/AI機能が自動的に有効になります。SANボリュームで有効にすると、 "ARP/AIは評価期間中にデータを継続的に監視します"ワークロードが ARP に適しているかどうかを判断し、検出に最適な暗号化しきい値を設定します。

開始する前に

- プロトコルが有効になっているストレージ VM (SVM) が必要です。
  - NAS: NFS または SMB (あるいは両方)
  - SAN: iSCSI、FC、またはNVMe
- その"正しいライセンス" ONTAPバージョンに合わせてインストールする必要があります。
- クライアントが構成された NAS または SAN ワークロードが必要です。
- （NAS環境のみ）ARPを設定するボリュームには、アクティブな"ジャンクションパス" 。
- ボリュームの使用率が100%未満である必要があります。
- ARPアクティビティの通知を含む電子メール通知を送信するようにEMSシステムを設定することをお勧めします。詳細については、を参照してください "EMSイベントを設定してEメール通知を送信する"。
- ONTAP 9.13.1以降では、Autonomous Ransomware Protection（ARP；自律ランサムウェア対策）設定に複数の認証済みユーザ管理者が必要になるように、Multi-admin Verification（MAV；マルチ管理者検証）を有効にすることを推奨します。詳細については、を参照してください "マルチ管理者検証を有効にします"。

新規または既存のボリュームで**ARP**を有効にする

System ManagerまたはONTAP CLIを使用してARPを有効化できます。

System Manager

手順

1. [ストレージ]>[ボリューム]*を選択し、保護するボリュームを選択します。
2. [ボリューム]概要の*タブで[ステータス]*を選択し、[無効]から[有効]に切り替えます。

    ◦ (NAS 環境のみ) ONTAP 9.15.1 以前、またはFlexGroupボリュームを備えたONTAP 9.16.1 で ARP を使用している場合は、[**Anti-ransomware**] ボックスで [**Enabled in learning-mode**] を選択します。

    ONTAP 9 .13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、スイッチが自動化されます。ラーニングモードからアクティブモードへの移行を手動で制御することができます"関連付けられているStorage VMでこの設定を無効にしてください"。

    既存のボリュームでは、ラーニングモードとアクティブモードは新しく書き込まれたデータにのみ適用され、ボリューム内の既存のデータには適用されません。ARPを有効にしたボリュームでは、以前の通常のデータトラフィックの特性が新しいデータに基づいて想定されるため、既存のデータはスキャンおよび分析されません。

3. ボリュームのARP状態は、* Anti-ransomware *ボックスで確認できます。

    すべてのボリュームのARPステータスを表示するには、* Volumes ペインで Show/Hide を選択し、Anti-ransomware *ステータスがチェックされていることを確認します。

CLI

CLI を使用して ARP を有効にするプロセスは、既存のボリュームで有効にする場合と新しいボリュームで有効にする場合で異なります。

既存のボリュームで**ARP**を有効にする

1. 既存のボリュームを変更してランサムウェアからの保護を有効にします。

    ◦ ARP/AIのないNAS環境またはFlexGroupボリュームの場合は、 `dry-run`新しいボリュームが学習モードで開始されるように状態を設定します。

    ◦ ONTAP 9.16.1以降を実行しているNAS環境またはONTAP 9.17.1のSAN環境では、 `enabled`州。

    ```
    security anti-ransomware volume <dry-run|enabled> -volume
    <vol_name> -vserver <svm_name>
    ```

    の詳細については `security anti-ransomware volume dry-run`、を"ONTAPコマンド リファレンス"参照してください。

2. NAS環境をONTAP 9.13.1からONTAP 9.15.1にアップグレードし、デフォルトの状態が `dry-run` （学習モード）では、適応学習が有効になり、 `enabled`状態（アクティブモード）は自動的に行われます。この自動化を希望しない場合は、関連付けられているすべてのボリュームの設定をSVMレベルで変更します。

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning
-to-enabled false
```

3. ボリュームのARPの状態を確認します。

```
security anti-ransomware volume show
```

新しいボリュームで**ARP**を有効にする

1. データをプロビジョニングする前に、ARPを有効にして新しいボリュームを作成します。
   - ARP/AIのないNAS環境またはFlexGroupボリュームの場合は、 `dry-run`新しいボリュームが学習モードで開始されるように状態を設定します。
   - ONTAP 9.16.1以降を実行しているNAS環境またはONTAP 9.17.1のSAN環境では、 `enabled`州。

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state <dry-run|enabled>
-junction-path </path_name>
```

2. NAS環境をONTAP 9.13.1からONTAP 9.15.1にアップグレードし、デフォルトの状態が `dry-run` （学習モード）では、適応学習が有効になり、 `enabled`状態（アクティブモード）は自動的に行われます。この自動化を希望しない場合は、関連付けられているすべてのボリュームの設定をSVMレベルで変更します。

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning
-to-enabled false
```

3. ボリュームが状態に設定されていることを確認します `enabled`。

```
security anti-ransomware volume show
```

の詳細については `security anti-ransomware volume show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "学習期間後にアクティブモードに切り替える"

新しいボリュームで**ONTAP Autonomous Ransomware Protection**をデフォルトで有効にする

ONTAP 9 .10.1以降では、Autonomous Ransomware Protection（ARP；自律型ランサム

ウェア対策）で新しいボリュームがデフォルトで有効になるようにStorage VM（SVM）を設定できます。この設定は、System ManagerまたはCLIを使用して変更できます。

デフォルトのARPを設定せずに新規または既存のボリュームを個別に設定する場合は、こちらを参照してください"関連するARP手順"。

タスクの内容

デフォルトでは、新しいボリュームはARPが無効モードに設定された状態で作成されます。ランサムウェア対策機能を有効にした後、SVM で作成された新しいボリュームでは、ARP がデフォルトでのみ有効になります。

既存のボリュームでは、ARPは自動的に有効になりません。この手順で説明する設定変更は、新しいボリュームにのみ適用されます。 "既存のボリュームのARPを有効にする" 。

- （**SAN**環境のみ） **FlexVol**を備えた**ONTAP 9.17.1**以降の場合 System ManagerまたはCLIを使用してARPを有効にすると、ARP/AI機能が自動的に有効になります。SANボリュームで有効にすると、 "ARP/AIは評価期間中にデータを継続的に監視します"ワークロードが ARP に適しているかどうかを判断し、検出に最適な暗号化しきい値を設定します。
- **(NAS** 環境のみ**) FlexVol**ボリュームを備えた**ONTAP 9.16.1** 以降の場合 System Manager または CLI を使用して ARP を有効にすると、ARP/AI 保護が有効になり、すぐにアクティブになります。学習期間は必要ありません。
- **(NAS**環境のみ**) ONTAP 9.15.1**～**9.10.1**または**FlexGroup**ボリュームの**ARP**の場合 デフォルトでは、ARPが有効になっている新しいボリュームは次のように設定されます。 "ラーニングモード" （または「ドライラン」状態）では、システムはワークロードを分析して通常の動作を特徴付けます。学習モードからアクティブ モードには、手動（すべてのARPバージョン）または自動（ARP 9.13.1以降）で移行できます。ARP 9.13.1以降、アダプティブ ラーニングがARP分析に追加され、学習モードからアクティブ モードへの切り替えは自動的に行われます。

開始する前に

- その"正しいライセンス" ONTAPバージョンに合わせてインストールする必要があります。
- ボリュームの使用率は 100% 未満である必要があります。
- （NAS環境のみ）ARPを設定するボリュームは保護されており、アクティブな"ジャンクションパス" 。
- ONTAP 9.13.1 以降では、ランサムウェア対策操作に 2 人以上の認証済みユーザー管理者が必要となるように、マルチ管理者検証 (MAV) を有効にすることをお勧めします。"詳細" 。

手順

System ManagerまたはONTAP CLIを使用して、新しいボリュームに対してデフォルトでARPを有効にすることができます。

System Manager

1. ストレージ*または*クラスター（環境によって異なります）を選択し、ストレージ **VM** を選択して、ARP で保護するボリュームが含まれているストレージ VM を選択します。
2. *設定*タブに移動します。*セキュリティ*の下にある*ランサムウェア対策*タイルを見つけて選択します。 。
3. ランサムウェア対策（ARP）を有効にするには、チェックボックスをオンにします。ストレージVM内のすべての対象ボリュームでARPを有効にするには、追加のチェックボックスをオンにします。
4. ONTAP 9.13.1 以降の場合は、オプションで「十分な学習が完了したら、学習モードからアクティブモードに自動的に切り替える」を選択します。そのため、ARPが最適な学習期間を判断して自動的にアクティブ モードへ切り替わります。

CLI

- 既存のSVMを変更して、新しいボリュームでデフォルトでARPを有効にします。
  - ARP/AIのないNAS環境またはFlexGroupボリュームの場合は、 `dry-run`新しいボリュームが学習モードで開始されるように状態を設定します。
  - ONTAP 9.16.1以降を実行しているNAS環境またはONTAP 9.17.1のSAN環境では、 `enabled`州。

```
vserver modify -vserver <svm_name> -anti-ransomware-default
-volume-state <dry-run|enabled>
```

- 新しいボリュームに対してデフォルトでARPを有効にして、新しいSVMを作成します。
  - ARP/AIのないNAS環境またはFlexGroupボリュームの場合は、 `dry-run`新しいボリュームが学習モードで開始されるように状態を設定します。
  - ONTAP 9.16.1以降を実行しているNAS環境またはONTAP 9.17.1のSAN環境では、 `enabled`州。

```
vserver create -vserver <svm_name> -anti-ransomware-default
-volume-state <dry-run|enabled>
```

- ONTAP 9.13.1からONTAP 9.15.1にアップグレードし、デフォルトの状態が `dry-run` （学習モード）では、適応学習が有効になり、 `enabled`状態（アクティブモード）は自動的に行われます。この動作を自動的に有効にしない場合は、既存のSVMを変更します。

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning
-to-enabled false
```

- ARPが有効なボリュームの状態が表示されることを確認します `enabled`。

```
security anti-ransomware volume show
```

の詳細については `security anti-ransomware volume show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "学習期間後にアクティブモードに切り替える"

ONTAP ARP/AIを有効にする

ONTAP 9.16.1以降、ARPは人工知能を利用した自律型ランサムウェア対策（ARP/AI）を導入し、脅威の検出と対応を強化しています。クラスタをONTAP 9.17.1（SANの場合）またはONTAP 9.16.1（NASの場合）にアップグレードすると、 FlexVolでARPがすでに有効になっている場合、ARP/AIが自動的に有効になります。ARPが"自動更新"クラスターの場合は、この手順で説明されているシナリオのいずれかに従う必要があります。

ARP/AIサポート付きのONTAPバージョンにアップグレードする前に、 "既存のARP検出をすべて終了します。" 。

開始する前に

- ARP/AIを使用するには、FlexVolが必要です。FlexGroupボリュームがある場合、ARP/AI より前に使用されていた ARP モデルは、 ONTAP 9.16.1 以降にアップグレードした後も引き続き動作します。

（NAS環境のみ） ONTAP 9.16.1以降にアップグレードすると、 FlexVolを持つ既存のARPインスタンスでARPが自動的に有効化され、アクティブになります。ARP/AIは広範な機械学習モデルでトレーニングされているため、学習期間が不要になります。アップグレード前に完了していなかった学習期間は自動的に終了し、ボリュームはアクティブARP/AIに移行します。

手順

1. 使用している構成に固有のシナリオに従います。
   - **SAN**環境のみ
     - * ONTAP 9.17.1以降でFlexVolボリュームを実行している新規および既存のクラスタの場合*: ONTAP 9.17.1以降にアップグレードまたはインストールする場合は、 "ARPを有効にする"保護対象のボリュームでARPを有効にします。System ManagerまたはCLIを使用してARPを有効にすると、ARP/AI機能も自動的に有効になります。SANボリュームで有効にすると、 "ARP/AIは評価期間中にデータを継続的に監視します"ワークロードが ARP に適しているかどうかを判断し、検出に最適な暗号化しきい値を設定します。
   - **NAS**環境のみ
     - *ONTAP9.16.1以降をFlexVolボリューム*で実行している新しいクラスタの場合： "ARPの有効化"。ARPはデフォルトでは有効になっていません。ARP を有効にすると、保護対象として選択したFlexVolボリュームで ARP/AI 機能が自動的に有効になります
     - * ONTAP 9.16.1以降に最近アップグレードされ、ARPが有効になっている既存のクラスタの場合*：操作は不要です。保護対象として選択したFlexVolでは、ARP/AIが自動的に脅威保護の新しいARP方式になります。
     - 最近**ONTAP9.16.1**以降にアップグレードされた既存のクラスタで、**ARP**が有効になっていない場合： "ARPの有効化"。ARP/AI は自動的に脅威保護の新しい ARP 方式になります。

2. ARP/AI を有効にした後、ARP/AI 保護の更新を配信してインストールするかどうかを決定します。 "自動または手動" 。

関連情報

- "ARP / AIの更新"

AI（ARP / AI）でONTAP自律型ランサムウェア対策を更新

最新のランサムウェアの脅威に対する保護を最新の状態に保つために、ARP / AIでは、通常のONTAPリリースサイクル外に発生する自動更新を提供しています。

ONTAP 9.16.1以降では、システムおよびファームウェアの更新に加えて、ARP/AIのセキュリティ更新もSystem Managerのソフトウェア ダウンロードから入手できます。ONTAPクラスタがすでに登録されている場合"システムとファームウェアの自動更新" ARP/AIセキュリティアップデートが利用可能になると自動的に通知されます。また、 更新設定 ONTAP がセキュリティ更新を自動的にインストールできるようにします。

必要に応じて、ARP / AIを手動で更新するNetAppサポートサイトから更新プログラムをダウンロードし、System Managerを使用してインストールできます。

タスクの内容

ARP/AI は System Manager を使用してのみ更新できます。

ARP/AIのアップデート設定を選択してください

システムマネージャでは、セキュリティファイルの自動更新を有効にするページの設定は次のように設定されています。 `Show notifications`ファームウェアとシステムの自動アップデートにすでに登録されている場合は、アップデート設定を変更して `Automatically update` ONTAP で最新のアップデートを自動的に適用したい場合。ダーク サイトを使用している場合や、更新を手動で実行する場合は、通知を表示するか、セキュリティ更新を自動的に却下するかを選択できます。

開始する前に

自動セキュリティ更新の場合は、を"AutoSupportとAutoSupport OnDemandを有効にし、転送プロトコルをHTTPSに設定する必要があります。"参照してください。

手順

1. System Managerで、*[クラスタ]>[設定]>[ソフトウェアの更新]*をクリックします。
2. [ソフトウェアの更新]*セクションで、を選択します→。
3. [ソフトウェアの更新]ページで、[その他のすべての更新]タブを選択します。
4. [その他のすべての更新]タブを選択し、*[詳細]*をクリックします。
5. [自動更新設定の編集]*を選択します。
6. [自動更新の設定]ページで、*[セキュリティファイル]*を選択します。
7. セキュリティファイル（ARP/AIアップデート）に対して実行するアクションを指定します。

   自動的に更新するか、通知を表示するか、または更新を自動的に却下するかを選択できます。

セキュリティ更新が自動的に更新されるようにするには、AutoSupportおよびAutoSupport OnDemandを有効にし、転送プロトコルをHTTPSに設定する必要があります。

8. 利用条件に同意し、*[保存]*を選択します。

最新のセキュリティパッケージを使用して**ARP/AI**を手動で更新する

Active IQ Unified Managerに登録しているかどうかに応じて、適切な手順を実行します。

意図しないARPダウングレードを避けるために、現在のバージョンよりも新しいARPアップデートのみをインストールしてください。

デジタルアドバイザ搭載の**ONTAP 9 .16.1**以降

1. System Managerで、*[ダッシュボード]*に移動します。

   クラスタに対して推奨されるセキュリティ更新プログラムがある場合は、* Health *セクションにメッセージが表示されます。

2. アラートメッセージをクリックします。
3. 推奨される更新プログラムのリストのセキュリティ更新プログラムの横にある*[アクション]*を選択します。
4. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。

   更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。

ONTAP 9 .16.1以降（デジタルアドバイザなし）

1. に移動"NetAppサポートサイト"してログインします。
2. プロンプトに従って、クラスタのARP / AIの更新に使用するセキュリティパッケージをダウンロードします。
3. ネットワーク上のHTTPサーバまたはFTPサーバ、またはARP / AIを使用してクラスタからアクセスできるローカルフォルダにファイルをコピーします。
4. System Managerで、*[クラスタ]>[設定]>[ソフトウェアの更新]*をクリックします。
5. で、[その他のすべての更新]*タブを選択します。
6. [手動アップデート]ペインで、*[セキュリティファイルの追加]*をクリックし、次のいずれかの環境設定を使用してファイルを追加します。
   - サーバからダウンロード:セキュリティファイルパッケージのURLを入力します。
   - ローカルクライアントからアップロード：ダウンロードしたTGZファイルに移動します。

   ファイル名がで始まり、がファイル拡張子である `.tgz` ことを確認します `ontap_security_file_arpai_`。

7. [追加]*をクリックして更新を適用します。

ARP / AIの更新を確認

却下された、またはインストールに失敗した自動更新の履歴を表示するには、次の手順を実行します。

1. System Managerで、*[クラスタ]>[設定]>[ソフトウェアの更新]*をクリックします。
2. [ソフトウェアの更新]*セクションで、を選択します→。
3. [ソフトウェアの更新]ページで、**[**その他のすべての更新**]***タブを選択し、[詳細]*をクリックします。
4. [すべての自動更新を表示]*を選択します。

関連情報

- "ARP / AIを有効にする"
- "ソフトウェアアップデートのEメール配信登録"

学習期間後に**ONTAP ARP**でアクティブモードに切り替える

NAS環境では、ARP対応ボリュームを学習モードからアクティブモードに手動または自動で切り替えます。ONTAP9.15.1以前でARPを使用している場合、またはFlexGroupボリュームでARPを実行している場合は、モードを切り替える必要があります。

ARPが推奨される最低30日間の学習モードの実行を完了したら、手動でアクティブ モードに切り替えることができます。ONTAP 9.13.1以降では、ARPによって最適な学習期間が自動的に決定され、30日が経過しなくても自動的に切り替えが行われる場合があります。

ONTAP 9.16.1以降のFlexVolボリュームでARPを使用している場合は、ARP / AI保護が有効になり、自動的にアクティブになります。学習期間は必要ありません。

> ⓘ 既存のボリュームでは、ラーニングモードとアクティブモードは新しく書き込まれたデータにのみ適用され、ボリューム内の既存のデータには適用されません。ARPを有効にしたボリュームでは、以前の通常のデータトラフィックの特性が新しいデータに基づいて想定されるため、既存のデータはスキャンおよび分析されません。

学習期間後に手動でアクティブモードに切り替える

ONTAP 9.10.1 ～ 9.15.1 およびFlexGroupボリュームを使用した ARP の場合、学習期間の完了後、System Manager またはONTAP CLI を使用して、ARP 学習モードからアクティブ モードに手動で移行できます。

タスクの内容

この手順で説明する学習期間後のアクティブ モードへの手動移行は、NAS 環境に固有のものです。

手順

System Manager またはONTAP CLI を使用して、学習モードからアクティブ モードに切り替えることができます。

System Manager

1. [ストレージ]>[ボリューム]*を選択し、アクティブモードにする準備ができたボリュームを選択します。
2. [Volumes]概要の*タブで、**[Anti-ransomware]**ボックスで[Switch to active mode]*を選択します。
3. ボリュームのARP状態は、* Anti-ransomware *ボックスで確認できます。

CLI

1. 保護されたボリュームを変更してアクティブ モードに切り替えます (まだ自動的に行われていない場合)。

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

modify volumeコマンドを使用して、アクティブ モードに切り替えることもできます。

```
volume modify -volume <vol_name> -vserver <svm_name> -anti
-ransomware-state enabled
```

2. ボリュームのARPの状態を確認します。

```
security anti-ransomware volume show
```

学習モードからアクティブモードへの自動切り替え

ONTAP 9.13.1以降、アダプティブ ラーニングがARP分析に追加され、学習モードからアクティブ モードへの切り替えは自動的に行われます。学習モードからアクティブ モードへARPを自動で切り替えるかどうかは、次のオプションの設定に基づいて決まります。

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

自動切り替えが有効になっている場合、すべての条件が満たされていなくても、最大30日後にボリュームは自動的にアクティブモードに切り替わります。この30日間の制限は固定されており、変更できません。

デフォルト値を含むARP設定オプションの詳細については、を参照してください"ONTAPコマンド リファレンス"。

関連情報

- "セキュリティ ランサムウェア対策 ボリューム"

SANボリュームのONTAP ARP評価期間について学ぶ

ONTAP 9.17.1以降、ARPはSANボリュームのワークロードのエントロピーレベルがランサムウェア保護に適しているかどうかを判断するために評価期間を必要とします。SANボリュームでARPを有効にすると、評価期間中にデータを継続的に監視し、最適な暗号化しきい値を決定します。ARPは評価対象のSANボリューム内の適切なワークロードと不適切なワークロードを区別し、ワークロードが保護に適していると判断された場合は、評価期間の統計に基づいて暗号化しきい値を自動的に設定します。

エントロピー評価を理解する

システムは10分間隔で継続的に暗号化統計を収集します。評価中は、ARP 定期スナップショットも 4 時間ごとに継続的に作成されます。一定間隔内の暗号化率がこのボリュームに対して特定された最適な暗号化しきい値を超えると、アラートがトリガーされ、 `Anti_ransomware_attack_backup`スナップショットが作成され、定期的な ARP スナップショットでスナップショットの保持時間が延長されます。

評価期間が有効であることを確認する

以下のコマンドを実行し、以下のステータスを確認することで、評価が有効であることを確認できる `evaluation_period`。ボリュームが評価対象外の場合、評価ステータスは表示されません。

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

応答例:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : evaluation_period
```

評価期間のデータ収集を監視する

次のコマンドを実行することで、暗号化検出をリアルタイムで監視できます。このコマンドは、暗号化率の各範囲におけるデータ量を示すヒストグラムを返します。ヒストグラムは10分ごとに更新されます。

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

応答例:

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

適切な作業負荷と適応閾値

評価は次のいずれかの結果で終了します。

- このワークロードは**ARP**に適しています。ARPは、評価期間中に観測された最大暗号化率の10%を超える値に適応しきい値を自動的に設定します。また、ARPは統計情報の収集を継続し、定期的にARPスナップショットを作成します。
- ワークロードは**ARP**に適していません。ARPは、評価期間中に確認された最大の暗号化率に適応しきい値を自動的に設定します。また、ARPは統計情報の収集を継続し、定期的にARPスナップショットを作成しますが、最終的にはボリューム上でARPを無効にすることを推奨します。

評価結果を決定する

評価期間が終了すると、ARP は評価結果に基づいて適応しきい値を自動的に設定します。

次のコマンドを実行することで評価結果を確認できます。ボリュームの適合性は、 `Block device detection status`分野：

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

応答例:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

評価の結果として採用された値のしきい値を表示することもできます。

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

応答例:

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

ONTAP Autonomous Ransomware Protectionを一時停止して、ワークロードイベントを分析対象から除外する

異常なワークロードイベントが発生する可能性がある場合は、Autonomous Ransomware Protection（ARP）分析をいつでも一時的に中断して再開できます。

ONTAP 9.13.1以降では、マルチ管理者検証（MAV）をイネーブルにして、複数の認証済みユーザ管理者がARPを一時停止する必要があります。

"MAVの詳細については、こちらをご覧ください"です。

タスクの内容

ARP の一時停止中は、新しい書き込みのイベントやアクションは記録されませんが、以前のログの分析操作はバックグラウンドで継続されます。

ARP無効機能を使用して分析を一時停止しないでください。これにより、ボリュームのARPが無効になり、学習したワークロードの動作に関する既存の情報がすべて失われます。これには、学習期間の再起動が必要になります。

手順

ARPは、System ManagerまたはONTAP CLIを使用して一時停止できます。

System Manager

1. [ストレージ]>[ボリューム]*を選択し、ARPを一時停止するボリュームを選択します。
2. ボリュームの概要の セキュリティ タブで、ランサムウェア対策 ボックスの ランサムウェア対策の一時停止 を選択します。

> ONTAP 9 .13.1以降では、MAVを使用してARP設定を保護している場合、一時停止操作によって、1人以上の追加管理者の承認を得るように求められます。"すべての管理者から承認を受ける必要があります"MAV承認グループに関連付けられているか、操作が失敗します。

3. 監視を再開するには、「ランサムウェア対策を再開」を選択します。

CLI

1. ボリュームでARPを一時停止します。

```
security anti-ransomware volume pause -vserver <svm_name> -volume
<vol_name>
```

2. 処理を再開するには、次のコマンドを使用し `resume`ます。

```
security anti-ransomware volume resume -vserver <svm_name> -volume
<vol_name>
```

の詳細については `security anti-ransomware volume`、を"ONTAPコマンド リファレンス"参照してください。

3. ONTAP 9設定を保護するためにMAV（ARP .13.1以降で使用可能）を使用している場合は、一時停止操作によって、1人以上の追加管理者の承認を得るように求められます。MAV承認グループに関連付けられているすべての管理者から承認を受ける必要があります。そうしないと、操作が失敗します。

   MAVを使用していて、予定されている一時停止操作で追加の承認が必要な場合は、各MAVグループ承認者が次の処理を行います。

   a. 要求を表示します。

```
security multi-admin-verify request show
```

   b. 要求を承認します。

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

   最後のグループの承認者には、ボリュームが変更され、ARPが一時停止状態になった旨の応答が

返されます。

MAVを使用していて、MAVグループの承認者である場合、一時停止処理の要求を却下できます。

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

+
の詳細については `security multi-admin-verify request`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP自律型ランサムウェア対策攻撃検出パラメータの管理

ONTAP 9.11.1以降では、Autonomous Ransomware Protectionが有効になっている特定のボリュームでランサムウェア検出のパラメータを変更し、通常のファイルアクティビティとして既知の急増を報告できます。検出パラメータを調整すると、特定のボリュームワークロードに基づいてレポートの精度が向上します。

攻撃検出の仕組み

自律ランサムウェア保護（ARP）が学習モードまたは評価モードにある場合、ボリュームの動作に関するベースライン値を作成します。これには、エントロピー、ファイル拡張子、そしてONTAP 9.11.1以降ではIOPSが含まれます。設定されたベースラインは、ランサムウェアの脅威を評価するために使用されます。"ARPが検出する内容" 。

特定のボリュームやワークロードでは、異なる検出パラメータが必要です。たとえば、ARP対応ボリュームで多数の種類のファイル拡張子がホストされている場合、以前に見たことのないファイル拡張子のしきい値をデフォルトの20よりも大きい値に変更したり、以前に見たことのないファイル拡張子に基づいて警告を無効にしたりすることができます。ONTAP 9 .11.1以降では、攻撃検出パラメータを変更して、特定のワークロードに適したパラメータにすることができます。

ONTAP 9.14.1以降では、ARPが新しいファイル拡張子を監視したとき、およびARPがスナップショットを作成したときにアラートを設定できます。詳細については、を参照してください [modify-alerts]。

NAS環境における攻撃検出

ONTAP 9 .10.1では、次の両方の条件が検出されると、ARPは警告を発行します。

- 以前にボリュームで認識されなかったファイル拡張子を持つファイルが20個を超える
- 高エントロピーデータ

ONTAP 9.11.1以降では、_only_oneの条件が満たされた場合にARPから脅威警告が発行されます。たとえば、ボリュームで以前に観察されたことがないファイル拡張子を持つ20を超えるファイルが24時間以内に観察された場合、ARPはこれをthreat_expendered_of observed entropyに分類します。24時間と20ファイルの値はデフォルトであり、変更可能です。

誤検知アラートの数を減らすには、「ストレージ」>「ボリューム」>「セキュリティ」>「ワークロード特性の設定」に移動し、「新しいファイルタイプの監視」を無効にしてください。この設定は、 ONTAP 9.14.1 P7、9.15.1 P1、9.16.1以降ではデフォルトで無効になっています。

SAN環境における攻撃検出

ONTAP 9.17.1以降、ARPは自動的に学習されたしきい値を超える高い暗号化レートを検出すると警告を発します。このしきい値は、 "評価期間"ただし変更可能です。

攻撃検出パラメータの変更

ARP 対応ボリュームの予想される動作に応じて、攻撃検出パラメータを変更する必要がある場合があります。

手順

1. 既存の攻撃検出パラメータを表示します。

```
security anti-ransomware volume attack-detection-parameters show
-vserver <svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                              Vserver Name : vs1
                                               Volume Name : vol1
           Block Device Auto Learned Encryption Threshold : 10
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                 Is Detection Based on File Create Rate? : true
                 Is Detection Based on File Rename Rate? : true
                 Is Detection Based on File Delete Rate? : true
          Is Detection Relaxing Popular File Extensions? : true
               High Entropy Data Surge Notify Percentage : 100
                File Create Rate Surge Notify Percentage : 100
                File Rename Rate Surge Notify Percentage : 100
                File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. 表示されているすべてのフィールドはブール値または整数値で変更できます。フィールドを変更するには、 `security anti-ransomware volume attack-detection-parameters modify`指示。

   の詳細については `security anti-ransomware volume attack-detection-parameters modify`、を"ONTAPコマンド リファレンス"参照してください。

既知のサージを報告

ARPは、アクティブな場合でも、検出パラメータのベースライン値の変更を継続します。ボリュームアクティビティのサージ（1回限りのサージ、またはニューノーマルの特徴であるサージ）を知っている場合は、それらを安全であると報告する必要があります。これらの急増を安全として手動で報告することは、ARPの脅威評価の精度を向上させるのに役立ちます。

1回限りの急増を報告する

1. 既知の状況で1回限りのサージが発生していて、ARPで将来の状況でも同様のサージを報告する場合は、ワークロードの動作からサージをクリアします。

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   <svm_name> -volume <volume_name>
   ```

   の詳細については `security anti-ransomware volume workload-behavior clear-surge`、を"ONTAPコマンド リファレンス"参照してください。

ベースラインサージの修正

1. 報告されたサージを通常のアプリケーション動作と見なす必要がある場合は、サージを報告してベースラインサージ値を変更します。

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver <svm_name> -volume <volume_name>
   ```

   詳細はこちら `security anti-ransomware volume workload-behavior update-baseline-from-surge`の中で"ONTAPコマンド リファレンス" 。

ARPアラートの設定

ONTAP 9.14.1以降では、ARPで2つのARPイベントのアラートを指定できます。

- ボリューム上の新しいファイル拡張子の観測
- ARPスナップショットの作成

これら2つのイベントのアラートは、個々のボリュームかSVM全体に対して設定できます。SVMでアラートを有効にした場合、アラートの設定は、アラートを有効にしたあとに作成されたボリュームにのみ継承されます。デフォルトでは、アラートはどのボリュームでも有効になっていません。

イベント アラートは、マルチ管理者認証で制御できます。詳細については、 "ARPで保護されたボリュームを使用したマルチ管理者検証" 。

手順

System Manager またはONTAP CLI を使用して、ARP イベントのアラートを設定できます。

System Manager

ボリュームのアラートの設定

1. *ボリューム*に移動します。設定を変更するボリュームを個別に選択します。
2. *セキュリティ*タブを選択し、次に*イベントの重大度設定*を選択します。
3. 新しいファイル拡張子の検出*および*ランサムウェアのスナップショットの作成*に関するアラートを受信するには、「*重大度」の見出しの下にあるドロップダウンメニューを選択します。設定を「イベントを生成しない」から「通知」に変更します。
4. [保存（ Save ）] を選択します。

SVMのアラートを設定する

1. ストレージ **VM** に移動し、設定を有効にする SVM を選択します。
2. 「セキュリティ」の見出しの下にある「ランサムウェア対策」カードを⋮次に*ランサムウェア イベントの重大度を編集*します。
3. 新しいファイル拡張子の検出*および*ランサムウェアのスナップショットの作成*に関するアラートを受信するには、「*重大度」の見出しの下にあるドロップダウンメニューを選択します。設定を「イベントを生成しない」から「通知」に変更します。
4. [保存（ Save ）] を選択します。

CLI

ボリュームのアラートの設定

- 新しいファイル拡張子にアラートを設定するには、次の手順を実行します。

```
security anti-ransomware volume event-log modify -vserver <svm_name> -is
-enabled-on-new-file-extension-seen true
```

- ARPスナップショットの作成に関するアラートを設定するには、次の手順を実行します。

```
security anti-ransomware volume event-log modify -vserver <svm_name> -is
-enabled-on-snapshot-copy-creation true
```

- コマンドを使用して設定を確認し `anti-ransomware volume event-log show`ます。

SVMのアラートを設定する

- 新しいファイル拡張子にアラートを設定するには、次の手順を実行します。

```
security anti-ransomware vserver event-log modify -vserver <svm_name> -is
-enabled-on-new-file-extension-seen true
```

- ARPスナップショットの作成に関するアラートを設定するには、次の手順を実行します。

```
security anti-ransomware vserver event-log modify -vserver <svm_name> -is
-enabled-on-snapshot-copy-creation true
```

- コマンドを使用して設定を確認し `security anti-ransomware vserver event-log show`ます。

詳細はこちら `security anti-ransomware vserver event-log`コマンド"ONTAPコマンド リファレンス" 。

関連情報

- "Autonomous Ransomware Protection AttacksとAutonomous Ransomware Protectionのスナップショットについて理解する"です。
- "ONTAPコマンド リファレンス"

ONTAP ARPによって検出された異常なアクティビティへの対応

Autonomous Ransomware Protection（ARP）は、保護されたボリューム内の異常なアクティビティを検出すると警告を発行します。通知を評価して、アクティビティが許容可能か（false positive）、または攻撃が悪意のあるものと思われるかどうかを判断する必要があります。攻撃を分類したら、疑わしいファイルに関する警告と通知をクリアできます。

攻撃を分類すると、ARP スナップショットは、分類操作によって開始された短縮期間にわたって保持されるか（ONTAP 9.16.1 以降）、または即座に削除されます（ONTAP 9.15.1 以前）。

ONTAP 9.11.1以降では、 "保持設定" ARP スナップショット用。

タスクの内容

ARPは、データ エントロピーの上昇、データ暗号化に関連した異常なボリューム アクティビティ、および一般的でないファイル拡張子のいくつかを検出すると、疑わしいファイルのリストを表示します。ONTAP 9.17.1 以降では、NAS 環境と SAN 環境の両方で、エントロピー スパイクの詳細が System Manager の Anti-ransomware ページでも報告されるようになりました。

ARP 警告通知が発行された場合は、次の 2 つの方法のいずれかでアクティビティを指定して応答します。

- 偽陽性

  特定されたファイル タイプまたはエントロピー スパイクはワークロードで予期されるものであり、無視できます。

- ランサムウェア攻撃の可能性

  特定されたファイル タイプまたはエントロピー スパイクはワークロードでは予期されないものであり、潜在的な攻撃として扱う必要があります。

決定を更新し、ARP 通知をクリアすると、通常の監視が再開されます。ARPは、脅威評価プロファイルに評価を記録し、選択した評価に基づいて、後続のファイル アクティビティを監視します。

攻撃の疑いがある場合は、通知をクリアする前に、攻撃であるかどうかを確認し、攻撃である場合はそれに対応し、保護されたデータを復元する必要があります。"ランサムウェア攻撃から回復する方法の詳細をご覧ください"です。

ボリューム全体をリストアする場合、クリアする通知はありません。

開始する前に

ARP はボリュームをアクティブに保護している必要があり、学習モードや評価モードであってはなりません。

手順

System ManagerまたはONTAP CLIを使用して、異常なアクティビティに対応できます。

System Manager

1. 異常なアクティビティに関する通知を受け取ったら、リンクをクリックします。または、*ボリューム*概要の*セキュリティ*タブに移動します。

   警告は*メニューの[概要]*ペインに表示されます。

2. セキュリティ タブで、疑わしいファイルの種類またはエントロピー スパイクのレポートを確認します。
   - 疑わしいファイルについては、[疑わしいファイルの種類] ダイアログ ボックスで各ファイルの種類を調べ、それぞれを個別にマークします。
   - エントロピーの急上昇については、エントロピー レポートを調べます。
3. 応答を記録します:

この値を選択した場合…	対処方法
誤検出	a. 次のいずれかを実行します。 ◦ ファイル タイプに関する警告の場合は、[疑わしいファイル タイプを更新してクリアする] を選択します。 ◦ エントロピースパイクの場合は、「誤検知としてマーク」を選択します。 これらのアクションにより、疑わしいファイルまたはアクティビティに関する警告通知がクリアされます。その後、ARPはボリュームの通常の監視を再開します。ONTAP9.16.1以降のONTAP /AIでは、分類操作によってトリガーされた短縮された保持期間の経過後に、ARPスナップショットは自動的に削除されます。9.15.1以前のバージョンでは、疑わしいファイルタイプをクリアすると、関連するARPスナップショットが自動的に削除されますONTAP ONTAP 9 .13.1以降では、MAVを使用してARP設定を保護している場合、clear-suspect操作によって、1人以上の追加管理者の承認を得るように求められます。"すべての管理者から承認を受ける必要があります"MAV承認グループに関連付けられているか、操作が失敗します。

ランサムウェア攻撃の可能性	a. 攻撃に応答する: ◦ ファイルタイプの警告については、選択したファイルを*潜在的なランサムウェア攻撃*としてマークし、"保護されたデータのリストア"。 ◦ 攻撃を示唆するエントロピースパイクの場合は、「潜在的なランサムウェア攻撃としてマーク」を選択し、"保護されたデータのリストア"。 b. データの復元が完了したら、決定を記録し、通常の ARP 監視を再開します。 ◦ ファイル タイプに関する警告の場合は、[疑わしいファイル タイプを更新してクリアする] を選択します。 ◦ エントロピースパイクの場合は、「潜在的なランサムウェア攻撃としてマーク」を選択し、「保存して閉じる」を選択します。 ボリューム全体を復元した場合、クリアする必要がある疑わしいファイル タイプ通知はありません。 決定を記録すると、攻撃レポートがクリアされます。ONTAP9.16.1以降のONTAP /AIでは、分類操作によってトリガーされた短縮された保持期間の経過後に、ARPスナップショットは自動的に削除されます。9.15.1以前では、ボリュームをリストアするとARPスナップショットは自動的に削除されますONTAP

CLI

1. ランサムウェア攻撃の疑いがあるという通知を受け取ったら、攻撃の時間と重大度を確認します。

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

出力例：

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

EMSメッセージを確認することもできます。

```
event log show -message-name callhome.arw.activity.seen
```

2. 攻撃レポートを生成し、保存場所を指定します。

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

コマンド例：

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

出力例：

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. 管理クライアントシステムでレポートを表示します。例：

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

4. ファイル拡張子またはエントロピー スパイクの評価に基づいて、次のいずれかのアクションを実行します。

◦ False positive

決定を記録し、通常の Autonomous Ransomware Protection 監視を再開するには、次のいずれかのコマンドを実行します。

▪ ファイル拡張子の場合:

```
anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> [<extension_identifiers>] -false
-positive true
```

特定の拡張子のみをfalse positiveとして識別するには、次のオプションパラメータを使用します。

▪ `[-extension <text>, … ]`:ファイル拡張子

▪ エントロピースパイクの場合:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
```

- ランサムウェア攻撃の可能性

  攻撃に対応し "ARPによって作成されたバックアップスナップショットからデータをリカバリします".データが回復されたら、次のコマンドのいずれかを実行して決定を記録し、通常の ARP 監視を再開します

  - ファイル拡張子の場合:

    ```
    anti-ransomware volume attack clear-suspect -vserver
    <svm_name> -volume <vol_name> [<extension identifiers>] -false
    -positive false
    ```

    特定の拡張機能のみをランサムウェアの可能性があると特定するには、次のオプションパラメータを使用します。

    - `[-extension <text>, … ]`:ファイル拡張子

  - エントロピースパイクの場合:

    ```
    security anti-ransomware volume attack clear-suspect -vserver
    <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
    HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
    false
    ```

これ `clear-suspect`操作により攻撃レポートがクリアされます。ボリューム全体をリストアした場合、クリアする疑わしいファイルタイプの通知はありません。ONTAP9.16.1以降のONTAP /AIでは、分類操作によってトリガーされた短縮された保持期間の経過後に、ARPスナップショットは自動的に削除されます。9.15.1以前では、ボリュームをリストアするか疑わしいイベントをクリアすると、ARPスナップショットは自動的に削除されますONTAP

5. MAVを使用していて、想定される操作に追加の承認が必要な場合 `clear-suspect`、各MAVグループ承認者は次の作業を行う必要があります。

   a. 要求を表示します。

   ```
   security multi-admin-verify request show
   ```

   b. 通常のランサムウェア対策監視の再開要求を承認します。

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

最後のグループ承認者に対する応答は、ボリュームが変更され、誤検出が記録されたことを示します。

6. MAVを使用していて、MAVグループ承認者である場合は、疑わしいリクエストを却下することもできます。

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

関連情報

- "NetAppナレッジベース: Autonomous Ransomware Protection 攻撃と Autonomous Ransomware Protection スナップショットについて"
- "自動スナップショットオプションを変更します。"
- "セキュリティ ランサムウェア対策 ボリューム"
- "セキュリティ マルチ管理者検証リクエスト"

ランサムウェア攻撃後にONTAP ARPスナップショットからデータをリストア

Autonomous Ransomware Protection (ARP) は、潜在的なランサムウェアの脅威から保護するためのスナップショットを作成します。これらのARP Snapshotのいずれかまたはボリュームの別のSnapshotを使用して、データをリストアできます。

タスクの内容

ARP は、次のいずれかの名前を先頭に付けたスナップショットを作成します。

- `Anti_ransomware_periodic_backup` : ONTAP 9.17.1以降で、定期的に作成されるスナップショットに使用されます。例： `Anti_ransomware_periodic_backup.2025-06-01_1248` 。
- `Anti_ransomware_attack_backup`: ONTAP 9.17.1 以降で、異常発生時に作成されるスナップショットに使用されます。例： `Anti_ransomware_attack_backup.2025-08-25_1248` 。
- `Anti_ransomware_backup` : ONTAP 9.16.1以前で、異常発生時に作成されるスナップショットで使用されます。例： `Anti_ransomware_backup.2022-12-20_1248` 。

スナップショット以外のものから復元するには `Anti_ransomware`システム攻撃が特定された後にスナップショットを作成する場合は、まず ARP スナップショットを解放する必要があります。

システム攻撃が報告されていない場合は、まず `Anti_ransomware`スナップショットを作成し、選択したスナップショットからボリュームの後続の復元を完了します。

ARP保護されたボリュームがSnapMirror関係の一部である場合、スナップショットから復元した後、ボリュームのすべてのミラーコピーを手動で更新する必要があります。この手順を省略すると、ミラーコピーが使用できなくなり、削除して再作成する必要が生じる可能性があります。

開始する前に

"攻撃を潜在的なランサムウェア攻撃としてマークする必要があります"スナップショットからデータを復元する前に。

手順

データは、System ManagerまたはONTAP CLIを使用してリストアできます。

System Manager

システム攻撃後の復元

1. ARPスナップショットから復元するには、手順2に進みます。以前のスナップショットから復元するには、まずARPスナップショットのロックを解除する必要があります。
   a. Storage > Volumes （ストレージ）を選択します。
   b. を選択し、[疑わしいファイルの種類を表示]*を選択します。
   c. ファイルを「ランサムウェア攻撃の可能性」としてマークします。
   d. [更新]*および[疑わしいファイルの種類をクリア]*を選択します。
2. ボリューム内のSnapshotを表示します。

   [ストレージ]>[ボリューム]を選択し、ボリュームと Snapshotコピー*を選択します。
3. リストアするSnapshotの横にあるを選択し、*[リストア]*を選択します。

システム攻撃が特定されなかった場合のリストア

1. ボリューム内のSnapshotを表示します。

   [ストレージ]>[ボリューム]を選択し、ボリュームと Snapshotコピー*を選択します。
2. 選択次に、 `Anti_ransomware`スナップショット。
3. [* Restore] を選択します。
4. メニューに戻り、使用する**Snapshot**を選択します。**[** Restore] を選択します。

CLI

システム攻撃後の復元

ARPスナップショットから復元するには、手順2に進みます。以前のスナップショットからデータを復元するには、ARPスナップショットのロックを解除する必要があります。

> 以下のようにコマンドを使用している場合にのみ、以前のスナップショットから復元する前にAnti-Ransomware SnapLockを解放する必要があり `volume snapshot restore`ます。FlexClone、単一ファイルSnapRestore、またはその他の方法を使用してデータをリストアする場合は、この作業は必要ありません。

1. 攻撃を潜在的なランサムウェア攻撃としてマークする(`-false-positive false` ）および疑わしいファイルをクリアする(`clear-suspect`):

   ```
   anti-ransomware volume attack clear-suspect -vserver <svm_name>
   -volume <vol_name> [<extension identifiers>] -false-positive false
   ```

   次のいずれかのパラメータを使用して拡張子を特定します。

   - `[-seq-no` *`integer`*`]`：疑わしいリスト内のファイルのシーケンス番号。
   - `[-extension` *`text`*`, … ]`：ファイル拡張子

- `[-start-time date_time -end-time date_time]`：クリアするファイルの範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。

2. ボリューム内のSnapshotを一覧表示します。

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

次の例は、のSnapshotを示してい `vol1`ます。

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

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

7 entries were displayed.
```

3. Snapshotからボリュームの内容をリストアします。

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

次の例は、の内容をリストアし `vol1`ます。

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

システム攻撃が特定されなかった場合のリストア

1. ボリューム内のSnapshotを一覧表示します。

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

次の例は、のSnapshotを示してい `vol1`ます。

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

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

7 entries were displayed.
```

2. Snapshotからボリュームの内容をリストアします。

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

次の例は、の内容をリストアし `vol1`ます。

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

の詳細については `volume snapshot`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "NetAppナレッジベース: ONTAPにおけるランサムウェアの防止とリカバリ"
- "ONTAPコマンド リファレンス"

自動生成された**ARP**スナップショットの設定を調整する

ONTAP 9 .11.1以降では、CLIを使用して、ランサムウェア攻撃の疑いがある場合に自動的に生成されるAutonomous Ransomware Protection（ARP）Snapshotの保持設定を制御できます。

開始する前に

ARPスナップショットオプションを変更できるのは、 "ノードSVM"他の SVM タイプでは適用されません。

手順

1. 現在のARPスナップショット設定をすべて表示します。

```
options -option-name arw*
```

2. 選択した現在のARPスナップショット設定を表示：

```
options -option-name <arw_setting_name>
```

3. ARPスナップショット設定を変更します。

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

次の設定を変更できます。

ここで説明するコマンドの一部は、 ONTAP 9.17.1以降では廃止されています。ONTAPONTAPで導入されたコマンドは、NAS環境とSAN環境の両方をサポートします。

設定	説明	サポート対象のバージョン
`arw.snap.max.count`	ボリューム内に同時に存在できるARPスナップショットの最大数を指定します。ARPスナップショットの総数が指定された制限内に収まるように、古いコピーは削除されます。	ONTAP 9.11.1以降
`arw.snap.create.interval.hours`	ARPスナップショットの間隔（時間単位）を指定します。データエントロピーベースの攻撃が疑われる場合、かつ最後に作成されたARPスナップショットが指定された間隔よりも古い場合、新しいARPスナップショットが作成されます。	ONTAP 9.11.1以降
`arw.snap.normal.retain.interval.hours`	ARPスナップショットを保持する期間（時間単位）を指定します。ARPスナップショットが保持しきい値に達すると、削除されます。	• ONTAP 9.11.1からONTAP 9.16.1 • ONTAP 9.17.1以降では非推奨

設定	説明	サポート対象のバージョン
`arw.snap.max.retain.interval.days`	ARPスナップショットを保持できる最大期間（日数）を指定します。ボリュームで攻撃が報告されていない場合、この期間よりも古いARPスナップショットは削除されます。 中程度の脅威が検出された場合、ARPスナップショットの最大保持間隔は無視されます。脅威に対応して作成されたARPスナップショットは、脅威に対応するまで保持されます。脅威を誤検出としてマークすると、ONTAPはそのボリュームのARPスナップショットを削除します。	• ONTAP 9.11.1 からONTAP 9.16.1 • ONTAP 9.17.1 以降では非推奨
`arw.snap.create.interval.hours.post.max.count`	ボリュームにすでに最大数のARPスナップショットが含まれている場合の、ARPスナップショット間の間隔（時間単位）を指定します。最大数に達すると、ARP Snapshotが削除されて、新しいコピー用のスペースが確保されます。このオプションを使用すると、新しいARP Snapshotの作成速度を遅くして、古いコピーを保持することができます。ボリュームにすでに最大数のARPスナップショットが含まれている場合、このオプションで指定された間隔は、次回のARPスナップショットの作成時に使用されます。 `arw.snap.create.interval.hours` 。	• ONTAP 9.11.1 から 9.16.1 • ONTAP 9.17.1 以降では非推奨
`arw.snap.low.encryption.retain.duration.hours`	暗号化アクティビティが少ない期間中に作成された ARP スナップショットの保持期間を時間単位で指定します。	• ONTAP 9.17.1 以降
`arw.snap.new.extns.interval.hours`	新しいファイル拡張子が検出されたときに作成されるARPスナップショットの間隔（時間単位）を指定します。新しいファイル拡張子が見つかると、新しいARP Snapshotが作成されます。新しいファイル拡張子を監視しているときに作成された以前のSnapshotは、この指定された間隔よりも古いものです。頻繁に新しいファイル拡張子が作成されるワークロードでは、この間隔によってARPスナップショットの頻度を制御できます。このオプションは、`arw.snap.create.interval.hours`データ エントロピー ベースのARP スナップショットの間隔を指定します。	• ONTAP 9.11.1 からONTAP 9.16.1 • ONTAP 9.17.1 以降では非推奨
`arw.snap.retain.hours.after.clear.suspect.false.alert`	管理者が攻撃インシデントを誤検知と判定した後、予防措置としてARPスナップショットを保持する間隔（時間単位）を指定します。この予防措置保持期間が経過すると、スナップショットはオプションで定義された標準保持期間に従って削除されます。 `arw.snap.normal.retain.interval.hours`そして `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 以降

設定	説明	サポート対象のバージョン
`arw.snap.retain.hours.after.clear.suspect.real.attack`	管理者が攻撃インシデントを実際の攻撃としてマークした後、予防措置としてARPスナップショットを保持する間隔（時間単位）を指定します。この予防措置保持期間が経過すると、スナップショットはオプションで定義された標準保持期間に従って削除されます。`arw.snap.normal.retain.interval.hours`そして`arw.snap.max.retain.interval.days`。	• ONTAP 9.16.1以降
`arw.snap.surge.interval.days`	IOサージに応答して作成されるARPスナップショット間のinterval_in days_betweenを指定します。ONTAPは、IOトラフィックが急増し、最後に作成されたARPスナップショットがこの指定された間隔よりも古い場合に、ARPスナップショットサージコピーを作成します。このオプションは、ARPサージスナップショットの保持期間（日数_）も指定します。	ONTAP 9.11.1以降
`arw.high.encryption.alert.enabled`	高度な暗号化に関するアラートを有効にします。このオプションが`on`（デフォルト）、暗号化の割合が指定されたしきい値を超えると、 ONTAPはアラートを送信します。`arw.high.encryption.percentage.threshold`。	ONTAP 9.17.1以降
`arw.high.encryption.percentage.threshold`	ボリュームの暗号化の最大割合を指定します。暗号化の割合がこのしきい値を超えると、 ONTAP は増加を攻撃とみなし、ARP スナップショットを作成します。`arw.high.encryption.alert.enabled`に設定する必要があります`on`このオプションを有効にするには、	ONTAP 9.17.1以降
`arw.snap.high.encryption.retain.duration.hours`	高い暗号化しきい値イベント中に作成されたスナップショットの保持期間間隔を 時間単位 で指定します。	ONTAP 9.17.1以降

4. SAN 環境で ARP を使用している場合は、次の評価期間設定を変更することもできます。

設定	説明	サポート対象のバージョン
`arw.block_device.auto.learn.threshold.min_value`	ブロック デバイスの評価の自動学習フェーズ中の最小暗号化しきい値のパーセンテージ値を指定します。	ONTAP 9.17.1以降
`arw.block_device.auto.learn.threshold.max_value`	ブロック デバイスの評価の自動学習フェーズ中の最大暗号化しきい値のパーセンテージ値を指定します。	ONTAP 9.17.1以降
`arw.block_device.evaluation.phase.min_hours`	暗号化しきい値が設定される前に評価フェーズを実行する必要がある最小間隔（時間単位）を指定します。	ONTAP 9.17.1以降

設定	説明	サポート対象のバージョン
`arw.block_device.evaluation.phase.max_hours`	暗号化しきい値が設定される前に評価フェーズを実行する必要がある最大間隔（時間単位）を指定します。	ONTAP 9.17.1以降
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	暗号化しきい値が設定される前に、評価フェーズ中に取り込む必要があるデータの最小量（GB 単位）を指定します。	ONTAP 9.17.1以降
`arw.block_device.evaluation.phase.alert.enabled`	ブロックデバイス上のARPの評価フェーズでアラートを有効にするかどうかを指定します。デフォルト値は `True` 。	ONTAP 9.17.1以降
`arw.block_device.evaluation.phase.alert.threshold`	ブロックデバイスにおけるARPの評価フェーズにおけるしきい値のパーセンテージを指定します。暗号化の割合がこのしきい値を超えると、アラートがトリガーされます。	ONTAP 9.17.1以降

関連情報

- "脅威評価とARPスナップショット"
- "SANエントロピー評価期間"

Vscanによるウィルス保護

ONTAP Vscanを使用したウイルス対策設定について学ぶ

Vscanは、NetAppが開発したウィルススキャンソリューションです。ウィルスやその他の悪意のあるコードからデータを保護できます。

Vscanは、クライアントがSMB経由でファイルにアクセスするときにウィルススキャンを実行します。Vscanは、オンデマンドまたはスケジュールに基づいてスキャンするように設定できます。Vscanは、ONTAPのコマンドラインインターフェイス（CLI）またはONTAPのアプリケーションプログラミングインターフェイス（API）を使用して操作できます。

関連情報

"Vscanパートナーソリューション"

NetAppアンチウイルスによる保護について

ONTAP Vscanを使用したNetAppウイルススキャンについて学ぶ

Vscanは、NetAppが開発したウィルススキャンソリューションです。ウィルスやその他の悪意のあるコードからデータを保護できます。パートナーが提供するウイルス対策ソフトウェアとONTAPの機能を組み合わせることで、お客様はファイルスキャンの管理に必要な柔軟性を得ることができます。

スキャン処理は、サードパーティベンダーのウィルス対策ソフトウェアをホストする外部サーバにオフロードされます。

ONTAPは、アクティブなスキャンモードに基づいて、クライアントがSMB経由でファイルにアクセスする場合（オンアクセス）、または特定の場所にあるファイルにスケジュールに従ってアクセスする場合、またはただちに（オンデマンドで）アクセスする場合にスキャン要求を送信します。

- クライアントが SMB 経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、 _on_access scanning_to を使用します。ファイル操作は、外部サーバからファイルのスキャンステータスが報告されるまで中断されます。ファイルがすでにスキャンされている場合、ONTAPはファイル操作を許可します。それ以外の場合は、サーバからのスキャンを要求します。

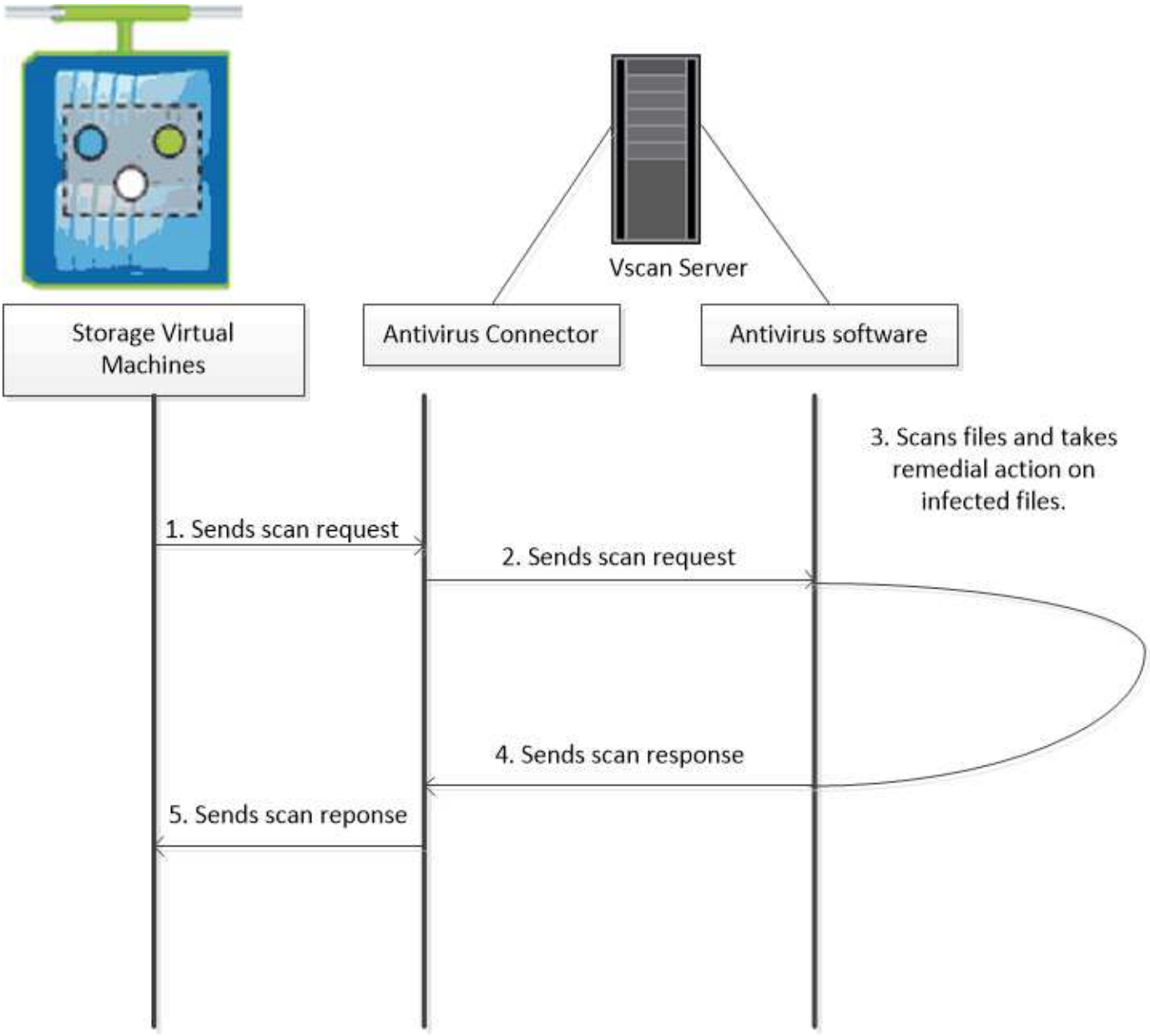
  NFSではオンアクセススキャンはサポートされていません。

- オンデマンドスキャン _ を使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。通常はオンアクセススキャン用にサイジングされている既存のAVインフラが過負荷にならないように、オンデマンドスキャンはオフピークの時間帯にのみ実行することを推奨します。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB経由でのファイルアクセスのレイテンシが低減されます。ファイルの変更またはソフトウェアバージョンの更新があった場合は、外部サーバから新しいファイルスキャンを要求します。

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

通常は、SVMでオンアクセスモードとオンデマンドスキャンモードの両方を有効にします。どちらのモードでも、ウィルス対策ソフトウェアはソフトウェアの設定に基づいて感染したファイルに対して修復アクションを実行します。

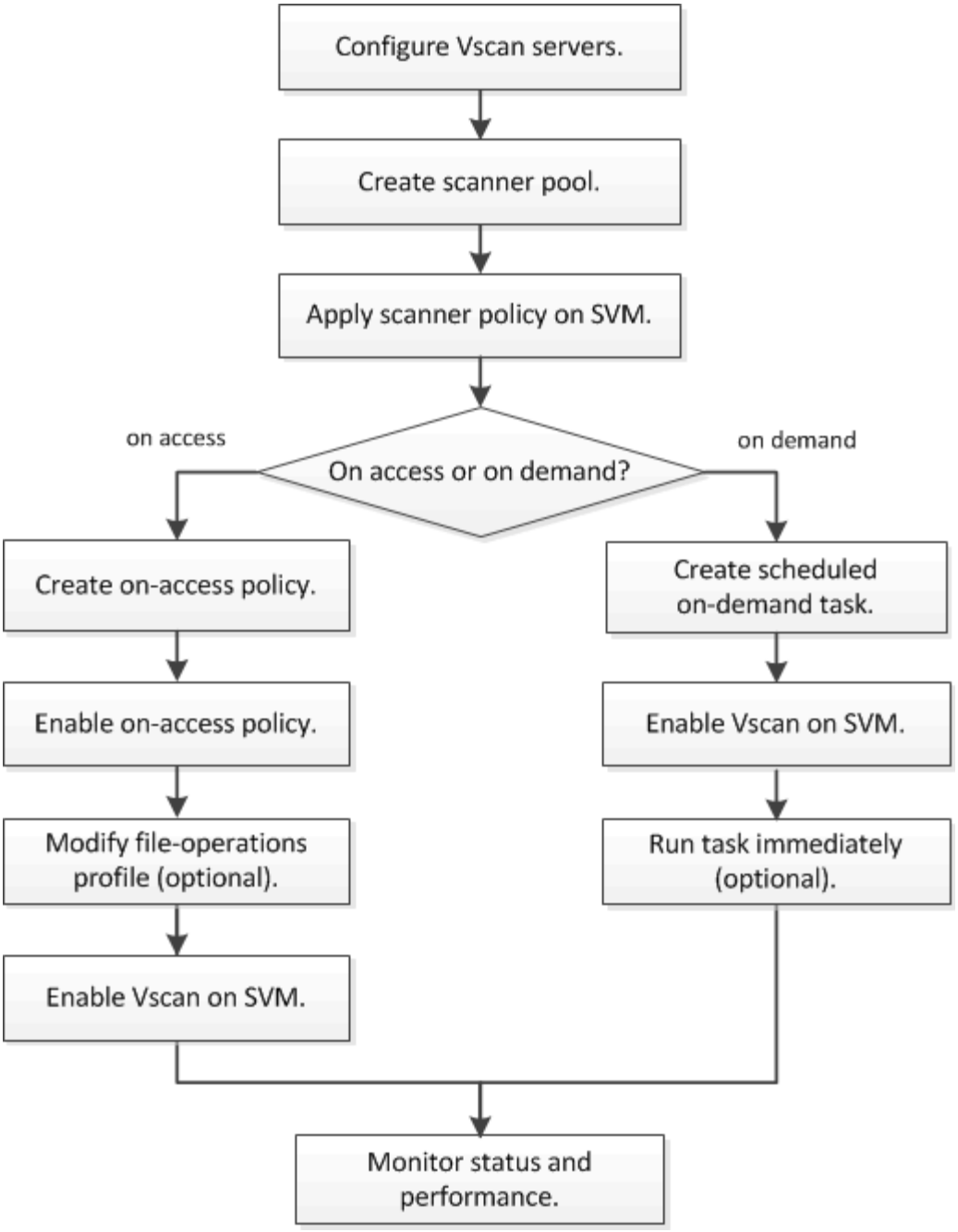
NetAppが提供し、外部サーバにインストールされるONTAP Antivirus Connectorは、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。



ONTAP Vscanによるウイルススキャンワークフロー

スキャンを有効にする前に、スキャナプールを作成してスキャナポリシーを適用する必要があります。通常は、SVMでオンアクセスモードとオンデマンドスキャンモードの両方を有効にします。

CIFSの設定が完了している必要があります。



オンデマンドタスクを作成するには、少なくとも1つのオンアクセスポリシーを有効にする必要があります。デフォルトポリシーまたはユーザが作成したオンアクセスポリシーを使用できます。

次のステップ

- 単一クラスタにスキャナプールを作成する
- 単一のクラスタにスキャナポリシーを適用する
- オンアクセスポリシーを作成する

ONTAP Vscan を使用したウイルス対策アーキテクチャ

NetAppウィルス対策アーキテクチャは、Vscanサーバソフトウェアと関連する設定で構

成されます。

Vscanサーバソフトウェア

このソフトウェアはVscanサーバにインストールする必要があります。

- * ONTAP Antivirus Connector *

  NetAppが提供するソフトウェアで、SVMとウィルス対策ソフトウェアの間のスキャン要求と応答の通信を処理します。仮想マシン上で実行できますが、最高のパフォーマンスを得るには物理マシンを使用します。このソフトウェアはNetAppサポートサイトからダウンロードできます（ログインが必要です）。

- * アンチウイルスソフトウェア *

  これは、ウイルスやその他の悪意のあるコードのファイルをスキャンするパートナー提供のソフトウェアです。ソフトウェアを設定する際に、感染したファイルに対して実行する処理を指定します。

Vscanソフトウェア設定

これらのソフトウェアをVscanサーバで設定する必要があります。

- * スキャナプール *

  この設定では、SVMに接続できるVscanサーバと特権ユーザを定義します。また、スキャン要求のタイムアウト時間も定義します。この時間が経過すると、代替のVscanサーバがある場合はそのサーバにスキャン要求が送信されます。

  > Vscanサーバ上のウィルス対策ソフトウェアのタイムアウト時間は、scanner-poolのスキャン要求タイムアウト時間よりも5秒短く設定する必要があります。これにより、ソフトウェアのタイムアウト時間がスキャン要求のタイムアウト時間よりも長いため、ファイルアクセスが遅延または拒否される状況を回避できます。

- * 特権ユーザ *

  この設定は、VscanサーバがSVMへの接続に使用するドメインユーザアカウントです。スキャナプール内の特権ユーザのリストにアカウントが存在している必要があります。

- * スキャナポリシー *

  この設定では、スキャナプールをアクティブにするかどうかを指定します。スキャナポリシーはシステムで定義されるため、カスタムのスキャナポリシーを作成することはできません。次の3つのポリシーのみを使用できます。

  - `Primary`スキャナプールをアクティブにします。
  - `Secondary`プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
  - `Idle`スキャナプールを非アクティブにします。

- * オンアクセスポリシー *

  この設定では、オンアクセススキャンの範囲を定義します。スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。

デフォルトでは、読み取り/書き込みボリュームのみがスキャンされます。読み取り専用ボリュームのスキャンを有効にするフィルタや、実行アクセス権で開かれたファイルのみにスキャンを制限するフィルタを指定することができます。

- `scan-ro-volume`読み取り専用ボリュームのスキャンを有効にします。
- `scan-execute-access`実行アクセス権で開かれたファイルにスキャンを制限します。

> 「アクセスの実行」と「アクセスの実行」は「アクセスの実行」とは異なります。 指定されたクライアントは、実行ファイルが「実行意図」で開かれている場合にのみ、実行ファイルに対して「実行アクセス」を持つことになります。

このオプションをoffに設定する `scan-mandatory`と、ウィルススキャンに使用できるVscanサーバがない場合にファイルアクセスを許可します。オンアクセスモードでは、次の2つのオプションのいずれかを選択できます。

- 必須：このオプションを指定すると、タイムアウト時間が経過するまで、Vscanはサーバへのスキャン要求の配信を試みます。サーバがスキャン要求を受け入れなかった場合、クライアントアクセス要求は拒否されます。
- 必須以外：このオプションを使用すると、Vscanサーバがウィルススキャンに使用できるかどうかに関係なく、Vscanでクライアントアクセスが常に許可されます。

- * オンデマンドタスク *

この設定では、オンデマンドスキャンの範囲を定義します。スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。デフォルトでは、サブディレクトリ内のファイルがスキャンされます。

cronスケジュールを使用して、タスクを実行するタイミングを指定します。コマンドを使用すると、タスクをすぐに実行できます `vserver vscan on-demand-task run`。の詳細については `vserver vscan on-demand-task run`、を"ONTAPコマンド リファレンス"参照してください。

- * Vscan ファイル処理プロファイル（オンアクセススキャンのみ） *

コマンドのパラメータ `vserver cifs share create`は、 `vscan-fileop-profile`ウィルススキャンをトリガーするSMBファイル処理を定義します。デフォルトでは、パラメータは（NetAppのベストプラクティス）に設定され `standard`ます。このパラメータは、SMB共有を作成または変更するときに必要に応じて調整できます。

- `no-scan`共有に対してウィルススキャンを一切トリガーしません。
- `standard`開く、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。
- `strict`開く、読み取る、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。

  プロファイルを使用する `strict`と、複数のクライアントが同時に1つのファイルにアクセスする場合のセキュリティが強化されます。では、あるクライアントがウィルスを書き込んだあとにファイルを閉じたときに別のクライアントが同じファイルを開いていた場合、2番目のクライアントが `strict`ファイルを閉じる前に読み取り処理を実行したときにスキャンがトリガーされます。

`strict`同時にアクセスされる可能性があるファイルを含む共有にプロファイルを制限するように注意してください。このプロファイルはより多くのスキャン要求を生成するため、パフォーマンスに影響を与える可能性があります。

- `writes-only`変更されたファイルが閉じられたときにのみウィルススキャンをトリガーします。

`writes-only`で生成されるスキャン要求が少なくなるため、通常はパフォーマンスが向上します。

このプロファイルを使用する場合は、修復不可能な感染ファイルを削除または隔離するようにスキャナを設定して、アクセスできないようにする必要があります。たとえば、あるクライアントがウィルスを書き込んだあとにファイルを閉じた場合、そのファイルが修復、削除、または隔離されていないと、書き込み先のファイルにアクセスしたすべてのクライアント `without`が感染します。

クライアントアプリケーションが名前変更処理を実行すると、ファイルは新しい名前で閉じられ、スキャンされません。このような処理によってセキュリティが懸念される環境では、または `strict`プロファイルを使用する必要があり `standard`ます。

の詳細については `vserver cifs share create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP Vscanパートナーソリューションの詳細

NetAppは、Trellix、Symantec、Trend Micro、Sentinel One、Deep Instinct、OPSWATと協力して、ONTAP Vscanテクノロジを基盤とする業界をリードするアンチマルウェアおよびアンチウイルスソリューションを提供しています。これらのソリューションは、ファイルをスキャンしてマルウェアを検出し、影響を受けるファイルを修正するのに役立ちます。

次の表に示すように、Trellix、Symantec、Trend Microの相互運用性の詳細については、NetAppのInteroperability Matrixを参照してください。Trellix、Symantec、Deep Instinct、OPSWATの相互運用性の詳細については、パートナーのWebサイトを参照してください。Sentinel One、Deep Instinct、OPSWAT、およびその他の新しいパートナーの相互運用性の詳細は、パートナーのWebサイトで管理されます。

パートナー	ソリューションのドキュメント	相互運用性の詳細
Trellix（旧McAfee）	"Trellix製品ドキュメント"	• "NetApp Interoperability Matrix Tool" • "Endpoint Security Storage Protectionでサポートされるプラットフォーム（trellix.com）"

パートナー	ソリューションのドキュメント	相互運用性の詳細
シマンテック	"Symantec Protection Engine 9.0.0"	• "NetApp Interoperability Matrix Tool" • "Symantec Protection Engine（SPE）for Network Attached Storage（NAS）9.x.xと認定されたパートナーデバイスのサポートマトリックス"
トレンドマイクロ	"『Trend Micro ServerProtect for Storage 6.0 Getting Started Guide』"	"NetApp Interoperability Matrix Tool"
Sentinel One	• "SentinelOne Singularityクラウドデータセキュリティ" • "SentinelOneのサポート" このリンクにはユーザ ログインが必要です。SentinelOneにアクセス権をリクエストしてください。	N/A
Deep Instinct	Deep Instinct DSX for NAS • "ドキュメントと相互運用性" このリンクにはユーザ ログインが必要です。Deep Instinctにアクセス権をリクエストしてください。 • "データシート"	N/A
オプスワット	OPSWAT MetaDefenderストレージセキュリティ • "MetaDefenderストレージセキュリティとNetAppの統合" • "OPSWATパートナーページ" • "統合ソリューション概要"	N/A

Vscanサーバのインストールと設定

ONTAP Vscanサーバーのインストールと構成

1つ以上のVscanサーバを設定して、システム上のファイルがウィルススキャンされるようにします。サーバにウィルス対策ソフトウェアをインストールして設定するには、ベ

ンダーの指示に従ってください。

NetAppが提供するREADMEファイルの手順に従って、ONTAP Antivirus Connectorをインストールして設定します。または、の手順に従います"[Install ONTAP Antivirus Connectorページ"]。

ディザスタリカバリおよびMetroCluster構成の場合は、プライマリ/ローカルおよびセカンダリ/パートナーのONTAPクラスタ用に個別のVscanサーバをセットアップして設定する必要があります。

ウィルス対策ソフトウェアの要件

- ウィルス対策ソフトウェアの要件については、ベンダーのドキュメントを参照してください。
- Vscanでサポートされるベンダー、ソフトウェア、およびバージョンについては、"Vscanパートナーソリューション"ページを参照してください。

ONTAP Antivirus Connectorの要件

- ONTAP Antivirus Connectorは、NetAppサポートサイトの*ソフトウェアダウンロード*ページからダウンロードできます。"NetAppのダウンロード：ソフトウェア"
- ONTAP Antivirus Connectorでサポートされるバージョンと相互運用性の要件については、を参照してください"Vscanパートナーソリューション"。

クラスタ内のVscanサーバごとに異なるバージョンのWindowsサーバをインストールできます。

- Windowsサーバに.NET 3.0以降がインストールされている必要があります。
- WindowsサーバでSMB 2.0が有効になっている必要があります。

ONTAP Vscan アンチウイルスコネクタをインストールする

ONTAPを実行しているシステムとVscanサーバの間の通信を有効にするには、ONTAP Antivirus ConnectorをVscanサーバにインストールします。ONTAP Antivirus Connectorをインストールすると、ウイルス対策ソフトウェアが1台以上のStorage Virtual Machine（SVM）と通信できるようになります。

タスクの内容

- "Vscanパートナーソリューション"サポートされるプロトコル、ウィルス対策ベンダーのソフトウェアのバージョン、ONTAPのバージョン、相互運用性の要件、およびWindowsサーバについては、ページを参照してください。
- .NET 4.5.1以降がインストールされている必要があります。
- ONTAP Antivirus Connectorは仮想マシンで実行できます。ただし、最高のパフォーマンスを得るために、NetAppではアンチウイルススキャンに専用の物理マシンを使用することを推奨しています。
- ONTAP Antivirus Connectorをインストールして実行するWindowsサーバでSMB 2.0が有効になっている必要があります。

開始する前に

- サポートサイトからONTAP Antivirus Connectorセットアップファイルをダウンロードし、ハードドライブ

のディレクトリに保存します。

- ONTAP Antivirus Connectorをインストールするための要件を満たしていることを確認します。
- Antivirus Connectorをインストールするための管理者権限があることを確認します。

手順

1. 適切なセットアップファイルを実行して、Antivirus Connectorインストールウィザードを開始します。
2. ［次へ］を選択します。[インストール先フォルダ]ダイアログボックスが開きます。
3. 表示されているフォルダにAntivirus Connectorをインストールするには、_Next_を選択します。別のフォルダにインストールするには、_Change__を選択します。
4. [Windows AV Connector ONTAPサービスのクレデンシャル]ダイアログボックスが開きます。
5. Windowsサービスのクレデンシャルを入力するか、*[追加]*を選択してユーザを選択します。ONTAPシステムの場合、このユーザは有効なドメインユーザであり、SVMのスキャナプール設定に存在している必要があります。
6. 「 * 次へ * 」を選択します。[プログラムをインストールする準備ができました]ダイアログボックスが開きます。
7. インストールを開始するには*を選択します。設定を変更する場合は[戻る]*を選択します。ステータス・ボックスが開き'インストールの進行状況が表示され'InstallShield Wizard Completedダイアログ・ボックスが表示されます
8. ONTAP ONTAP管理LIFまたはデータLIFの設定を続行する場合は、[LIFの設定]チェックボックスを選択します。このVscanサーバを使用するには、ONTAP管理LIFまたはデータLIFを少なくとも1つ設定する必要があります。
9. インストールログを表示する場合は、[Windowsインストーラログを表示する]チェックボックスをオンにします。
10. を選択してインストールを終了し、**InstallShield**ウィザードを閉じます。**ONTAP LIF**を設定するための[Configure ONTAP LIFs]*アイコンがデスクトップに保存されます。
11. Antivirus ConnectorにSVMを追加します。Antivirus ConnectorにSVMを追加するには、データLIFのリストを取得するためにポーリングするONTAP管理LIFを追加するか、1つ以上のデータLIFを直接設定します。ONTAP管理LIFを設定する場合は、ポーリング情報とONTAP管理者アカウントのクレデンシャルも指定する必要があります。
    - SVMの管理LIFまたはIPアドレスがで有効になっていることを確認します `management-https`。これは、データLIFのみを設定する場合は必要ありません。
    - HTTPアプリケーション用のユーザアカウントを作成し、REST APIへの（少なくとも読み取り専用）アクセスを持つロールを割り当てたことを確認します `/api/network/ip/interfaces`。
    - および `security login create`の詳細については `security login role create`、を"ONTAPコマンド リファレンス"参照してください。

> 管理 SVM に認証トンネル SVM を追加して、ドメイン ユーザーをアカウントとして使用することもできます。の詳細については `security login domain-tunnel create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた*アイコンを右クリックし、[Run as Administrator]*を選択します。

2. [Configure ONTAP LIFs]ダイアログボックスで、優先する設定タイプを選択し、次の操作を実行します。

作成するLIFのタイプ	実行する手順
Data LIF	a. 「role」を「data」に設定 b. 「data protocol」を「cifs」に設定 c. 「firewall policy」を「data」に設定する d. 「service policy」を「default-data-files」に設定
管理LIF	a. 「role *」を「data」に設定 b. 「data protocol」を「none」に設定します。 c. 「firewall policy」を「mgmt」に設定 d. 「service policy」を「default-management」に設定

詳細については、をご覧ください"LIFの作成"。

LIFを作成したら、追加するSVMのデータLIF、管理LIF、またはIPアドレスを入力します。クラスタ管理LIFを入力することもできます。クラスタ管理LIFを指定すると、そのクラスタ内にある、SMBを提供するすべてのSVMでVscanサーバを使用できます。

VscanサーバでKerberos認証が必要な場合は、各SVMデータLIFに一意のDNS名を付ける必要があり、その名前をWindows Active DirectoryにServer Principal Name（SPN；サーバプリンシパル名）として登録する必要があります。一意のDNS名が各データLIFに使用できない場合、またはSPNとして登録されていない場合、VscanサーバはNT LAN Managerメカニズムを使用して認証します。Vscanサーバを接続したあとにDNS名やSPNを追加または変更した場合は、変更を適用するために、VscanサーバでAntivirus Connectorサービスを再起動する必要があります。

3. 管理LIFを設定するには、ポーリング期間を秒単位で入力します。ポーリング期間とは、Antivirus ConnectorがSVMまたはクラスタのLIF設定に対する変更をチェックする頻度です。デフォルトのポーリング期間は60秒です。
4. ONTAP管理者アカウント名とパスワードを入力して、管理LIFを設定します。
5. [テスト]*をクリックして接続を確認し、認証を確認します。認証は管理LIFの設定でのみ検証されます。
6. ポーリングまたは接続先のLIFのリストにLIFを追加するには、*[更新]*をクリックします。
7. [保存]*をクリックして、レジストリへの接続を保存します。
8. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、*エクスポート*をクリックします。これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

設定オプションについては、を参照してください"ONTAP Antivirus Connectorページの設定"。

ONTAP Vscan ウイルス対策コネクタを構成する

ONTAP Antivirus Connectorを設定して、接続するStorage Virtual Machine（SVM）を1つまたは複数指定します。この設定では、ONTAP管理LIF、ポーリング情報、ONTAP管

理者アカウントのクレデンシャルを入力するか、データLIFのみを入力します。また、SVM接続の詳細を変更するか、SVM接続自体を削除することもできます。デフォルトでは、ONTAP管理LIFが設定済みの場合、ONTAP Antivirus ConnectorはREST APIを使用してデータLIFの一覧を取得します。

SVM接続の詳細の変更

Antivirus Connectorに追加済みのStorage Virtual Machine（SVM）の詳細を更新するには、ONTAP管理LIFおよびポーリング情報を変更します。追加済みのデータLIFを更新することはできません。データLIFを更新するには、まず該当のLIFを削除してから、新しいLIFまたはIPアドレスで追加し直す必要があります。

開始する前に

HTTPアプリケーション用のユーザアカウントを作成し、REST APIへの（少なくとも読み取り専用）アクセスを持つロールを割り当てたことを確認します `/api/network/ip/interfaces`。

および `security login create`の詳細については `security login role create`、を"ONTAPコマンド リファレンス"参照してください。

管理SVM用に認証トンネルSVMを追加して、ドメインユーザをアカウントとして使用することもできます。の詳細については `security login domain-tunnel create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた*アイコンを右クリックし、[Run as Administrator]*を選択します。[Configure ONTAP LIF]ダイアログボックスが開きます。
2. SVMのIPアドレスを選択し、*[更新]*をクリックします。
3. 必要に応じて情報を更新します。
4. [保存]*をクリックして、レジストリの接続の詳細を更新します。
5. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、*エクスポート*をクリックします。これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

Antivirus ConnectorからSVM接続を削除する

不要になったSVM接続は削除できます。

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた*アイコンを右クリックし、[Run as Administrator]*を選択します。[Configure ONTAP LIF]ダイアログボックスが開きます。
2. SVMのIPアドレスを1つ以上選択し、*[削除]*をクリックします。
3. [保存]*をクリックして、レジストリの接続の詳細を更新します。
4. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、*エクスポート*をクリックします。これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

開始する前に

この手順でレジストリ値を作成する場合は、右側のペインを使用します。

診断目的でAntivirus Connectorログを有効または無効にすることができます。デフォルトでは、これらのログは無効になっています。パフォーマンスを強化するには、Antivirus Connectorのログを無効なままにし、重大イベントに対してのみ有効にする必要があります。

手順

1. [スタート]*を選択し、検索ボックスに「regedit」と入力して、[プログラム]リストでを選択します `regedit.exe`。
2. レジストリエディタ*で、ONTAP Antivirus Connectorの次のサブキーを探します。 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 次の表に示すタイプ、名前、および値を指定して、レジストリ値を作成します。

タイプ	名前	値
文字列	トレースパス	C：\ avshim.log

このレジストリ値には、他の有効なパスを指定できます。

4. 次の表に示すタイプ、名前、値、およびログ情報を指定して、別のレジストリ値を作成します。

タイプ	名前	重要なロギング	中間ロギング	詳細なロギング
DWORD	Tracelevel	1	2または3	4

これにより、手順3でTracePathに指定したパス値に保存されるAntivirus Connectorログが有効になります。

5. 手順3および4で作成したレジストリ値を削除して、Antivirus Connectorログを無効にします。
6. 「LogRotation」という名前でタイプ「multi_sz」の別のレジストリ値を作成します（引用符なし）。「LogRotation」で、ローテーションサイズ（1は1MB）のエントリとして「logFileSize:1」を指定し、次の行でローテーションの制限（5は制限）のエントリとして「logFileCount:5」を指定します。

> これらの値はオプションです。指定しない場合は、ローテーションサイズとローテーションの上限にそれぞれデフォルト値の20MBと10ファイルが使用されます。指定された整数値には、小数または小数の値は指定されません。デフォルト値よりも大きい値を指定した場合は、代わりにデフォルト値が使用されます。

7. ユーザ設定のログ ローテーションを無効化する場合は、手順6で作成したレジストリ値を削除します。

カスタム バナー

カスタムバナーを使用すると、法的拘束力のあるステートメントとシステムアクセスに関する免責事項を_Configure ONTAP LIFAPI_windowに配置できます。

ステップ

1. インストールディレクトリのファイルの内容を更新して変更を保存することで、デフォルトバナーを変更し `banner.txt`ます。変更内容がバナーに反映されるようにするには、[Configure ONTAP LIF]ウィンドウを再度開いてください。

Extended Ordinance（EO）モードを有効にする

セキュアな運用のために、拡張規則（EO）モードを有効または無効にすることができます。

手順

1. [スタート]*を選択し、検索ボックスに「regedit」と入力し、[プログラム]リストでを選択します `regedit.exe`。
2. レジストリエディタ*で、ONTAP Antivirus Connectorの次のサブキーを探します。
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 右側のペインで、EOモードを有効にするには「EO_Mode」（引用符なし）と値「1」（引用符なし）という名前の「DWORD」タイプの新しいレジストリ値を作成し、EOモードを無効にするには「0」（引用符なし）を作成します。

> デフォルトでは、レジストリエントリが存在しない場合、 `EO_Mode`EOモードは無効になっています。EOモードをイネーブルにする場合は、外部syslogサーバと相互証明書認証の両方を設定する必要があります。

外部syslogサーバの設定

開始する前に

この手順でレジストリ値を作成する場合は、右側のペインを使用することに注意してください。

手順

1. [スタート]*を選択し、検索ボックスに「regedit」と入力し、[プログラム]リストでを選択します `regedit.exe`。
2. レジストリエディタ*で、syslog設定用のONTAP Antivirus Connector用の次のサブキーを作成します。
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 次の表に示すように、タイプ、名前、および値を指定してレジストリ値を作成します。

タイプ	名前	値
DWORD	syslog_enabled	1または0

   値「1」を指定するとsyslogが有効になり、値「0」を指定するとsyslogが無効になります。

4. 次の表に示す情報を指定して、別のレジストリ値を作成します。

タイプ	名前
REG_SZ	Syslog_host

[値]フィールドには、syslogホストのIPアドレスまたはドメイン名を入力します。

5. 次の表に示す情報を指定して、別のレジストリ値を作成します。

タイプ	名前
REG_SZ	syslog_port

[Value]フィールドに、syslogサーバが実行されているポート番号を入力します。

6. 次の表に示す情報を指定して、別のレジストリ値を作成します。

タイプ	名前
REG_SZ	syslog_protocol

syslogサーバで使用中のプロトコル（「tcp」または「udp」）を[Value]フィールドに入力します。

7. 次の表に示す情報を指定して、別のレジストリ値を作成します。

タイプ	名前	LOG_CRIT	LOG_NOTICE	ログ情報	LOG_DEBUG
DWORD	syslog_level	2	5	6	7

8. 次の表に示す情報を指定して、別のレジストリ値を作成します。

タイプ	名前	値
DWORD	syslog_tls	1または0

値が「1」の場合はTransport Layer Security（TLS）でsyslogが有効になり、値が「0」の場合はTLSでsyslogが無効になります。

設定された外部**syslog**サーバがスムーズに動作することを確認する

- キーが存在しない場合、またはnull値がある場合は、次の手順を実行します。
  - プロトコルのデフォルトは「TCP」です。
  - ポートのデフォルトは、プレーンな「TCP/UDP」の場合は「514」、TLSの場合は「6514」です。
  - syslogレベルのデフォルト値は5（log_notice）です。
- syslogが有効になっていることを確認するには、値が「1」であることを確認し `syslog_enabled`ます。値が「1」の場合は `syslog_enabled`、EOモードが有効かどうかに関係なく、設定されたリモートサーバにログインできます。
- EOモードが「1」に設定されていて、値を「1」から「0」に変更すると、 `syslog_enabled`以下が適用されます。
  - syslogがEOモードでイネーブルになっていない場合は、サービスを開始できません。

- システムが安定した状態で実行されている場合は、EOモードでsyslogを無効にできず、syslogが強制的に「1」に設定されていることを示す警告が表示されます。これはレジストリに表示されます。この場合は、まずEOモードをディセーブルにしてから、syslogをディセーブルにする必要があります。

- EOモードおよびsyslogが有効になっているときにsyslogサーバが正常に実行できない場合、サービスの実行は停止します。これは、次のいずれかの理由で発生する可能性があります。
  - syslog_hostが無効であるか設定されていない。
  - UDPとTCP以外の無効なプロトコルが設定されている。
  - ポート番号が無効である。
- TCP設定またはTCP経由のTLS設定の場合、サーバでIPポートがリスンされていないと、接続に失敗しサービスが終了します。

X.509相互証明書認証の設定

管理パス内でのAntivirus ConnectorとONTAP間のSecure Sockets Layer（SSL）通信には、X.509証明書ベースの相互認証を使用できます。EOモードが有効な状態で証明書が見つからない場合、AV Connectorは強制終了します。Antivirus Connectorで次の手順を実行します。

手順

1. Antivirus Connectorは、Antivirus Connectorのインストールディレクトリを実行するディレクトリパスで、Antivirus Connectorクライアント証明書とNetAppサーバの認証局（CA）証明書を検索します。証明書をこの固定ディレクトリパスにコピーします。
2. クライアント証明書とその秘密鍵をPKCS12形式で埋め込み、「av_client.p12」という名前を付けます。
3. NetAppサーバの証明書への署名に使用したCA証明書（およびルートCAまでの中間署名機関）が、ONTAP拡張メール（PEM）形式で「PEM_CA.pem」という名前のものであることを確認します。Antivirus Connectorインストールディレクトリに配置します。NetApp ONTAPシステムで、Antivirus Connectorのクライアント証明書に「client-ca」タイプの証明書として署名するためのCA証明書（およびルートCAまでの中間署名機関）を「ONTAP」にインストールします。

スキャナプールを設定

ONTAP Vscanスキャナプールの設定について学ぶ

スキャナプールは、SVMに接続できるVscanサーバと特権ユーザを定義します。スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。

> SMBサーバでエクスポートポリシーを使用する場合は、各Vscanサーバをエクスポートポリシーに追加する必要があります。

単一クラスタに ONTAP Vscan スキャナ プールを作成する

スキャナプールは、SVMに接続できるVscanサーバと特権ユーザを定義します。

開始する前に

- SVMとVscanサーバは、同じドメインまたは信頼できるドメインに属している必要があります。
- クラスタ管理LIFにONTAP Antivirus Connectorを設定します。

- 特権ユーザのリストには、VscanサーバがSVMへの接続に使用するドメインとユーザ名が含まれている必要があります。
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

手順

1. スキャナプールを作成します。

   ```
   vserver vscan scanner-pool create -vserver cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - クラスタ管理SVMを指定します。
   - 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
   - 各特権ユーザのドメイン名とユーザ名を指定します。

   の詳細については `vserver vscan scanner-pool create`、を"ONTAPコマンド リファレンス"参照してください。

2. スキャナプールが作成されたことを確認します。

   ```
   vserver vscan scanner-pool show -vserver cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   次のコマンドは、スキャナプールの詳細を表示し `SP`ます。

   ```
   cluster1::> vserver vscan scanner-pool show -vserver cluster_admin_SVM
   -scanner-pool SP

                                       Vserver: cluster_admin_SVM
                                  Scanner Pool: SP
                                Applied Policy: idle
                                Current Status: off
            Cluster on Which Policy Is Applied: -
                     Scanner Pool Config Owner: cluster
           List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                      List of Privileged Users: cifs\u1, cifs\u2
   ```

   コマンドを使用して、クラスタのすべてのスキャナプールを表示することもできます `vserver vscan scanner-pool show`。の詳細については `vserver vscan scanner-pool show`、を"ONTAPコマンド リファレンス"参照してください。

MetroCluster構成で**ONTAP Vscan**スキャナプールを作成する

MetroCluster構成の各クラスタには、クラスタのプライマリとセカンダリのSVMに対応するプライマリとセカンダリのスキャナプールを作成する必要があります。

開始する前に

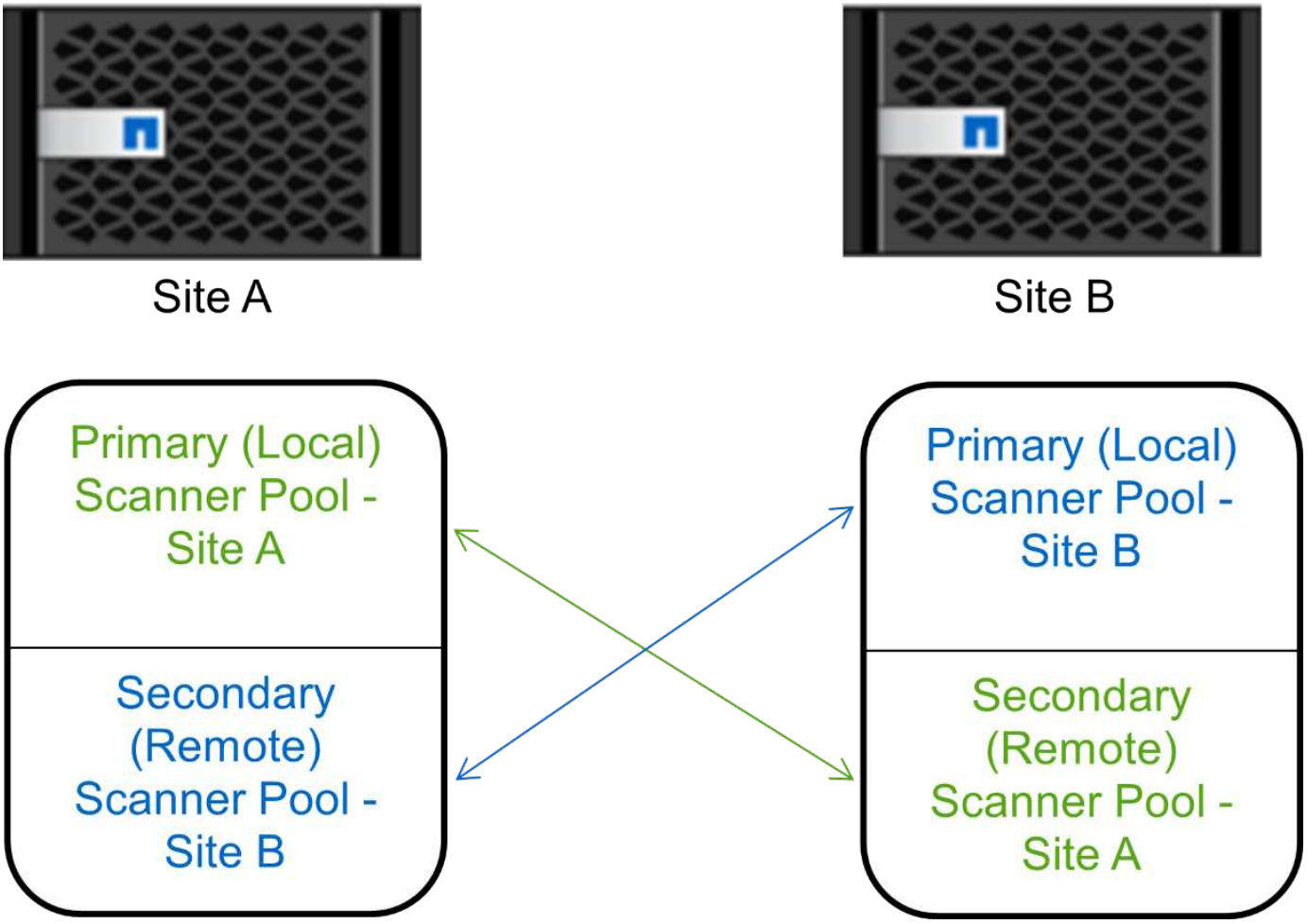
- SVMとVscanサーバは、同じドメインまたは信頼できるドメインに属している必要があります。
- 個 々 のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、VscanサーバがSVMへの接続に使用するドメインユーザアカウントが含まれている必要があります。
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

タスクの内容

MetroCluster構成では、物理的に分離された2つのミラークラスタを実装することでデータを保護各クラスタが、もう一方のクラスタのデータとSVMの設定を同期的にレプリケートします。クラスタがオンラインのときは、ローカルクラスタのプライマリSVMがデータを提供します。リモートクラスタがオフラインのときは、ローカルクラスタのセカンダリSVMがデータを提供します。

つまり、MetroCluster構成の各クラスタにプライマリとセカンダリのスキャナプールを作成する必要があり、クラスタがセカンダリSVMからデータの提供を開始すると、セカンダリプールがアクティブになります。ディザスタリカバリ（DR）の設定はMetroClusterと同様です。

この図は、一般的なMetroCluster / DR構成を示しています。



手順

1. スキャナプールを作成します。

   `vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users`

   - 個々の SVM 用のプールの場合はデータ SVM 、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。
   - 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
   - 各特権ユーザのドメイン名とユーザ名を指定します。

     スキャナプールは、すべてプライマリSVMを含むクラスタから作成する必要があります。

     の詳細については `vserver vscan scanner-pool create`、を"ONTAPコマンド リファレンス"参照してください。

     次のコマンドは、MetroCluster構成の各クラスタにプライマリとセカンダリのスキャナプールを作成します。

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. スキャナプールが作成されたことを確認します。

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   次のコマンドは、スキャナプールの詳細を表示し `pool1`ます。

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

コマンドを使用して、SVMのすべてのスキャナプールを表示することもできます `vserver vscan scanner-pool show`。の詳細については `vserver vscan scanner-pool show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP Vscanを使用して単一クラスタにスキャナポリシーを適用する

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。スキャナプールが定義するVscanサーバがSVMに接続できるようにするには、スキャナプールをアクティブ化する必要があります。

タスクの内容

- 1つのスキャナプールに適用できるスキャナポリシーは1つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。

手順

1. スキャナポリシーを適用します。

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   スキャナポリシーには次のいずれかの値を指定できます。

   - `Primary`スキャナプールをアクティブにします。
   - `Secondary`プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
   - `Idle`スキャナプールを非アクティブにします。

   次の例は、 `vs1`SVMのという名前のスキャナプールがアクティブになっていることを示しています `SP`。

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. スキャナプールがアクティブになっていることを確認します。

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

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

   次のコマンドは、スキャナプールの詳細を表示し `SP`ます。

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

   コマンドを使用すると、SVMのアクティブなスキャナプールを表示できます `vserver vscan scanner-pool show-active`。の詳細については `vserver vscan scanner-pool show-active`、を"ONTAPコマンド リファレンス"参照してください。

MetroCluster ONTAP Vscan構成でスキャナポリシーを適用する

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。MetroCluster構成の各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用する必要があります。

タスクの内容

- 1つのスキャナプールに適用できるスキャナポリシーは1つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。
- ディザスタリカバリおよびMetroCluster構成では、ローカルクラスタとリモートクラスタ内のすべてのスキャナプールにスキャナポリシーを適用する必要があります。
- ローカルクラスタ用に作成するポリシーでは、パラメータにローカルクラスタを指定する必要があります

cluster。リモートクラスタ用に作成するポリシーでは、パラメータにリモートクラスタを指定する必要があります cluster。これにより、災害発生時にリモートクラスタがウィルススキャン処理をテイクオーバーできるようになります。

手順

1. スキャナポリシーを適用します。

   vserver vscan scanner-pool apply-policy -vserver *data_SVM* -scanner-pool *scanner_pool* -scanner-policy primary|secondary|idle -cluster *cluster_to_apply_policy_on*

   の詳細については vserver vscan scanner-pool apply-policy、を"ONTAPコマンド リファレンス"参照してください。

   スキャナポリシーには次のいずれかの値を指定できます。

   - `Primary`スキャナプールをアクティブにします。
   - `Secondary`プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
   - `Idle`スキャナプールを非アクティブにします。

   > スキャナポリシーはすべて、プライマリSVMを含むクラスタから適用する必要があります。

   次のコマンドは、MetroCluster構成の各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用します。

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. スキャナプールがアクティブになっていることを確認します。

   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool

   の詳細については vserver vscan scanner-pool show、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、スキャナプールの詳細を表示し `pool1`ます。

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                     List of Privileged Users: cifs\u1,cifs\u2
```

コマンドを使用すると、SVMのアクティブなスキャナプールを表示できます `vserver vscan scanner-pool show-active`。の詳細については `vserver vscan scanner-pool show-active`、を"ONTAPコマンド リファレンス"参照してください。

Vscan でスキャナ プールを管理するための **ONTAP** コマンド

スキャナプールを変更および削除したり、スキャナプールの特権ユーザやVscanサーバを管理したりできます。また、スキャナプールに関する概要情報を確認することもできます。

状況	入力するコマンド
スキャナプールを変更する	`vserver vscan scanner-pool modify`
スキャナプールを削除する	`vserver vscan scanner-pool delete`
スキャナプールに特権ユーザを追加する	`vserver vscan scanner-pool privileged-users add`
スキャナプールから特権ユーザを削除する	`vserver vscan scanner-pool privileged-users remove`
スキャナプールにVscanサーバを追加する	`vserver vscan scanner-pool servers add`
スキャナプールからVscanサーバを削除する	`vserver vscan scanner-pool servers remove`
スキャナプールの概要と詳細を表示する	`vserver vscan scanner-pool show`

スキャナプールの特権ユーザを表示する	`vserver vscan scanner-pool privileged-users show`
すべてのスキャナプールのVscanサーバを表示する	`vserver vscan scanner-pool servers show`

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

オンアクセススキャンの設定

ONTAP Vscanオンアクセスポリシーを作成する

オンアクセスポリシーはオンアクセススキャンの範囲を定義します。オンアクセスポリシーは、個 々 のSVMまたはクラスタ内のすべてのSVMに対して作成できます。クラスタ内のすべてのSVM用のオンアクセスポリシーを作成した場合は、各SVMでポリシーを個別に有効にする必要があります。

タスクの内容

- スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。
- このオプションをoffに設定する `scan-mandatory`と、ウィルススキャンに使用できるVscanサーバがない場合にファイルアクセスを許可します。
- デフォルトでは、ONTAPは「default_cifs」という名前のオンアクセスポリシーを作成し、クラスタ内のすべてのSVMに対して有効にします。
- 、、 `file-ext-to-exclude`、または `max-file-size`パラメータに基づいてスキャン除外の対象となるファイル `paths-to-exclude`は、オプションが`on`に設定されていてもスキャン対象とみなされません `scan-mandatory`。（オプションに関連する接続の問題については、このセクションを `scan-mandatory`確認してください"トラブルシューティング"）。
- デフォルトでは、読み取り/書き込みボリュームのみがスキャンされます。読み取り専用ボリュームのスキャンを有効にするフィルタや、実行アクセス権で開かれたファイルのみにスキャンを制限するフィルタを指定することができます。
- continuously-availableパラメータがYesに設定されているSMB共有ではウィルススキャンは実行されません。
- _vscanファイル処理プロファイル_の詳細については、セクションを参照してください"ウィルス対策アーキテクチャ"。
- SVMごとに最大10個のオンアクセスポリシーを作成できます。ただし、一度に有効にできるオンアクセスポリシーは1つだけです。
  - オンアクセスポリシーでは、最大100個のパスとファイル拡張子をウィルススキャンの対象から除外できます。
- ファイル除外の推奨事項：
  - 大容量ファイル（ファイルサイズを指定可能）は、CIFSユーザの応答に時間がかかるか、スキャン要求がタイムアウトする可能性があるため、ウィルススキャンの対象から除外することを検討してください。除外するデフォルトのファイルサイズは2GBです。
  - や `.tmp`などのファイル拡張子は除外することを検討してください `.vhd`。これらの拡張子のファ

イルはスキャンに適していない可能性があります。

- 隔離ディレクトリなどのファイルパスや、仮想ハードドライブまたはデータベースのみが格納されているパスを除外することを検討してください。
- 一度に有効にできるポリシーは1つだけであるため、すべての除外が同じポリシーに指定されていることを確認します。NetAppでは、アンチウイルスエンジンで指定されているのと同じ除外を設定することを強く推奨します。

- にはオンアクセスポリシーが必要オンデマンドスキャンです。のオンアクセススキャンを実行しないようにするには、falseと `-file-ext-to-exclude`*をに設定し `-scan-files-with-no-ext`てすべての拡張子を除外します。

手順

1. オンアクセスポリシーを作成します。

   ```
   vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
   -policy-name policy_name -protocol CIFS -max-file-size
   max_size_of_files_to_scan –filters [scan-ro-volume,][scan-execute-access]
   -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
   extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
   -exclude paths_of_files_to_exclude -scan-mandatory on|off
   ```

   - 個々の SVM 用のポリシーの場合はデータ SVM 、クラスタ内のすべての SVM 用のポリシーの場合はクラスタ管理 SVM を指定します。
   - `-file-ext-to-exclude`設定は設定よりも優先され `-file-ext-to-include`ます。
   - 拡張子のないファイルをスキャンするには、trueに設定し `-scan-files-with-no-ext`ます。次のコマンドは、SVM上に `vs1`という名前のオンアクセスポリシーを作成し `Policy1`ます。

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include "mp*","tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. オンアクセスポリシーが作成されたことを確認します。 `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

   の詳細については `vserver vscan on-access-policy`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、ポリシーの詳細を表示し `Policy1`ます。

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

ONTAP Vscanオンアクセスポリシーを有効にする

オンアクセスポリシーはオンアクセススキャンの範囲を定義します。SVMのファイルをスキャンするには、そのSVMでオンアクセスポリシーを有効にする必要があります。

クラスタ内のすべてのSVM用のオンアクセスポリシーを作成した場合は、各SVMでポリシーを個別に有効にする必要があります。SVMで一度に有効にできるオンアクセスポリシーは1つだけです。

手順

1. オンアクセスポリシーを有効にします。

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   次のコマンドは `vs1`、SVMでという名前のオンアクセスポリシーを有効にし `Policy1`ます。

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. オンアクセスポリシーが有効になっていることを確認します。

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

   の詳細については `vserver vscan on-access-policy show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、オンアクセスポリシーの詳細を表示し `Policy1`ます。

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

SMB共有の**ONTAP Vscan**ファイル操作プロファイルを変更する

SMB共有の_vscanファイル処理プロファイル_は、スキャンをトリガーできる共有に対する処理を定義します。デフォルトでは、パラメータはに設定されてい `standard`ます。このパラメータは、SMB共有を作成または変更するときに必要に応じて調整できます。

_vscanファイル処理プロファイル_の詳細については、セクションを参照してください"ウィルス対策アーキテクチャ"。

パラメータがに設定され `Yes`ているSMB共有ではウィルススキャンは実行されません `continuously-available`。

ステップ

1. SMB共有のVscanファイル処理プロファイルの値を変更します。

   ```
   vserver cifs share modify -vserver data_SVM -share-name share -path share_path
   -vscan-fileop-profile no-scan|standard|strict|writes-only
   ```

   の詳細については `vserver cifs share modify`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、SMB共有のVscanファイル処理プロファイルをに変更し `strict`ます。

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

オンアクセスポリシーは変更、無効化、削除できます。ポリシーの概要と詳細を表示できます。

状況	入力するコマンド
オンアクセスポリシーを作成する	`vserver vscan on-access-policy create`
オンアクセスポリシーを変更する	`vserver vscan on-access-policy modify`
オンアクセスポリシーを有効にする	`vserver vscan on-access-policy enable`
オンアクセスポリシーを無効にする	`vserver vscan on-access-policy disable`
オンアクセスポリシーを削除する	`vserver vscan on-access-policy delete`
オンアクセスポリシーの概要と詳細を表示する	`vserver vscan on-access-policy show`
対象から除外するパスをリストに追加する	`vserver vscan on-access-policy paths-to-exclude add`
対象から除外するパスをリストから削除します。	`vserver vscan on-access-policy paths-to-exclude remove`
対象から除外するパスのリストを表示する	`vserver vscan on-access-policy paths-to-exclude show`
対象から除外するファイル拡張子をリストに追加する	`vserver vscan on-access-policy file-ext-to-exclude add`
対象から除外するファイル拡張子をリストから削除する	`vserver vscan on-access-policy file-ext-to-exclude remove`
対象から除外するファイル拡張子のリストを表示する	`vserver vscan on-access-policy file-ext-to-exclude show`
対象に含めるファイル拡張子をリストに追加する	`vserver vscan on-access-policy file-ext-to-include add`
対象に含めるファイル拡張子をリストから削除する	`vserver vscan on-access-policy file-ext-to-include remove`
対象に含めるファイル拡張子のリストを表示する	`vserver vscan on-access-policy file-ext-to-include show`

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

オンデマンドスキャンの設定

ONTAP Vscanオンデマンドスキャンの設定について学ぶ

オンデマンドスキャンを使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。

たとえば、ピーク時以外の時間帯にのみスキャンを実行したり、オンアクセススキャンから除外された非常に大きなファイルをスキャンしたりすることができます。cronスケジュールを使用して、タスクを実行するタイミングを指定できます。

> オンデマンドタスクを作成するには、少なくとも1つのオンアクセスポリシーを有効にする必要があります。デフォルトポリシーまたはユーザが作成したオンアクセスポリシーを使用できます。

このトピックについて

- スケジュールはタスクの作成時に割り当てることができます。
- SVM で同時にスケジュールできるタスクは 1 つだけです。
- オンデマンドスキャンでは、シンボリックリンクやストリームファイルのスキャンはサポートされていません。

> オンデマンドスキャンでは、シンボリックリンクやストリームファイルのスキャンはサポートされていません。

> オンデマンドタスクを作成するには、少なくとも1つのオンアクセスポリシーを有効にする必要があります。デフォルトポリシーまたはユーザが作成したオンアクセスポリシーを使用できます。

ONTAP Vscanでオンデマンドタスクを作成する

オンデマンドタスクは、オンデマンドウィルススキャンの範囲を定義します。スキャンするファイルの最大サイズ、スキャン対象に含めるファイルの拡張子とパス、およびスキャン対象から除外するファイルの拡張子とパスを指定できます。デフォルトでは、サブディレクトリ内のファイルもスキャンされます。

タスクの内容

- SVMごとに最大10個のオンデマンドタスクを作成できますが、アクティブにできるのは1つだけです。
- オンデマンドタスクは、スキャンに関連する統計情報を含むレポートを作成します。このレポートには、コマンドを使用するか、タスクによって作成されたレポートファイルを定義された場所にダウンロードしてアクセスできます。

開始する前に

- そうだろうな オンアクセスポリシーを作成しました。デフォルトのポリシーでもユーザが作成したポリシーでもかまいません。オンアクセスポリシーがないと、スキャンを有効にできません。

手順

1. オンデマンドタスクを作成します。

   `vserver vscan on-demand-task create -vserver data_SVM -task-name task_name -scan-paths paths_of_files_to_scan -report-directory report_directory_path -report-expiry-time expiration_time_for_report -schedule cron_schedule -max -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with -no-ext true|false -directory-recursion true|false`

   - `-file-ext-to-exclude`設定は設定よりも優先され `-file-ext-to-include`ます。
   - 拡張子のないファイルをスキャンするには、trueに設定し `-scan-files-with-no-ext`ます。

     の詳細については `vserver vscan on-demand-task create`、を"ONTAPコマンド リファレンス"参照してください。

     次のコマンドは、「vs1」VMにという名前のオンデマンドタスクを作成します `Task1`。

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

   +

   ジョブのステータスは、コマンドを使用して表示できます `job show`。コマンドと `job resume`コマンドを使用してジョブを一時停止および再開するか、 `job stop`コマンドを使用してジョブを終了でき `job pause`ます。の詳細については `job`、を"ONTAPコマンド リファレンス"参照してください。

2. オンデマンドタスクが作成されたことを確認します。

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   の詳細については `vserver vscan on-demand-task show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、タスクの詳細を表示し `Task1`ます。

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
        Expiration Time for Report: -
```

終了後

タスクの実行をスケジュールする前に、SVMでスキャンを有効にする必要があります。

ONTAP Vscanでオンデマンドタスクをスケジュールする

スケジュールを割り当てずにタスクを作成し、コマンドを使用してスケジュールを割り当てることも、タスクの作成時にスケジュールを追加することもできます `vserver vscan on-demand-task schedule`。

タスクの内容

コマンドで割り当てたスケジュール `vserver vscan on-demand-task schedule`は、コマンドですでに割り当てられているスケジュールよりも優先され `vserver vscan on-demand-task create`ます。

手順

1. オンデマンドタスクのスケジュールを設定します。

   ```
   vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name
   -schedule cron_schedule
   ```

   次のコマンドは、SVMに `vs2`という名前のオンアクセスタスクをスケジュールし `Task2`ます。

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

の詳細については `vserver vscan on-demand-task schedule`、を"ONTAPコマンド リファレンス"参照してください。

> ジョブのステータスを表示するには、コマンドを使用し `job show`ます。 `job pause`コマンドと `job resume`コマンドは、それぞれジョブを一時停止して再開します。コマンドはジョブを終了します。 `job stop`の詳細については `job`、を"ONTAPコマンド リファレンス"参照してください。

2. オンデマンドタスクがスケジュールされていることを確認します。

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   の詳細については `vserver vscan on-demand-task show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、タスクの詳細を表示し `Task 2`ます。

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                  List of Scan Paths: /vol1/, /vol2/cifs/
               Report Directory Path: /report
                        Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
              File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

終了後

タスクの実行をスケジュールする前に、SVMでスキャンを有効にする必要があります。

ONTAP Vscanオンデマンドタスクをすぐに実行

オンデマンドタスクは、スケジュールが割り当てられているかどうかに関係なく、すぐに実行できます。

開始する前に

SVM でスキャンを有効にしておく必要があります。

ステップ

1. オンデマンドタスクをただちに実行します。

   `vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

   次のコマンドは、という名前のオンアクセスタスクをSVM上で `vs1`実行し `Task1`ます。

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   の詳細については `vserver vscan on-demand-task run`、を"ONTAPコマンド リファレンス"参照してください。

   ジョブのステータスは、コマンドを使用して表示できます `job show`。コマンドと `job resume`コマンドを使用してジョブを一時停止および再開するか、 `job stop`コマンドを使用してジョブを終了でき `job pause`ます。の詳細については `job`、を"ONTAPコマンド リファレンス"参照してください。

オンデマンドタスクを管理するための ONTAP Vscan コマンド

オンデマンドタスクは、変更、削除、またはスケジュール解除できます。タスクの概要と詳細を表示したり、タスクのレポートを管理したりできます。

状況	入力するコマンド
オンデマンドタスクを作成する	`vserver vscan on-demand-task create`
オンデマンドタスクを変更する	`vserver vscan on-demand-task modify`
オンデマンドタスクを削除する	`vserver vscan on-demand-task delete`
オンデマンドタスクを実行する	`vserver vscan on-demand-task run`
オンデマンドタスクのスケジュールを設定する	`vserver vscan on-demand-task schedule`

オンデマンドタスクのスケジュールを解除する	`vserver vscan on-demand-task unschedule`
オンデマンドタスクの概要と詳細を表示する	`vserver vscan on-demand-task show`
オンデマンドレポートを表示する	`vserver vscan on-demand-task report show`
オンデマンドレポートを削除する	`vserver vscan on-demand-task report delete`

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

ONTAP Vscan のオフボックスウイルス対策機能を設定するためのベストプラクティス

ONTAPでオフボックス機能を設定する場合は、次の推奨事項を考慮してください。

- 特権ユーザのウィルススキャン処理を制限します。通常のユーザは、特権ユーザクレデンシャルを使用しないでください。この制限は、Active Directoryの特権ユーザのログイン権限を無効にすることで実現できます。
- AdministratorsグループやBackup Operatorsグループなど、ドメイン内で多数の権限を持つユーザグループには、特権ユーザを含める必要はありません。特権ユーザは、Vscanサーバ接続の確立およびウィルススキャン用ファイルへのアクセスを許可するために、ストレージシステムでのみ検証する必要があります。
- Vscanサーバを実行しているコンピュータは、ウィルススキャンの目的でのみ使用してください。一般的な使用を避けるには、これらのマシンのWindowsターミナルサービスおよびその他のリモートアクセスプロビジョニングを無効にし、これらのマシンに新しいソフトウェアをインストールする権利を管理者のみに付与します。
- Vscanサーバはウィルススキャン専用にし、バックアップなどの他の処理には使用しないでください。Vscanサーバを仮想マシン（VM）として実行することもできます。VscanサーバをVMとして実行する場合は、VMに割り当てられているリソースが共有されておらず、ウィルススキャンを実行するのに十分であることを確認してください。
- Vscanサーバに適切なCPU、メモリ、およびディスク容量を提供して、リソースの過剰割り当てを回避します。ほとんどのVscanサーバは、複数のCPUコアサーバを使用してCPU間で負荷を分散するように設計されています。
- SVMからVscanサーバへの接続には、スキャントラフィックが他のクライアントネットワークトラフィックの影響を受けないように、専用ネットワークとプライベートVLANを使用することを推奨しますNetApp。Vscanサーバ上のウィルス対策VLAN専用およびSVM上のデータLIF専用の、独立したネットワークインターフェイスカード（NIC）を作成します。この手順により、ネットワークの問題が発生した場合の管理とトラブルシューティングが簡単になります。アンチウイルストラフィックは、プライベートネットワークを使用して分離する必要があります。ウィルス対策サーバは、次のいずれかの方法でドメインコントローラ（DC）およびONTAPと通信するように設定する必要があります。
  - DCは、トラフィックの分離に使用されるプライベートネットワークを介してアンチウイルスサーバと通信する必要があります。
  - DCサーバとウィルス対策サーバは、CIFSクライアントネットワークとは異なる別のネットワーク（前述のプライベートネットワークではない）を介して通信する必要があります。

◦ ウィルス対策通信でKerberos認証を有効にするには、プライベートLIF用のDNSエントリと、プライベートLIF用に作成したDNSエントリに対応するサービスプリンシパル名をDC上に作成します。この名前は、Antivirus ConnectorにLIFを追加するときに使用します。DNSは、Antivirus Connectorに接続されている各プライベートLIFに対して一意の名前を返すことができる必要があります。

Vscanトラフィック用のLIFがクライアントトラフィック用のLIFとは別のポートに設定されている場合、ポート障害が発生したときにVscan LIFが別のノードにフェイルオーバーする可能性があります。変更によって新しいノードからVscanサーバに到達できなくなり、ノード上のファイル処理に関するスキャン通知が失敗します。ノード上の少なくとも1つのLIFを介してVscanサーバにアクセスできることを確認し、そのノードで実行されたファイル処理のスキャン要求を処理できるようにします。

- 少なくとも1GbEネットワークを使用して、NetAppストレージシステムとVscanサーバを接続します。
- 複数のVscanサーバがある環境では、同様の高パフォーマンスネットワーク接続があるすべてのサーバを接続します。Vscanサーバを接続すると、負荷を分散できるためパフォーマンスが向上します。
- リモートサイトやブランチオフィスには、NetAppではリモートのVscanサーバではなくローカルのVscanサーバを使用することを推奨します。これは、Vscanサーバが高レイテンシの場合に最適なサーバであるためです。コストが要因の場合は、中程度のウイルス保護のためにラップトップまたはPCを使用してください。ボリュームまたはqtreeを共有し、リモートサイトの任意のシステムからスキャンすることで、ファイルシステム全体の定期的なスキャンをスケジュールできます。
- 複数のVscanサーバを使用してSVM上のデータをスキャンし、ロードバランシングと冗長性を確保します。CIFSワークロードとその結果のウィルス対策トラフィックの量は、SVMごとに異なります。ストレージコントローラでCIFSとウィルススキャンのレイテンシを監視します。時間の経過に伴う結果の傾向を監視します。VscanサーバのCPUキューやアプリケーションキューが原因でCIFSのレイテンシやウィルススキャンのレイテンシがトレンドのしきい値を超えて上昇すると、CIFSクライアントの待機時間が長くなることがあります。負荷を分散するためにVscanサーバを追加します。
- 最新バージョンのONTAP Antivirus Connectorをインストールします。
- ウイルス対策のエンジンと定義を常に最新の状態に保ちます。推奨される更新頻度については、パートナーにお問い合わせください。
- マルチテナンシー環境では、スキャナ プール（Vscanサーバのプール）を複数のSVMで共有できます。ただし、VscanサーバとSVMが同じドメインか、信頼できるドメインに属していることが条件になります。
- 感染したファイルに関するウイルス対策ソフトウェア ポリシーは、大半のウイルス対策ベンダーが設定しているデフォルト値である「delete」または「quarantine」に設定します。「vscan-fileop-profile」が「write_only」に設定されていると、感染したファイルが検出された場合も、ファイルは共有に残り、開くことができます。これは、ファイルを開いただけではスキャンはトリガーされないためです。ウイルス対策スキャンは、ファイルを閉じるまでトリガーされません。
- `scan-engine timeout`値は値より小さくする必要があります `scanner-pool request-timeout`。この値を大きい値に設定すると、ファイルへのアクセスに遅延が生じ、最終的にタイムアウトする可能性があります。これを回避するには、を値より5秒短く `scanner-pool request-timeout`設定し `scan-engine timeout`ます。設定の変更方法については、スキャンエンジンベンダーのマニュアルを参照して `scan-engine timeout`ください。を `scanner-pool timeout`変更するには、`advanced`モードで次のコマンドを使用し、パラメータに適切な値を指定し `request-timeout`ます。
`vserver vscan scanner-pool modify`
- オンアクセススキャンのワークロード向けにサイジングされていて、オンデマンドスキャンの使用が必要な環境では、NetAppでは、既存のウィルス対策インフラへの負荷の増大を避けるために、オンデマンドスキャンジョブをオフピークの時間帯にスケジュールすることを推奨しています。

パートナー様固有のベストプラクティスの詳細については、を参照してください"Vscanパートナーソリューション"。

SVM ONTAP Vscanでウイルススキャンを有効にする

オンアクセススキャンまたはオンデマンドスキャンを実行するには、SVMでウィルススキャンを有効にする必要があります。

手順

1. SVMでウィルススキャンを有効にします。

   `vserver vscan enable -vserver data_SVM`

   の詳細については `vserver vscan enable`、を"ONTAPコマンド リファレンス"参照してください。

   > 必要に応じて、コマンドを使用してウィルススキャンを無効にできます `vserver vscan disable`。の詳細については `vserver vscan disable`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、SVMでウィルススキャンを有効にし `vs1`ます。

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. SVMでウィルススキャンが有効になっていることを確認します。

   `vserver vscan show -vserver data_SVM`

   の詳細については `vserver vscan show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、SVMのVscanステータスを表示し `vs1`ます。

   ```
   cluster1::> vserver vscan show -vserver vs1

                               Vserver: vs1
                          Vscan Status: on
   ```

ONTAP Vscanでスキャンしたファイルのステータスをリセットする

SVMでスキャンに成功したファイルのスキャンステータスをリセットする必要がある場合は、コマンドを使用して `vserver vscan reset`キャッシュされているファイル情報を破棄します。このコマンドを使用すると、たとえばスキャンの設定が正しくない場合にウィルススキャン処理を再開できます。の詳細については `vserver vscan reset`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

コマンドの実行後、 `vserver vscan reset`対象となるすべてのファイルが次回アクセスされたときにスキャンされます。

> このコマンドを使用すると、再スキャンするファイルの数やサイズによっては、パフォーマンスが低下する可能性があります。

開始する前に

このタスクには高度なPrivilegesが必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

   の詳細については `set -privilege advanced`、を"ONTAPコマンド リファレンス"参照してください。

2. スキャン済みファイルのステータスをリセットします。

   ```
   vserver vscan reset -vserver data_SVM
   ```

   次のコマンドは、SVMのスキャン済みファイルのステータスをリセットし `vs1`ます。

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

ONTAPを使用したVscanイベントログ情報の表示

コマンドを使用すると、感染したファイルやVscanサーバの更新などに関するイベントログ情報を表示できます `vserver vscan show-events`。クラスタ、特定のノード、SVM 、または Vscan サーバについてのイベント情報を表示できます。

開始する前に

Vscanイベントログを表示するには、Advanced Privilegesが必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

   の詳細については `set`、を"ONTAPコマンド リファレンス"参照してください。

2. Vscanイベントログ情報を表示します。

   ```
   vserver vscan show-events
   ```

   の詳細については `vserver vscan show-events`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、クラスタのイベントログ情報を表示し `cluster1`ます。

```
cluster1::*> vserver vscan show-events

Vserver     Node              Server          Event Type         Event Time
----------- ---------------- --------------- ------------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

接続の問題の監視とトラブルシューティング

スキャン必須オプションに関連する潜在的な **ONTAP Vscan** 接続の問題

コマンドを使用すると、接続の問題のトラブルシューティングに役立つVscanサーバ接続に関する情報を確認できます `vserver vscan connection-status show`。

デフォルトでは、オンアクセススキャンのオプションを使用する `scan-mandatory`と、Vscanサーバ接続をスキャンに使用できない場合にファイルアクセスが拒否されます。このオプションは重要な安全機能を備えていますが、いくつかの状況で問題が発生する可能性があります。

- クライアントアクセスを有効にする前に、 LIF が設定された各ノードの SVM に少なくとも 1 つの Vscan サーバが接続されていることを確認する必要があります。クライアントアクセスを有効にしたあとにSVMにサーバを接続する必要がある場合は、SVMでオプションをオフにして、Vscanサーバ接続を使用できないためにファイルアクセスが拒否されないようにする必要があります `scan-mandatory`。サーバの接続が完了したら、オプションをオンに戻すことができます。
- 1 つのターゲット LIF で SVM のすべての Vscan サーバ接続をホストしている場合、その LIF を移行するとサーバと SVM の間の接続が失われます。Vscanサーバ接続を使用できないためにファイルアクセスが拒否されないようにするには、LIFを移行する前にオプションをオフにする必要があり `scan-mandatory`ます。LIF の移行が完了したら、オプションをオンに戻すことができます。

各 SVM に少なくとも 2 つの Vscan サーバを割り当てる必要があります。ストレージシステムへの Vscan サーバの接続には、クライアントアクセスとは別のネットワークを使用することを推奨します。

の詳細については `vserver vscan connection-status show`、を"ONTAPコマンド リファレンス"参照してください。

Vscan サーバの接続ステータスを表示するための **ONTAP** コマンド

コマンドを使用すると、Vscanサーバの接続ステータスに関する概要と詳細情報を表示できます `vserver vscan connection-status show`。

状況	入力するコマンド
Vscanサーバ接続の概要を表示する	`vserver vscan connection-status show`
Vscanサーバ接続の詳細を表示する	`vserver vscan connection-status show-all`
接続されているVscanサーバの詳細を表示する	`vserver vscan connection-status show-connected`
未接続の使用可能なVscanサーバの詳細を表示する	`vserver vscan connection-status show-not-connected`

の詳細については `vserver vscan connection-status show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP Vscanスキャンによるウイルスのトラブルシューティング

一般的なウイルススキャンの問題については、考えられる原因と解決方法があります。ウィルススキャンはVscanとも呼ばれます。

問題	解決方法
VscanサーバをClustered ONTAPストレージシステムに接続できません。	スキャナプールの設定でVscanサーバのIPアドレスが指定されているかどうかを確認します。また、スキャナプールのリストで許可されている特権ユーザがアクティブかどうかも確認します。スキャナプールを確認するには、ストレージシステムのコマンドプロンプトでコマンドを実行し `vserver vscan scanner-pool show`ます。それでもVscanサーバが接続できない場合は、ネットワークに問題がある可能性があります。
クライアントで高レイテンシが観察されます。	スキャナプールにVscanサーバを追加するタイミングが来たと考えられます。
トリガーされたスキャンが多すぎます。	パラメータの値を変更し `vscan-fileop-profile`て、ウィルススキャンの対象として監視するファイル操作の数を制限します。
一部のファイルがスキャンされていません。	オンアクセスポリシーを確認します。これらのファイルのパスがパス除外リストに追加されているか、ファイルのサイズが除外の設定値を超えている可能性があります。オンアクセスポリシーを確認するには、ストレージシステムのコマンドプロンプトでコマンドを実行し `vserver vscan on-access-policy show`ます。

ファイルアクセスが拒否されました。	ポリシー設定で_scan-mandatory_settingが指定されているかどうかを確認します。この設定では、Vscanサーバが接続されていない場合にデータアクセスが拒否されます。必要に応じて設定を変更します。

関連情報

- "vserver vscan scanner-pool showのコマンド"
- "vserver vscan on-access-policy showを使用します"

ONTAP Vscanのステータスとパフォーマンスアクティビティを監視する

Vscanサーバの接続ステータス、Vscanサーバの健常性、スキャンされたファイル数など、Vscanモジュールの重要な要素を監視できます。この情報は、Vscanサーバに関連する問題を診断する際に役立ちます。

Vscanサーバの接続情報の表示

Vscanサーバの接続ステータスを表示して、使用中の接続や使用可能な接続を管理できます。Vscanサーバの接続ステータスに関する情報は、さまざまなコマンドで表示されます。

コマンド…	表示される情報…
`vserver vscan connection-status show`	接続ステータスの概要
`vserver vscan connection-status show-all`	接続ステータスに関する詳細情報
`vserver vscan connection-status show-not-connected`	使用可能だが未接続の接続のステータス
`vserver vscan connection-status show-connected`	接続されているVscanサーバに関する情報

の詳細については `vserver vscan connection-status show`、を"ONTAPコマンド リファレンス"参照してください。

Vscanサーバの統計の表示

Vscanサーバ固有の統計情報を表示して、パフォーマンスを監視し、ウイルススキャンに関連する問題を診断できます。この機能を使用する前に、データサンプルを収集する必要があります。 `statistics show` Vscan サーバーの統計情報を表示するコマンド。

の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

データサンプルを完了するには、次の手順を実行します。

ステップ

1. コマンドとオプションのコマンドを `statistics stop`実行します `statistics start`。

   詳細はこちら `statistics start`そして `statistics stop`の中で"ONTAPコマンド リファレンス" 。

Vscanサーバ要求とレイテンシの統計を表示する

ONTAPカウンタをSVM単位で使用し `offbox_vscan`て、1秒あたりに送出および受信されるVscanサーバ要求の割合、およびすべてのVscanサーバのサーバレイテンシを監視できます。これらの統計を表示するには、次の手順を実行します。

ステップ

1. 次のカウンタを指定してコマンドを実行し `statistics show -object offbox_vscan –instance SVM`ます。

カウンタ…	表示される情報…
scan_request_dispatched_rate	ONTAPからVscanサーバに送信される1秒あたりのウィルススキャン要求数
scan_noti_received_rate	ONTAPがVscanサーバから受信した1秒あたりのウィルススキャン要求数
dispatch_latency	使用可能なVscanサーバを特定してそのVscanサーバに要求を送信するためのONTAP内のレイテンシ
scan_latency	ONTAPからVscanサーバへのラウンドトリップレイテンシ（スキャンの実行時間を含む）

ONTAP外部Vscanカウンタから生成される統計の例

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

個 々 の**Vscan**サーバ要求とレイテンシの統計を表示する

SVM単位、オフボックスのVscanサーバ単位、およびノード単位でONTAPカウンタを使用して、各Vscanサーバでディスパッチされ`Vscan`サーバ要求の速度とサーバレイテンシを個別に監視できます `offbox_vscan_server`。この情報を収集するには、次の手順を実行します。

ステップ

1. 次のカウンタを指定してコマンドを実行し `statistics show –object offbox_vscan –instance SVM:servername:nodename`ます。

カウンタ…	表示される情報…
`scan_request_dispatched_rate`	ONTAPから送信されたウィルススキャン要求の数
`scan_latency`	ONTAPからVscanサーバへのラウンドトリップレイテンシ（Vscanサーバでのスキャンの1秒あたりの実行時間を含む）

ONTAP offbox_vscan_serverカウンタで生成される統計の例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

Vscanサーバ使用率の統計を表示する

ONTAPカウンタを使用して、Vscanサーバ側の利用率の統計を収集することもできます `offbox_vscan_server`。これらの統計は、SVM単位、オフボックスのVscanサーバ単位、ノード単位で追跡されます。これには、VscanサーバでのCPU利用率、Vscanサーバでのスキャン処理のキュー深度（現在と最大の両方）、使用済みメモリ、使用済みネットワークが含まれます。これらの統計は、Antivirus ConnectorによってONTAP内の統計カウンタに転送されます。これらの値は、20秒ごとにポーリングされるデータに基づいており、正確に収集するために複数回収集する必要があります。収集されていない場合、統計に表示される値は最後のポーリングのみを反映します。CPU利用率とキューは、監視と分析に特に重要です。平均キューの値が大きい場合は、Vscanサーバがボトルネックになっている可能性があります。SVM単位、オフボックスVscanサーバ単位、およびノード単位でVscanサーバの利用率の統計を収集するには、次の手順を実行します。

ステップ

1. Vscanサーバの使用率の統計を収集します。

次のカウンタを指定してコマンドを `offbox_vscan_server`実行し `statistics show –object offbox_vscan_server –instance SVM:servername:nodename`ます。

カウンタ…	表示される情報…
`scanner_stats_pct_cpu_used`	VscanサーバのCPU利用率
`scanner_stats_pct_input_queue_avg`	Vscanサーバのスキャン要求の平均キュー
`scanner_stats_pct_input_queue_hiwatermark`	Vscanサーバのスキャン要求のピーク キュー
`scanner_stats_pct_mem_used`	Vscanサーバの使用済みメモリ
`scanner_stats_pct_network_used`	Vscanサーバの使用済みネットワーク

Vscanサーバの利用率に関する統計の例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-------------------------------------------------------------------
```

関連情報

- "ONTAPコマンド リファレンス"

SVMでのNASイベントの監査

SMBプロトコルとNFSプロトコル両方のONTAPを使用したファイルアクセスの監査について

ONTAPのSMBプロトコルおよびNFSプロトコルで使用できるファイルアクセス監査機能

（標準の監査やFPolicyを使用したファイルポリシー管理など）を使用できます。

SMBおよびNFSのファイルアクセスイベントの監査は、次のような場合に設計し、実装する必要があります。

- SMBプロトコルとNFSプロトコルの基本的なファイルアクセスが設定されている。
- 次のいずれかの方法を使用して監査の設定を作成および管理する。
  - ONTAPの標準機能
  - ガイブFPolicyサーバ

SVMでのNASイベントの監査

NASイベントの監査は、Storage Virtual Machine（SVM）で特定のSMBおよびNFSイベントを追跡してログに記録できるセキュリティ対策です。これにより、潜在的なセキュリティの問題を追跡し、セキュリティ違反の証拠を提供できます。また、Active Directoryの集約型アクセスポリシーをステージングおよび監査して、それらを実装した場合の結果を確認することもできます。

SMBイベント

次のイベントを監査できます。

- SMBフアイルオヨヒフオルタアクセスイヘント

  監査が有効になっているSVMに属するFlexVol上に格納されているオブジェクトに対するSMBのファイルおよびフォルダアクセスイベントを監査できます。

- SMBロクオンオヨヒログオフイヘント

  SVM上のSMBサーバでのSMBログオンおよびログオフイベントを監査できます。

- 集約型アクセスポリシーのステージングイベント

  提案された集約型アクセスポリシーによって適用された権限を使用して、SMBサーバ上のオブジェクトの有効なアクセスを監査できます。集約型アクセスポリシーのステージングによる監査では、集約型アクセスポリシーを導入する前に、その影響を確認できます。

  集約型アクセスポリシーのステージングによる監査は、Active DirectoryのGPOを使用してセットアップされます。ただし、SVMの監査の設定は、集約型アクセスポリシーのステージングイベントを監査するように設定する必要があります。

  監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。

NFSイベント

ファイルおよびディレクトリイベントを監査するには、SVMに格納されているオブジェクトのNFSv4 ACLを使用します。

監査の仕組み

ONTAP監査の基本概念

ONTAP の監査について理解するために、監査の基本概念を確認しておく必要があります。

- * ステージングファイル *

  統合および変換の前に監査レコードが格納される、個々のノード上の中間バイナリファイル。ステージングファイルはステージングボリュームに格納されます。

- * ステージングボリューム *

  ステージングファイルを格納するために ONTAP によって作成される専用ボリューム。各アグリゲートに1つのステージングボリュームがあります。ステージングボリュームは、そのアグリゲート内のデータボリュームを対象としたデータアクセスの監査レコードを格納するために、監査が有効なすべての Storage Virtual Machine （ SVM ）で共有されます。各 SVM の監査レコードは、ステージングボリューム内の個別のディレクトリに格納されます。

  クラスタ管理者はステージングボリュームに関する情報を表示できますが、それ以外のほとんどのボリューム操作は実行できません。ステージングボリュームを作成できるのは ONTAP のみです。ONTAP では、ステージングボリュームに自動的に名前が割り当てられます。すべてのステージングボリューム名はで始まり `MDV_aud_`、そのあとにステージングボリュームを含むアグリゲートのUUIDが続きます（例：`MDV_aud_1d0131843d4811e296fc123478563412`）。

- * システムボリューム *

  ファイルサービスや監査ログのメタデータなど、特別なメタデータを格納する FlexVol ボリューム。システムボリュームの所有者は管理 SVM であり、システムボリュームはクラスタ全体で表示されます。ステージングボリュームはシステムボリュームの一種です。

- * 統合タスク *

  監査が有効になったときに作成されるタスク。各 SVM で長時間にわたって実行されるこのタスクは、SVM のメンバーノード全体のステージングファイルから監査レコードを取得します。このタスクでは、監査レコードを時間順にソートしてマージし、監査設定で指定されたユーザが読解可能なイベントログ形式（EVTXファイル形式またはXMLファイル形式）に変換します。変換されたイベントログは、 SVM 監査の設定で指定された監査イベントログディレクトリに格納されます。

ONTAP監査プロセスの機能について説明します。

ONTAPの監査プロセスは、Microsoftの監査プロセスとは異なります。監査を設定する前に、ONTAP監査プロセスの仕組みを理解しておく必要があります。

監査レコードは、最初に個 々 のノードのバイナリステージングファイルに格納されます。あるSVMで監査が有効になると、すべてのメンバーノードでそのSVMのステージングファイルが保持されます。定期的に統合され、ユーザが読解可能なイベントログに変換されて、SVMの監査イベントログディレクトリに格納されます。

あるSVMで監査が有効になっている場合の処理

監査はSVMでのみ有効にできます。ストレージ管理者がSVMで監査を有効にすると、監査サブシステムによってステージングボリュームが存在するかどうかが確認されます。ステージングボリュームは、SVMに所有されているデータボリュームを含むアグリゲートごとに必要です。存在しない場合は、監査サブシステムによって、必要なステージングボリュームが作成されます。

また、監査が有効になる前に、前提条件となるその他のタスクが実行されます。

- 監査サブシステムによって、ログ ディレクトリのパスが使用可能でシンボリック リンクが含まれていないことが検証されます。

  ログ ディレクトリは、SVMのネームスペース内のパスとしてすでに存在している必要があります。監査ログ ファイルの保存用に新しいボリュームまたはqtreeを作成することを推奨します。監査サブシステムは、デフォルトのログ ファイルの場所を割り当てません。監査の設定で指定されているログディレクトリのパスが有効なパスでないと、エラーが表示されて監査の設定の作成に失敗します `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"`。

  ディレクトリは存在しているがシンボリックリンクが含まれている場合、設定の作成に失敗します。

- 監査によって統合タスクがスケジュールされます。

  このタスクがスケジュールされたあと、監査が有効になります。SVMの監査設定とログ ファイルは、リブート後も、NFSサーバまたはSMBサーバが停止したり再起動したりした場合も維持されます。

イベント ログの統合

ログの統合は、監査が無効になるまで定期的に実行されるスケジュール済みタスクです。監査が無効になると、統合タスクによって残りのすべてのログが統合されたことが検証されます。

監査の保証

デフォルトでは、監査が保証されています。ONTAPでは、あるノードが利用できない場合でも、監査可能なファイル アクセス イベント（設定された監査ポリシーのACLで指定されている）はすべて記録されます。要求されたファイル処理は、その処理の監査レコードが永続的ストレージのステージング ボリュームに保存されるまで完了できません。スペース不足またはその他の問題が原因で監査レコードをディスクのステージング ファイルにコミットできない場合、クライアント処理は拒否されます。

> 管理者または特権レベルのアクセス権を持つアカウント ユーザは、NetApp Manageability SDKまたはREST APIを使用してファイル監査ログ処理をバイパスできます。NetApp Manageability SDKまたはREST APIを使用してファイル操作が実行されたかどうかを確認するには、ファイルに保存されているコマンド履歴ログを確認し `audit.log`ます。
>
> コマンド履歴監査ログの詳細については、の「管理アクティビティの監査ログの管理」セクションを参照してください"システム管理"。

ノードが使用できない場合の統合プロセス

監査が有効になっているSVMに属するボリュームを含むノードが利用できない場合、監査の統合タスクの動作は、そのノードのストレージフェイルオーバー（SFO）パートナー（2ノードクラスタの場合はHAパートナー）が利用可能かどうかによって異なります。

- ステージングボリュームがSFOパートナー経由で使用可能な場合は、ノードから最後に報告されたステージングボリュームがスキャンされ、統合が正常に行われます。
- SFOパートナーを使用できない場合は、部分的なログファイルが作成されます。

  あるノードにアクセスできない場合は、統合タスクによって、そのSVMの使用可能な他のノードの監査レコードが統合されます。完了していないことを識別するために、統合ファイル名にサフィックスが追加され `.partial`ます。

- 利用できないノードが利用可能になったら、そのノードの監査レコードが、その時点における他のノードの監査レコードと統合されます。
- 監査レコードはすべて維持されます。

イベント ログのローテーション

監査イベント ログ ファイルは、設定されたログ サイズしきい値に達した場合に、または設定されたスケジュールに従ってローテーションされます。イベント ログ ファイルがローテーションされると、スケジュールされた統合タスクによって、まず、アクティブな変換済みファイルの名前がタイムスタンプのあるアーカイブ ファイルに変更され、そのあとで新しいアクティブな変換済みイベント ログ ファイルが作成されます。

SVMで監査が無効になっている場合の処理

SVMで監査が無効になると、もう一度統合タスクがトリガーされます。未処理の記録済みの監査レコードはすべて、ユーザが読解可能な形式でログに記録されます。SVMで監査が無効になっても、イベント ログ ディレクトリに格納されている既存のイベント ログは削除されず、参照が可能です。

そのSVMの既存のステージング ファイルがすべて統合されたら、スケジュールから統合タスクが削除されます。SVMの監査設定を無効にしても、監査設定は削除されません。ストレージ管理者は、監査をいつでも再度有効にできます。

監査の統合ジョブは、監査が有効になったときに作成され、統合タスクを監視して、統合タスクがエラーによって終了した場合に統合タスクを再作成します。ユーザが監査の統合ジョブを削除することはできません。

ONTAP監査の前提条件

Storage Virtual Machine（SVM）で監査を設定して有効にする前に、一定の要件と考慮事項について確認しておく必要があります。

- NFS監査が有効になっているSVMとS3監査が有効になっているSVMの合計数は、ONTAPのバージョンによって異なります。

ONTAPのバージョン	最大
9.8以前	50
9.9.1以降	400

- 監査は、SMBまたはNFSのライセンスとは関係ありません。

  クラスタにSMBとNFSのライセンスがインストールされていない場合でも、監査を設定して有効にすることができます。

- NFS監査では、セキュリティACE（タイプU）がサポートされます。

- NFS監査では、モードビットと監査ACEの間のマッピングはありません。

  ACLをモードビットに変換する場合、監査ACEはスキップされます。モードビットをACLに変換する場合、監査ACEは生成されません。

- 監査の設定で指定するディレクトリが存在している必要があります。

  存在しない場合、監査の設定を作成するコマンドは失敗します。

- 監査の設定で指定するディレクトリは、次の要件を満たしている必要があります。
  - ディレクトリにシンボリックリンクを含めることはできません。

    監査の設定で指定されたディレクトリにシンボリックリンクが含まれている場合、監査の設定を作成するコマンドは失敗します。

  - 絶対パスを使用してディレクトリを指定する必要があります。

    相対パス（など）は指定しないで `/vs1/../`ください。

- 監査は、ステージングボリューム内に利用可能なスペースがあるかどうかによって異なります。

  監査対象のボリュームを含むアグリゲート内のステージングボリュームに十分なスペースを確保するための計画を把握しておく必要があります。

- 監査は、変換されたイベントログの格納先ディレクトリを含むボリューム内に利用可能なスペースがあるかどうかに依存します。

  イベントログの格納に使用するボリュームに十分なスペースを確保するための計画を把握しておく必要があります。監査ディレクトリに保持するイベントログの数は、監査の設定の作成時にパラメータを使用して指定でき `-rotate-limit`ます。これは、ボリューム内のイベントログ用に十分なスペースを確保するのに役立ちます。

- 監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントを生成するには、ダイナミックアクセス制御を有効にする必要があります。

  ダイナミックアクセス制御は、デフォルトでは有効になっていません。

監査を有効にする際のアグリゲートスペースに関する考慮事項

監査の設定が作成され、クラスタ内の少なくとも1つのStorage Virtual Machine（SVM）で監査が有効になっている場合、監査サブシステムは、既存のすべてのアグリゲートと、作成されるすべての新しいアグリゲートにステージングボリュームを作成します。クラスタで監査を有効にする場合は、アグリゲートスペースに関する考慮事項について理解しておく必要があります。

アグリゲートにスペースがないと、ステージングボリュームの作成に失敗することがあります。これは、監査の設定を作成し、既存のアグリゲートにステージングボリュームを格納できるだけの十分なスペースがない場合に発生することがあります。

SVMで監査を有効にする前に、既存のアグリゲートにステージングボリューム用の十分なスペースがあることを確認する必要があります。

ONTAP監査レコードのステージングファイルのサイズ制限

ステージングファイルの監査レコードのサイズは32KB以下にする必要があります。

監査レコードが大規模になる状況

管理監査中に、次のいずれかの状況で監査レコードが大量に発生する可能性があります。

- 多数のユーザを含むグループに対してユーザを追加または削除します。
- 多数のファイル共有ユーザがいるファイル共有に対するファイル共有のAccess Control List（ACL；アクセス制御リスト）の追加または削除。
- その他のシナリオ。

この問題を回避するには、管理監査を無効にしてください。これを行うには、監査設定を変更し、監査イベントタイプのリストから次の項目を削除します。

- ファイル共有
- ユーザアカウント
- セキュリティグループ
- 認証ポリシー変更

  削除した項目はファイルサービスの監査サブシステムで監査されなくなります。

監査レコードが大きすぎる場合の影響

- 監査レコードのサイズが大きすぎる（32KBを超える）と、監査レコードは作成されず、監査サブシステムによって次のようなイベント管理システム（EMS）メッセージが生成されます。

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  監査が保証されている場合、監査レコードを作成できないためにファイル処理が失敗します。

- 監査レコードのサイズが9、999バイトを超える場合は、上記と同じEMSメッセージが表示されます。大きいキー値が指定されていない部分的な監査レコードが作成されます。
- 監査レコードが 2 、 000 文字を超えている場合は、実際の値ではなく次のエラーメッセージが表示されます。

  ```
  The value of this field was too long to display.
  ```

ONTAP監査イベントログでサポートされる形式について

変換された監査イベントログでサポートされるファイル形式は、 `EVTX`および `XML`ファイル形式です。

監査の設定を作成する際には、ファイル形式の種類を指定できます。デフォルトでは、ONTAPはバイナリロ

グをファイル形式に変換し`EVTX`ます。

ONTAP監査イベントログの表示と処理

監査イベントログを使用して、ファイルセキュリティが適切であるかどうか、およびファイルやフォルダへの不適切なアクセス試行が行われたかどうかを確認できます。または`XML`ファイル形式で保存された監査イベントログを表示および処理できます`EVTX`。

- `EVTX`ファイル形式

  変換された監査イベントログは、保存されたファイルとしてMicrosoftイベントビューアを使用して開くことができます`EVTX`。

  イベントビューアを使用してイベントログを表示する場合は、次の2つのオプションを使用できます。

  - 全般表示

    イベントレコードについては、すべてのイベントに共通の情報が表示されます。このバージョンのONTAPでは、イベントレコードのイベント固有のデータは表示されません。詳細ビューを使用すると、イベント固有のデータを表示できます。

  - 詳細ビュー

    フレンドリビューとXMLビューを使用できます。フレンドリビューとXMLビューには、すべてのイベントに共通する情報とイベントレコードのイベント固有のデータの両方が表示されます。

- `XML`ファイル形式

  監査イベントログは、ファイル形式をサポートする他社製アプリケーションで`XML`表示および処理できます`XML`。XMLスキーマとXMLフィールドの定義に関する情報があれば、XML表示ツールを使用して監査ログを表示できます。XMLスキーマと定義の詳細については、を参照してください "ONTAP 監査スキーマリファレンス"。

イベントビューアを使用したアクティブな監査ログの表示方法

クラスタで監査の統合プロセスを実行している場合は、統合プロセスによって、監査を有効にしたStorage Virtual Machine（SVM）のアクティブな監査ログファイルに新しいレコードが追加されます。このアクティブな監査ログは、SMB共有を介してMicrosoftイベントビューアでアクセスして開くことができます。

イベントビューアには、既存の監査レコードの表示に加えて、コンソールウィンドウの内容を更新できる更新オプションがあります。アクティブな監査ログへのアクセスに使用される共有でoplockが有効になっているかどうかに応じて、新たに追加されたログをイベントビューアで表示できるかどうかが異なります。

共有での oplock の設定	動作
有効	イベントビューアは、その時点までに書き込まれたイベントを含むログを開きます。更新処理では、統合プロセスで追加された新しいイベントでログが更新されません。

無効にする	イベントビューアは、その時点までに書き込まれたイベントを含むログを開きます。更新処理を実行すると、ログが更新され、統合プロセスで追加された新しいイベントが表示されます。

この情報は、イベントログにのみ適用され `EVTX`ます。 `XML`イベントログは、SMBを介してブラウザで、または任意のXMLエディタまたはビューアを使用してNFSで表示できます。

カンサテキルSMBイヘント

ONTAPで結果を解釈するために監査できる**SMB**イベントについて説明します。

ONTAPでは、ファイルおよびフォルダのアクセスイベント、ログオンおよびログオフイベント、集約型アクセスポリシーのステージングイベントなど、特定のSMBイベントを監査できます。どのアクセスイベントを監査できるかを把握しておくと、イベントログの結果を解釈するときに役立ちます。

次の追加の SMB イベントを監査できます。

イベント ID （ EVT / EVTX ）	イベント	説明	カテゴリ
4670	オブジェクト権限の変更	オブジェクトアクセス：権限が変更された。	ファイルアクセス
4907	オブジェクトの監査設定の変更	オブジェクトアクセス：監査設定が変更された。	ファイルアクセス
4913	オブジェクトの集約型アクセスポリシーの変更	オブジェクトへのアクセス： CAP が変更された。	ファイルアクセス

ONTAP 9 .0以降では、次のSMBイベントを監査できます。

イベント ID （ EVT / EVTX ）	イベント	説明	カテゴリ
540/4624	アカウントが正常にログオンしました	ログオン/ログオフ：ネットワーク（SMB）ログオン。	ログオンおよびログオフ
529/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザ名が不明またはパスワードが無効です。	ログオンおよびログオフ
530/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：アカウントログオンの時間制限です。	ログオンおよびログオフ
531/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：アカウントは現在無効になっています。	ログオンおよびログオフ

532/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザアカウントの有効期限が切れています。	ログオンおよびログオフ
533/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザはこのコンピュータにログオンできません。	ログオンおよびログオフ
534/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザはログオンを許可されていません。	ログオンおよびログオフ
535/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザのパスワードが期限切れです。	ログオンおよびログオフ
537/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：上記以外の理由でログオンが失敗しました。	ログオンおよびログオフ
539/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：アカウントのロックアウト。	ログオンおよびログオフ
538/4634	アカウントがログオフされました	ログオン / ログオフ：ローカルまたはネットワークユーザのログオフ。	ログオンおよびログオフ
560/4656	オブジェクトを開く/オブジェクトを作成	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）が開きます。	ファイルアクセス
563/4659	削除するためのオブジェクトを開く	オブジェクトへのアクセス：削除するためにオブジェクト（ファイルまたはディレクトリ）へのハンドルが要求された。	ファイルアクセス
564 / 4660	オブジェクトの削除	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）を削除します。ONTAP は、Windowsクライアントがオブジェクト（ファイルまたはディレクトリ）を削除しようとしたときにこのイベントを生成します。	ファイルアクセス

567/4663	オブジェクトの読み取り / オブジェクトの書き込み / オブジェクトの属性の取得 / オブジェクトの属性の設定	オブジェクトへのアクセス：オブジェクトへのアクセスの試み（読み取り、書き込み、属性の取得、属性の設定）。 • 注： * このイベントでは、ONTAP はオブジェクトに対する最初の SMB 読み取り操作と SMB 書き込み操作（の成功または失敗）を監査します。これにより、単一のクライアントがオブジェクトを開き、同じオブジェクトに対して連続して多数の読み取りまたは書き込み処理を実行しても、ONTAPが過剰なログエントリを作成するのを防ぐことができます。	ファイルアクセス
NA / 4664	ハードリンク	オブジェクトへのアクセス：ハードリンクの作成が試行されました。	ファイルアクセス
NA / 4818	提案された集約型アクセスポリシーで現在の集約型アクセスポリシーと同じアクセス権限が付与されない	オブジェクトへのアクセス：集約型アクセスポリシーのステージング。	ファイルアクセス
NA/NA Data ONTAP イベントID 9999	オブジェクトの名前変更	オブジェクトへのアクセス：オブジェクトの名前変更。これはONTAPイベントです。Windowsでは現在、単一イベントとしてサポートされていません。	ファイルアクセス
NA/NA Data ONTAP イベントID 9998	オブジェクトのリンク解除	オブジェクトへのアクセス：オブジェクトのリンクが解除される。これはONTAPイベントです。Windowsでは現在、単一イベントとしてサポートされていません。	ファイルアクセス

イベント**4656**に関する追加情報

`HandleID`監査イベントのタグ
`XML`には、アクセスされたオブジェクト（ファイルまたはディレクトリ）のハンドルが含まれています。 `HandleID`EVTX
4656イベントのタグには、オープンイベントが新しいオブジェクトを作成するためのものか、既存のオブジェクトを開くためのものかによって、異なる情報が含まれます。

- openイベントが新しいオブジェクト（ファイルまたはディレクトリ）を作成するためのオープン要求であ

る場合、監査XMLイベントのタグには HandleID`空（例： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>）が表示されます HandleID。

が HandleID`空になっているのは、（新しいオブジェクトを作成するための）OPEN要求が、実際のオブジェクトの作成が行われる前、およびハンドルが存在する前に監査されるためです。同じオブジェクトの後続の監査対象イベントは、タグ内に適切なオブジェクトハンドルを持ちます `HandleID。

- openイベントが既存のオブジェクトを開くためのオープン要求である場合、監査イベントにはそのオブジェクトの割り当てられたハンドルがタグに含まれ HandleID`ます（例： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>）。

ONTAP監査対象オブジェクトへの完全なパスを決定する

監査レコードのタグに出力されたオブジェクトパス `<ObjectName>`には、ボリュームの名前（かっこ内）と、ボリュームを含むボリュームのルートからの相対パスが表示されます。ジャンクションパスを含む監査対象オブジェクトの完全パスを決定する場合には、実行する必要がある特定の手順があります。

手順

1. 監査イベントのタグを確認して、ボリューム名と監査対象オブジェクトへの相対パスを確認します <ObjectName>。

   この例では、ボリューム名は「data1」で、ファイルへの相対パスはです /dir1/file.txt。

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. 前の手順で確認したボリューム名を使用して、監査対象オブジェクトが含まれているボリュームのジャンクションパスを確認します。

   この例では、ボリューム名は「data1」で、監査対象オブジェクトを含むボリュームのジャンクションパスはです。 /data/data1

   ```
   volume show -junction -volume data1
   ```

   ```
                                Junction                       Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. タグ内の相対パスをボリュームのジャンクションパスに追加して、監査対象オブジェクトへの完全パスを決定します <ObjectName>。

   この例では、ボリュームのジャンクションパスは次のようになります。

   ```
   /data/data1/dir1/file.text
   ```

シンボリックリンクおよびハードリンクの**ONTAP**監査について

シンボリックリンクおよびハードリンクを監査する場合は、一定の考慮事項に注意する必要があります。

監査レコードには、タグで識別される監査対象オブジェクトのパスなど、監査対象オブジェクトに関する情報が含まれます。 `ObjectName`シンボリックリンクおよびハードリンクのパスがタグにどのように記録されるかを確認しておく必要があります `ObjectName`。

シンボリックリンク

シンボリックリンクとは、ターゲットと呼ばれるデスティネーションオブジェクトの場所へのポインタを含む、独立した inode を持つファイルです。シンボリックリンクを介してオブジェクトにアクセスする際、ONTAP は、シンボリックリンクを自動的に解釈し、ボリューム内のターゲットオブジェクトへの、プロトコルに依存しない本来のパスに従います。

次の出力例には、2つのシンボリックリンクがあり、どちらもという名前のファイルを指して `target.txt`います。一方のシンボリックリンクは相対シンボリックリンクであり、他方は絶対シンボリックリンクです。どちらかのシンボリックリンクが監査された場合、 `ObjectName`監査イベントのタグにファイルへのパスが含まれ `target.txt`ます。

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

ハードリンク

ハードリンクは、ファイルシステム上の既存のファイルに名前を関連付けるディレクトリエントリです。ハードリンクは元のファイルの inode の場所を指しています。ONTAP ONTAP は、シンボリックリンクの解釈方法と同様に、ハードリンクを解釈し、ボリューム内のターゲットオブジェクトへの本来のパスに従います。ハードリンクオブジェクトへのアクセスが監査されると、監査イベントはハードリンクパスではなく、この正規の絶対パスをタグに記録します `ObjectName`。

代替**NTFS**データストリームの**ONTAP**監査について

NTFS代替データストリームを含むファイルを監査する場合は、一定の考慮事項に注意する必要があります。

監査対象のオブジェクトの場所は、タグ（パス）とタグ（ハンドル）の `HandleID`2つのタグを使用してイベントレコードに記録されます `ObjectName`。ログに記録されているストリーム要求を適切に識別するには、NTFS代替データストリームの次のフィールドにONTAPが記録するものに注意する必要があります。

- EVTX ID ： 4656 のイベント（オープンおよび作成の監査イベント）
  - 代替データストリームのパスはタグに記録され `ObjectName`ます。
  - 代替データストリームのハンドルはタグに記録され `HandleID`ます。

- EVTX ID ： 4663 のイベント（読み取り、書き込み、属性の取得など、その他すべての監査イベント）
  - 代替データストリームではなく、ベースファイルのパスがタグに記録され `ObjectName`ます。
  - 代替データストリームのハンドルはタグに記録され `HandleID`ます。

例

次の例は、タグを使用して代替データストリームのEVTX ID：4663イベントを特定する方法を示してい `HandleID`ます。 `ObjectName`読み取り監査イベントで記録されたタグ（パス）はベースファイルパスに対するものですが、 `HandleID`タグを使用すると、代替データストリームの監査レコードとしてイベントを識別できます。

ストリームファイル名はの形式になり `base_file_name:stream_name`ます。この例では、 `dir1`次のパスを持つ代替データストリームを持つベースファイルがディレクトリに含まれています。

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

次のイベント例の出力は、示されているように省略されています。出力には、イベントで使用可能なすべての出力タグが表示されるわけではありません。

EVTX ID 4656（オープン監査イベント）の場合、代替データストリームの監査レコード出力では、代替データストリーム名がタグに記録され `ObjectName`ます。

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

EVTX ID 4663（読み取り監査イベント）の場合、同じ代替データストリームの監査レコード出力では、ベースファイル名がタグに記録され `ObjectName`ます。ただし、タグ内のハンドルは `HandleID`代替データストリームのハンドルであり、このイベントを代替データストリームと関連付けるために使用できます。

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

NFSファイルおよびディレクトリアクセスイベントのONTAP監査について

ONTAP は、特定の NFS ファイルおよびディレクトリへのアクセスイベントを監査できます。どのようなアクセスイベントを監査できるか理解しておくと、変換された監査イベントログの結果を解釈するときに役立ちます。

監査できるNFSファイルおよびディレクトリへのアクセスイベントは次のとおりです。

- 読み取り
- オープン
- を閉じます
- ディレクトリの読み取り
- 書き込み
- 属性の設定
- 作成
- リンク
- 属性を開く
- 取り外します
- 属性の取得
- 確認します
- 非検証
- 名前の変更

NFS の名前変更イベントを確実に監査するには、ファイルではなくディレクトリに監査 ACE を設定する必要

があります。これは、ディレクトリへのアクセス権がある場合に、名前変更の操作でファイルのアクセス権が確認されないためです。

ONTAP SVMでの監査の設定を計画する

Storage Virtual Machine（SVM）で監査を設定する前に、使用可能な設定オプションを理解し、各オプションに設定する値を計画する必要があります。この情報は、ビジネスニーズを満たす監査の設定に役立ちます。

すべての監査設定に共通の設定パラメータがあります。

また、統合および変換された監査ログのローテーション時に使用する方法を指定するためのパラメータもいくつかあります。監査の設定時に、次の3つの方法のいずれかを指定できます。

- ログサイズに基づくログのローテーション

  ログのローテーションに使用されるデフォルトの方法です。

- スケジュールに基づいたログのローテーション
- ログ サイズとスケジュール（早い方）に基づいたログのローテーション

ログのローテーション方法は必ず指定する必要があります。

すべての監査設定に共通するパラメータ

監査設定の作成時に指定する必要がある2つの必須パラメータがあります。また、指定できるオプションのパラメータが3つあります。

情報の種類	オプション	必須	含める	自分の価値観
SVM 名 _ 監査設定を作成するSVMの名前。SVMがすでに存在している必要があります。	`-vserver vserver_name`	○	○	

_ ログデスティネーションパス _ 変換された監査ログを格納するディレクトリ（通常は専用のボリュームまたはqtree）を指定します。SVMネームスペースにすでに存在しているパスを指定する必要があります。 パスは最大864文字で、読み取り/書き込み権限が必要です。 パスが無効な場合、監査設定コマンドは失敗します。 SVMがSVMディザスタリカバリのソースである場合、ログデスティネーションパスをルートボリュームに配置することはできません。これは、ルートボリュームのコンテンツがディザスタリカバリデスティネーションにレプリケートされないためです。 FlexCacheボリュームをログのデスティネーションとして使用することはできません（ONTAP 9 .7以降）。	`-destination text`	○	○	

_ 監査するイベントのカテゴリ _ 監査するイベントのカテゴリを指定します。監査できるイベント カテゴリは次のとおりです。 • ファイル アクセス イベント（SMBとNFSv4の両方） • SMBロクオンオヨヒログオフイヘント • 集約型アクセスポリシーのステージングイベント 集約型アクセスポリシーのステージングイベントは、Windows Server 2012 Active Directoryドメイン以降で使用できます。 • 非同期-削除 • ファイル共有カテゴリイベント • 監査ポリシー変更イベント • ローカルユーザアカウント管理イベント • セキュリティグループ管理イベント • 認証ポリシー変更イベント デフォルトでは、ファイルアクセスイベントとSMBログオンおよびログオフイベントが監査されます。 *注：*イベントカテゴリとしてを指定するには、 `cap-staging`SVM上にSMBサーバが存在している必要があります。監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。	-events{file-ops	cifs-logon-logoff	cap-staging	file-share
audit-policy-change	user-account	security-group	authorization-policy-change	async-delete}

いいえ			_ ログファイル出力形式 _ 監査ログの出力形式を指定します。出力形式は、ONTAP固有またはMicrosoft Windows `EVTX`ログ形式のいずれかになり`XML`ます。デフォルトの出力形式はです`EVTX`。	-format{xml

evtx}	いいえ			ログファイルのローテーションの上限 _ 保持する監査ログファイルの数を指定します。この数を超えると、最も古いログファイルがローテーションから除外されます。たとえば、の値を入力する `5` と、最後の5つのログファイルが保持されます。 値がの `0` 場合は、すべてのログファイルが保持されます。デフォルト値は0です。

監査イベントログのローテーションのタイミングの決定に使用するパラメータ

- ログサイズに基づいてログを回転 *

デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。

- デフォルトのログサイズは100MBです。
- デフォルトのログローテーション方式とデフォルトのログサイズを使用する場合は、ログローテーションのパラメータを設定する必要はありません。

- ログサイズのみに基づいて監査ログのローテーションを行う場合は、次のコマンドを使用してパラメータの設定を解除し -rotate-schedule-minute`ます。 `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -

デフォルトのログサイズを使用しない場合は、カスタムログサイズを指定するようにパラメータを設定でき `-rotate-size`ます。

情報の種類	オプション	必須	含める	自分の価値観
_ ログファイルサイズ制限 _ 監査ログファイルの最大サイズを決定します。	-rotate-size{integer[KB	MB	GB	TB

- スケジュールに基づいてログを回転 *

スケジュールに基づく監査ログのローテーションを選択した場合は、時間に基づくローテーションパラメータを任意の組み合わせで使用して、ログのローテーションをスケジュールできます。

- 時間に基づくローテーションを使用する場合、 `-rotate-schedule-minute`パラメータは必須です。
- その他の時間ベースのローテーションパラメータはすべてオプションです。
- ローテーションスケジュールは、時間に関連するすべての値を使用して計算されます。

  たとえば、パラメータのみを指定する `-rotate-schedule-minute`と、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。

- 時間に基づくローテーションパラメータを1つか2つだけ指定した場合（、など -rotate-schedule -month -rotate-schedule-minutes）、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

  たとえば、監査ログのローテーションを、1月、3月、8月の月曜日、水曜日、土曜日の午前10時30分に実行するように指定できます。

- との -rotate-schedule-day`両方に値を指定すると `-rotate-schedule-dayofweek、それらは独立して考慮されます。

  たとえば、にFridayを指定し、 `-rotate-schedule-day`に13を指定する `-rotate-schedule-dayofweek`と、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日、および指定した月の13日にも実行されます。

- スケジュールのみに基づいて監査ログのローテーションを行う場合は、次のコマンドを使用してパラメータの設定を解除し -rotate-size`ます。 `vserver audit modify -vserver vs0 -destination / -rotate-size -

次に示す使用可能な監査パラメータのリストを使用して、監査イベントログのローテーションのスケジュールの設定に使用する値を決定できます。

情報の種類	オプション	必須	含める	自分の価値観

ログローテーションスケジュール：Month_ 監査ログのローテーションを実行する月を指定します。 有効な値は `January`、〜 `December`、および `all`です。たとえば、監査ログのローテーションを1月、3月、8月に実行するように指定できます。	`-rotate-schedule-month chron_month`	いいえ		
ログローテーションスケジュール：曜日 _ 監査ログのローテーションを実行する日（曜日）を指定します。 有効な値は `Sunday`、〜 `Saturday`、および `all`です。たとえば、監査ログのローテーションを火曜日と金曜日に、またはすべての曜日に実行するように指定できます。	`-rotate-schedule -dayofweek chron_dayofweek`	いいえ		
ログローテーションスケジュール： Day _ 監査ログのローテーションを実行する日にちを指定します。 有効な値の範囲は `1`〜 `31`です。たとえば、監査ログのローテーションを毎月10日と20日に、またはすべての日に実行するように指定できます。	`-rotate-schedule-day chron_dayofmonth`	いいえ		
ログローテーションスケジュール： Hour _ 監査ログのローテーションを実行する時間単位のスケジュールを決定します。 有効な値の範囲は、 `0`（午前0時）〜 `23`（午後11時）です。を指定する `all`と、監査ログのローテーションが1時間ごとに行われます。たとえば、監査ログのローテーションを6（午前6時）と18（午後6時）に行うように指定できます。	`-rotate-schedule-hour chron_hour`	いいえ		

ログローテーションスケジュール：分 _ 監査ログのローテーションを実行する分を指定します。 有効な値の範囲は 0~ `59`です。たとえば、監査ログのローテーションを30分に行うように指定できます。	`-rotate-schedule-minute chron_minute`	はい（スケジュールベースのログローテーションを設定する場合）。それ以外の場合はいいえ。		

- ログサイズとスケジュールに基づいてログを回転 *

ログサイズとスケジュールに基づいてログファイルをローテーションするように選択するには、パラメータと時間ベースのローテーションパラメータの両方を任意に組み合わせて設定し `-rotate-size`ます。たとえば、が10MBに設定され、 `-rotate-schedule-minute`が15に設定されている場合 `-rotate-size`、ログファイルのサイズが10MBに達したとき、または1時間ごとの15分（いずれか早い方）にログファイルがローテーションされます。

SVMでファイルとディレクトリの監査設定を作成します。

ONTAP SVMでファイルとディレクトリの監査の設定を作成します。

Storage Virtual Machine（SVM）上でファイルとディレクトリの監査の設定を作成するには、使用可能な設定オプションについて理解し、設定を計画し、設定を行って有効にします。その後、監査の設定に関する情報を表示して、設定した設定が適切かどうかを確認できます。

ファイルおよびディレクトリイベントの監査を開始する前に、監査の設定をStorage Virtual Machine（SVM）で作成する必要があります。

開始する前に

集約型アクセスポリシーステージングの監査の設定を作成する場合は、SVM上にSMBサーバが存在している必要があります。

- 監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。

  ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。

- コマンドのフィールドの引数が無効な場合（フィールドのエントリが無効である、エントリが重複している、エントリがないなど）、コマンドは監査フェーズの前に失敗します。

  この場合、監査レコードは生成されません。

タスクの内容

SVMがSVMディザスタリカバリのソースである場合、デスティネーションパスをルートボリュームに配置することはできません。

ステップ

1. 計画ワークシートの情報を使用して、ログサイズまたはスケジュールに基づいて監査ログのローテーションを行うための監査の設定を作成します。

監査ログのローテーションの基準	入力するコマンド
ログサイズ	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
スケジュール	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

例

次の例は、サイズに基づくローテーションを使用してファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログ形式は（デフォルト）です `EVTX`。ログはディレクトリに保存され `/audit_log`ます。ログファイルの最大サイズはです `200 MB`。ログは、サイズが200MBに達するとローテーションされます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

次の例は、サイズに基づくローテーションを使用してファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログ形式は（デフォルト）です `EVTX`。ログはディレクトリに保存され `/cifs_event_logs`ます。ログファイルのサイズの上限は `100 MB`（デフォルト）、ログのローテーションの上限は次のとおり `5`です。

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

次の例は、時間に基づくローテーションを使用してファイル操作、CIFSのログオンおよびログオフイベント、集約型アクセスポリシーのステージングイベントを監査する監査の設定を作成します。ログ形式は（デフ

ォルト）です `EVTX`。監査ログのローテーションは、毎月、すべての曜日の午後12時30分に実行されます。ログのローテーションの上限は次のとおりです `5`。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

関連情報

- "SVMで監査を有効にする"
- "監査の設定を確認する"

監査の設定後に**ONTAP SVM**で監査を有効にする

監査の設定が完了したら、 Storage Virtual Machine （ SVM ）で監査を有効にする必要があります。

開始する前に

SVM の監査設定がすでに存在している必要があります。

タスクの内容

SVM ディザスタリカバリ ID 破棄の設定が（ SnapMirror 初期化完了後に）初めて開始され、 SVM に監査の設定がある場合、 ONTAP は監査の設定を自動的に無効にします。読み取り専用 SVM では、ステージングボリュームがいっぱいにならないように監査が無効になっています。SnapMirror 関係が解除されて SVM が読み書き可能になったあとでないと、監査を有効にすることはできません。

手順

1. SVM で監査を有効にします。

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

関連情報

- "監査の設定を作成する"
- "監査の設定を確認する"

ONTAP監査の設定を確認する

監査の設定が完了したら、監査が適切に設定されて有効になっていることを確認する必要があります。

手順

1. 監査の設定を確認します。

```
vserver audit show -instance -vserver vserver_name
```

次のコマンドは、Storage Virtual Machine（SVM）vs1のすべての監査の設定情報をリスト形式で表示します。

```
vserver audit show -instance -vserver vs1
```

```
                            Vserver: vs1
                  Auditing state: true
            Log Destination Path: /audit_log
   Categories of Events to Audit: file-ops
                     Log Format: evtx
              Log File Size Limit: 200MB
     Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
     Log Rotation Schedule: Hour: -
   Log Rotation Schedule: Minute: -
               Rotation Schedules: -
         Log Files Rotation Limit: 0
```

関連情報

- "監査の設定を作成する"
- "SVMで監査を有効にする"

ファイルおよびフォルダの監査ポリシーを設定する

ONTAP SVMで監査の設定を有効にし、ファイルとフォルダの監査ポリシーを設定する

ファイルおよびフォルダのアクセスイベントの監査は、 2 つのステップで実装します。まず、Storage Virtual Machine（SVM）で監査の設定を作成し、有効にする必要があります。次に、監視するファイルとフォルダに対して監査ポリシーを設定する必要があります。成功したアクセス試行と失敗したアクセス試行の両方を監視するように監査ポリシーを設定できます。

SMB と NFS の両方の監査ポリシーを設定できます。SMB と NFS の監査ポリシーでは、設定の要件や監査の機能が異なります。

適切な監査ポリシーが設定されている場合、 ONTAP は、 SMB または NFS サーバの稼働中に限り、監査ポリシーでの指定に従って SMB および NFS アクセスイベントを監視します。

NTFSセキュリティ形式のファイルおよびディレクトリに対する**ONTAP**監査ポリシーの設定

ファイルおよびディレクトリ操作を監査する前に、監査情報を収集するファイルおよびディレクトリに対して監査ポリシーを設定する必要があります。これは、監査設定のセットアップと有効化に加えて行います。NTFS監査ポリシーを設定するには、Windows

の[セキュリティ]タブを使用するか、ONTAP CLIを使用します。

Windowsの**[**セキュリティ**]**タブを使用した**NTFS**監査ポリシーの設定

Windows の [プロパティ] ウィンドウの [Windows セキュリティ *] タブを使用して、ファイルおよびディレクトリの NTFS 監査ポリシーを構成できます。これは、Windowsクライアント上に存在するデータに対して監査ポリシーを設定する場合と同じ方法で、使い慣れたものと同じGUIインターフェイスを使用できます。

開始する前に

監査は、システムアクセス制御リスト（SACL）を適用するデータが格納されているStorage Virtual Machine（SVM）で設定する必要があります。

タスクの内容

NTFS監査ポリシーを設定するには、NTFSセキュリティ記述子に関連付けられているNTFS SACLにエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。これらのタスクはWindows GUIで自動的に処理されます。セキュリティ記述子には、ファイルやフォルダのアクセス権限を適用するためのDiscretionary Access Control List（DACL；随意アクセス制御リスト）、ファイルやフォルダを監査するためのSACL、またはSACLとDACLの両方を含めることができます。

Windowsの[セキュリティ]タブを使用してNTFS監査ポリシーを設定するには、Windowsホストで次の手順を実行します。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
2. [ネットワークドライブの割り当て *] ボックスに入力します。

   a. ドライブ文字を選択します。

   b. [* フォルダ *] ボックスに、監査するデータと共有名を保持して、共有を含む SMB サーバー名を入力します。

      SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

      SMBサーバ名が「smb_server」で、共有の名前が「share1」の場合は、と入力します。
      `\\SMB_SERVER\share1`

   c. [完了] をクリックします。

   選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

3. アクセスの監査を有効にするファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
5. [* セキュリティ *] タブを選択します。
6. 「 * 詳細設定 * 」をクリックします。
7. [監査 *] タブを選択します。
8. 次のうち必要な操作を実行します。

状況	実行する処理

新しいユーザまたはグループの監査を設定する	a. [追加]*をクリックします。 b. [選択するオブジェクト名を入力してください]ボックスに、追加するユーザまたはグループの名前を入力します。 c. [OK]*をクリックします。
ユーザまたはグループから監査を削除する	a. [選択するオブジェクト名を入力してください]ボックスで、削除するユーザまたはグループを選択します。 b. [削除（ Remove ）] をクリックします。 c. [OK]*をクリックします。 d. この手順の残りの部分はスキップしてください。
ユーザまたはグループの監査を変更する	a. [選択するオブジェクト名を入力してください]ボックスで、変更するユーザまたはグループを選択します。 b. [編集（ Edit ）] をクリックします。 c. [OK]*をクリックします。

ユーザーまたはグループの監査を設定したり、既存のユーザーまたはグループの監査を変更したりする場合は、 [< オブジェクト > の監査エントリ] ボックスが開きます。

9. [* 適用先 *] ボックスで、この監査エントリの適用方法を選択します。

   次のいずれかを選択できます。

   - * このフォルダ、サブフォルダ、ファイル *
   - * このフォルダとサブフォルダ *
   - * このフォルダのみ *
   - * このフォルダとファイル *
   - * サブフォルダとファイルのみ *
   - * サブフォルダのみ *
   - * ファイルのみ * 単一ファイルに監査を設定している場合、 * 適用先 * ボックスはアクティブになりません。[* 適用先 * （ Apply to * ）] ボックスの設定は、デフォルトで * このオブジェクトのみ * に設定されています。

   監査ではSVMリソースが使用されるため、セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。

10. [* アクセス *] ボックスで、監査する対象と、成功したイベント、失敗イベント、またはその両方を監査するかどうかを選択します。

    - 成功したイベントを監査するには、成功ボックスを選択します。
    - 障害イベントを監査するには、 [障害] ボックスを選択します。

      セキュリティ要件を満たすために監視する必要がある操作のみを選択してください。これらの監査可

能なイベントの詳細については、Windowsのマニュアルを参照してください。次のイベントを監査できます。

- * フルコントロール *
- * フォルダの移動 / ファイルの実行 *
- * フォルダのリスト / データの読み取り *
- * 属性の読み取り *
- * 拡張属性の読み取り *
- * ファイルの作成 / データの書き込み *
- * フォルダの作成 / データの追加 *
- * 属性の書き込み *
- * 拡張属性の書き込み *
- * サブフォルダとファイルの削除 *
- * 削除 *
- * 読み取り許可 *
- * 権限の変更 *
- * 所有権を取りなさい *

11. 監査設定を元のコンテナの後続のファイルとフォルダに反映させない場合は、 [このコンテナ内のオブジェクトまたはコンテナにのみ監査エントリを適用する *] ボックスを選択します。
12. [適用（ Apply ）] をクリックします。
13. 監査エントリの追加、削除、または編集が完了したら、 **OK** をクリックします。

    [Auditing Entry for <object>] ボックスが閉じます。

14. [監査 *] ボックスで、このフォルダの継承設定を選択します。

    セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。次のいずれかを選択できます。

    - このオブジェクトの親から継承可能な監査エントリを含めるボックスを選択します
    - [このオブジェクトから継承可能な監査エントリをすべての子の既存の継承可能な監査エントリをすべて置換する] ボックスをオンにします
    - 両方のボックスを選択します。
    - どちらのボックスも選択しない。単一ファイルのSACLを設定している場合は、[監査]ボックスに[すべての子孫の既存の継承可能な監査エントリをすべてこのオブジェクトからの継承可能な監査エントリで置き換える]ボックスは表示されません。

15. [OK]*をクリックします。

    [監査]ボックスが閉じます。

ONTAP CLIを使用したNTFS監査ポリシーの設定

ONTAP CLIを使用して、ファイルやフォルダに対して監査ポリシーを設定できます。これにより、Windowsクライアントで SMB共有を使用してデータに接続することなくNTFS監査ポリシーを設定できます。

NTFS監査ポリシーを設定するには、コマンドファミリーを使用し `vserver security file-directory`ます。

CLIで設定できるのはNTFS SACLだけです。NFSv4 SACLの設定は、このONTAPコマンドファミリーではサポートされていません。これらのコマンドを使用してのファイルおよびフォルダに対してNTFS SACLを設定および追加する方法については、"ONTAPコマンド リファレンス"を参照してください。

UNIXセキュリティ形式のファイルおよびディレクトリのONTAP監査の設定

UNIX セキュリティ形式のファイルおよびディレクトリの監査を設定するには、NFSv4.x ACL に監査 ACE を追加します。これにより、セキュリティの目的で特定の NFS ファイルおよびディレクトリのアクセスイベントを監視できます。

タスクの内容

NFSv4.x では、随意 ACE とシステム ACE の両方が同じ ACL に格納されます。個別の DACL と SACL には格納されません。したがって、既存の ACL に監査 ACE を追加する場合は、既存の ACL を上書きして失われることがないように、細心の注意を払う必要があります。既存の ACL に監査 ACE を追加する順序は重要ではありません。

手順

1. または同等のコマンドを使用して、ファイルまたはディレクトリの既存のACLを取得します `nfs4_getfacl`。

   ACLの操作の詳細については、を"ONTAPコマンド リファレンス"参照してください。

2. 目的の監査 ACE を追加します。
3. または同等のコマンドを使用して、更新したACLをファイルまたはディレクトリに適用します `nfs4_setfacl`。

ファイルおよびディレクトリに適用されている監査ポリシーに関する情報を表示する

Windowsの[セキュリティ]タブへのアクセスによるONTAP監査ポリシーの情報の表示

Windowsの[プロパティ]ウィンドウの[セキュリティ]タブを使用して、ファイルとディレクトリに適用されている監査ポリシーに関する情報を表示できます。これは、Windowsサーバ上に存在するデータの場合と同じ方法であるため、ユーザは使い慣れたものと同じGUIインターフェイスを使用できます。

タスクの内容

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なSystem Access Control List（SACL；システムアクセス制御リスト）が設定されているかどうかを確認できます。

NTFSファイルおよびフォルダに適用されているSACLに関する情報を表示するには、Windowsホストで次の手順を実行します。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
2. [* ネットワークドライブの割り当て *] ダイアログボックスに入力します。

   a. ドライブ文字を選択します。

   b. [フォルダ]ボックスに、監査するデータが格納されている共有を含むStorage Virtual Machine（SVM）のIPアドレスまたはSMBサーバ名と、共有の名前を入力します。

      SMBサーバ名が「smb_server」で、共有の名前が「share1」の場合は、と入力します。
      `\\SMB_SERVER\share1`

      SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

   c. [完了] をクリックします。

   選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

3. 監査情報を表示するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
5. [* セキュリティ *] タブを選択します。
6. 「 * 詳細設定 * 」をクリックします。
7. [監査 *] タブを選択します。
8. [* Continue （続行）] をクリックします

   [監査]ボックスが開きます。[監査エントリ *] ボックスには、 SACL が適用されているユーザーとグループの概要が表示されます。

9. [* 監査エントリ *] ボックスで、 SACL エントリを表示するユーザーまたはグループを選択します。
10. [編集（ Edit ）] をクリックします。

    [< オブジェクト > の監査エントリ] ボックスが開きます。

11. [* アクセス * （ * Access * ）] ボックスで、選択したオブジェクトに適用されている現在の SACL を表示します。
12. [* キャンセル *] をクリックして、 [* 監査エントリ for < オブジェクト >*] ボックスを閉じます。
13. [* キャンセル *] をクリックして、 [* 監査 *] ボックスを閉じます。

ONTAP FlexVolのNTFS監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されている権限、システムアクセス制御リストに関する情報など、FlexVolのNTFS監査ポリシーに関する情報を表示できます。この情報を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

タスクの内容

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なSystem Access Control List（SACL；システムアクセス制御リスト）が設定されているかどうかを確認できます。

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、NTFSのシステムアクセス制御リスト（SACL）のみが監査ポリシーに使用されます。
- NTFS対応のセキュリティが有効なmixedセキュリティ形式のボリューム内のファイルやフォルダには、NTFS監査ポリシーを適用できます。

  mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixedセキュリティ形式のボリュームの最上位には、UNIX対応またはNTFS対応のセキュリティを設定でき、NTFS SACLが格納されている場合と格納されていない場合があります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、mixedセキュリティ形式のボリュームまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルおよびフォルダのNFSv4 SACLとストレージレベルのアクセス保護NTFS SACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。
- NTFS対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、UNIX関連の出力フィールドに表示専用のUNIXファイル権限情報が表示されます。

  ファイルアクセス権の決定時に、NTFSセキュリティ形式のファイルおよびフォルダでは、NTFSファイル権限とWindowsユーザおよびグループのみが使用されます。

- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルやフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。

ステップ

1. ファイルおよびディレクトリ監査ポリシーの設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`

詳細なリスト	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/corp`。パスにはNTFS対応のセキュリティが設定されています。NTFSセキュリティ記述子には、SUCCESSおよびSUCCESS / FAIL SACLエントリの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/datavol1`。このパスには、通常のファイルとフォルダのSACLとストレージレベルのアクセス保護のSACLの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ワイルドカード文字を使用した**ONTAP**ファイルセキュリティと監査ポリシーに関する情報の表示

ワイルドカード文字（ * ）を使用すると、特定のパスまたはルートボリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関す

る情報を表示できます。

ワイルドカード文字（ * ）は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。

という名前の特定のファイルまたはディレクトリの情報を表示する場合は、パス全体を二重引用符（ "" ）で囲む必要があります。

例

次のコマンドでワイルドカード文字を使用すると、SVM vs1のパスの下にあるすべてのファイルとディレクトリに関する情報が表示され `/1/` ます。

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

次のコマンドは、SVM vs1のパスの下にある「*」という名前のファイルの情報を表示します `/vol1/a`。パスは二重引用符（ "" ）で囲まれます。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

監査できる**CLI**変更イベント

監査可能な**ONTAP CLI**変更イベントについて説明します。

ONTAPでは、SMB共有イベント、監査ポリシーイベント、ローカルセキュリティグループイベント、ローカルユーザグループイベント、認証ポリシーイベントなど、特定のCLI変更イベントを監査できます。どの変更イベントを監査できるかを理解しておくと、イベントログの結果を解釈するときに役立ちます。

Storage Virtual Machine（SVM）によるCLI変更イベントの監査の管理作業として、手動での監査ログのローテーション、監査の有効化と無効化、監査変更イベントに関する情報の表示、監査変更イベントの変更、監査変更イベントの削除が可能です。

管理者がSMB共有、ローカルユーザグループ、ローカルセキュリティグループ、認証ポリシー、および監査ポリシーの各イベントに関連する設定を変更するコマンドを実行すると、レコードが生成され、対応するイベントが監査されます。

監査カテゴリ	イベント	イベント IDs	実行するコマンド
Mhostの監査	ポリシー変更	[4719] 監査設定が変更されました	`vserver audit disable

enable	modify`	ファイル共有	[5142] ネットワーク共有が追加されました
`vserver cifs share create`	[5143] ネットワーク共有の変更	`vserver cifs share modify` `vserver cifs share create`	modify
delete` `vserver cifs share add	remove`	[5144] ネットワーク共有が削除されました	`vserver cifs share delete`
監査	ユーザアカウント	[4720] ローカルユーザの作成	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] ローカルユーザの有効化	`vserver cifs users-and-groups local-user create	modify`	[4724] ローカルユーザのパスワードのリセット
`vserver cifs users-and-groups local-user set-password`	[4725] ローカルユーザの無効化	`vserver cifs users-and-groups local-user create	modify`
[4726] ローカルユーザの削除	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] ローカルユーザの変更	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] ローカルユーザの名前変更	`vserver cifs users-and-groups local-user rename`	セキュリティグループ	[4731] ローカルセキュリティグループが作成されました
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] ローカルセキュリティグループが削除されました	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] ローカルセキュリティグループの変更

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] ローカルグループへのユーザの追加	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] ローカルグループからユーザが削除されました	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	認証ポリシー変更	[4704] ユーザ権限の割り当て
`vserver cifs users-and-groups privilege add-privilege`	[4705] ユーザ権限が削除されました	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

関連情報

- "SVM"

ファイル共有**ONTAP**イベントを管理します。

Storage Virtual Machine（SVM）に対してファイル共有イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。ファイル共有イベントが生成されるのは、の関連コマンドを使用してSMBネットワーク共有が変更された場合 `vserver cifs share`です。

ファイル共有イベントは、SVMに対してSMBネットワーク共有が追加、変更、または削除されたときに生成されます。イベントIDは5142、5143、および5144です。SMBネットワーク共有の設定は、コマンドを使用して変更し `cifs share access control create|modify|delete`ます。

次の例では、「audit_dest」という名前の共有オブジェクトが作成され、IDが5143のファイル共有イベントが生成されています。

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

監査ポリシー変更**ONTAP**イベントの管理

Storage Virtual Machine（SVM）に対して監査ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。監査ポリシー変更イベントは、の関連コマンドを使用して監査ポリシーが変更された場合に生成され `vserver audit`ます。

監査ポリシー変更イベント（イベントID 4719）は、監査ポリシーが無効、有効、または変更されたときに生成され、ユーザが監査を無効にしようとしたタイミングを特定して追跡できます。このイベントはデフォルトで設定されており、無効にするには diagnostic 権限が必要です。

次の例では、監査が無効になっているときに、ID 4719の監査ポリシー変更イベントが生成されています。

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

ユーザアカウント**ONTAP**イベントを管理します。

Storage Virtual Machine（SVM）に対してユーザアカウントイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

イベントID 4720、4722、4724、4725、4726のユーザアカウントイベント 4738および4781は、ローカルSMBまたはNFSユーザがシステムから作成または削除されたとき、ローカルユーザアカウントが有効化、無効化または変更されたとき、ローカルSMBユーザパスワードがリセットまたは変更されたときに生成されます。ユーザアカウントイベントは、コマンドおよび `vserver services name-service *<unix user>*`コマンドを使用してユーザアカウントが変更されたときに生成され `vserver cifs users-and-groups *<local user>*`ます。

次の例では、ローカルSMBユーザが作成され、ID 4720のユーザアカウントイベントが生成されています。

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

次の例では、上記の例で作成されたローカルSMBユーザの名前が変更され、ID 4781のユーザアカウントイベントが生成されています。

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

セキュリティグループの**ONTAP**イベントを管理します。

Storage Virtual Machine（SVM）に対してセキュリティグループイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

セキュリティグループイベントは、システムのローカル SMB グループまたは NFS グループが作成または削除されたとき、それらのグループのローカルユーザが追加または削除されたときに生成されます。イベント ID は 4731 、 4732 、 4733 、 4734 、および 4735 です。セキュリティグループイベントは、コマンドおよび `vserver services name-service <*unix-group*>`コマンドを使用してユーザアカウントが変更されたときに生成され `vserver cifs users-and-groups <*local-group*>`ます。

次の例では、ローカルUNIXセキュリティグループが作成され、ID 4731のセキュリティグループイベントが生成されています。

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

認証ポリシー変更**ONTAP**イベントを管理します。

Storage Virtual Machine（SVM）に対して認証ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

認証ポリシー変更イベントは、SMBユーザおよびSMBグループに対して認証権限が付与または取り消されるたびに生成されます。イベントIDは4704および4705です。認証ポリシー変更イベントが生成されるのは、の関連コマンドを使用して認証権限が割り当てられた場合または取り消された場合 `vserver cifs users-and-groups privilege`です。

次の例では、SMBユーザグループの認証権限が割り当てられている場合に、ID 4704の認証ポリシーイベントが生成されています。

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

監査設定を管理します。

特定のONTAP SVMイベントログを表示するための監査イベントログの手動ローテーション

監査イベントログは、表示する前に、ユーザが読解可能な形式に変換する必要があります。ONTAPによるログの自動ローテーション前に特定のStorage Virtual Machine（SVM）のイベントログを表示する場合は、そのSVMで監査イベントログの手動ローテーションを実行できます。

ステップ

1. コマンドを使用して、監査イベントログのローテーションを行い `vserver audit rotate-log`ます。

   ```
   vserver audit rotate-log -vserver vs1
   ```

   監査イベントログは、監査の設定で指定されている形式でSVMの監査イベントログディレクトリに保存され(XML EVTX、該当するアプリケーションを使用して表示できます。

ONTAP SVMでの監査の有効化または無効化

Storage Virtual Machine（SVM）で監査を有効または無効にすることができます。必要に応じて、監査を無効にすることで、ファイルおよびディレクトリの監査を一時的に停止できます。監査はいつでも有効にできます（監査の設定が存在する場合）。

開始する前に

SVMで監査を有効にするには、SVMの監査の設定がすでに存在している必要があります。

"監査の設定を作成する"

タスクの内容

監査を無効にしても、監査の設定は削除されません。

手順

1. 適切なコマンドを実行します。

監査の設定	入力するコマンド
有効	`vserver audit enable -vserver vserver_name`
無効にする	`vserver audit disable -vserver vserver_name`

2. 監査が目的の状態になっていることを確認します。

   ```
   vserver audit show -vserver vserver_name
   ```

例

次の例では、SVM vs1で監査を有効にします。

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

次の例では、SVM vs1で監査を無効にします。

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

ONTAP監査の設定に関する情報を表示する

監査の設定に関する情報を表示できます。この情報は、各 SVM で適切な設定が使用されているかどうか確認するのに役立ちます。また、表示される情報から、監査の設定が有効になっているかどうかを確認することもできます。

タスクの内容

すべての SVM の監査の設定に関する詳細情報を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- 監査の設定が適用される SVM の名前
- 監査の状態（ `true`または） `false`

  監査の状態がの場合、 `true`監査は有効になっています。監査の状態がの場合、 `false`監査は無効になります。

- 監査するイベントのカテゴリ
- 監査ログの形式
- 統合および変換された監査ログが監査サブシステムによって格納されるターゲットディレクトリ

ステップ

1. コマンドを使用して、監査の設定に関する情報を表示します `vserver audit show`。

   の詳細については `vserver audit show`、を"ONTAPコマンド リファレンス"参照してください。

例

次の例は、すべての SVM の監査の設定の概要を表示したものです。

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

次の例は、すべての SVM の監査の設定情報をリスト形式で表示したものです。

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                         Log Format: evtx
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
```

監査の設定を変更するための**ONTAP**コマンド

監査設定を変更する場合は、ログのデスティネーションパスと形式の変更、監査するイベントのカテゴリの変更、ログファイルの自動保存方法など、現在の設定をいつでも変更できます。また、保存するログファイルの最大数の指定も可能です。

状況	使用するコマンド
ログのデスティネーションパスを変更します。	`vserver audit modify`パラメータを指定した場合 `-destination`
監査するイベントのカテゴリを変更する	`vserver audit modify`パラメータを指定した場合 `-events` 集約型アクセスポリシーのステージングイベントを監査するには、Dynamic Access Control（DAC；ダイナミックアクセス制御）SMBサーバオプションがStorage Virtual Machine（SVM）で有効になっている必要があります。

ログ形式の変更	`vserver audit modify`パラメータを指定した場合 `-format`
内部的な一時ログファイルサイズに基づく自動保存の有効化	`vserver audit modify`パラメータを指定した場合 `-rotate-size`
時間間隔に基づいた自動保存の有効化	`vserver audit modify`を使用して、 `-rotate-schedule-dayofweek、-rotate-schedule-day、、、-rotate-schedule-hour`および `-rotate-schedule-minute`パラメータを指定します。 `-rotate-schedule-month`
保存されるログファイルの最大数の指定	`vserver audit modify`パラメータを指定した場合 `-rotate-limit`

ONTAP SVMの監査の設定を削除する

Storage Virtual Machine（SVM）でのファイルおよびディレクトリイベントの監査が必要なくなり、SVMで監査の設定を維持する必要がなくなった場合は、監査の設定を削除できます。

手順

1. 監査の設定を無効にします。

```
vserver audit disable -vserver vserver_name

vserver audit disable -vserver vs1
```

2. 監査の設定を削除します。

```
vserver audit delete -vserver vserver_name

vserver audit delete -vserver vs1
```

監査対象の**ONTAP**クラスタをリバートする場合の影響を理解する

クラスタのリバートを予定している場合は、監査が有効になっているStorage Virtual Machine（SVM）がクラスタ内にあるときにONTAPが従うリバートプロセスに注意する必要があります。リバートを行う前に特定の操作を実行する必要があります。

SMBのログオンおよびログオフイベントと集約型アクセスポリシーのステージングイベントの監査をサポートしていないバージョンの**ONTAP**へのリバート

SMBのログオンおよびログオフイベントと集約型アクセスポリシーのステージングイベントのサポートは、clustered Data ONTAP 8で開始されました。3.これらのイベントタイプをサポートしていないバージョンのONTAPへのリバートを予定していて、これらのイベントタイプを監視する監査が設定されている場合は、リバート前に監査が有効になっているSVMの監査の設定を変更する必要があります。設定は、ファイル操作

イベントのみが監査されるように変更する必要があります。

ONTAPの監査とステージングボリュームのスペースに関する問題のトラブルシューティング

ステージングボリュームまたは監査イベントログを含むボリュームでスペースが不足していると、問題が発生する可能性があります。十分なスペースがないと新しい監査レコードを作成できないため、クライアントからデータにアクセスできず、アクセス要求が失敗します。ボリュームのスペースに関するこれらの問題について、トラブルシューティングを行って問題を解決する方法を確認しておく必要があります。

イベントログボリュームに関連するスペースの問題をトラブルシューティングする

イベントログファイルを含むボリュームのスペースが不足すると、監査でログレコードをログファイルに変換できません。その結果、クライアントアクセスが失敗します。イベントログボリュームに関連するスペースの問題のトラブルシューティング方法を把握しておく必要があります。

- Storage Virtual Machine（SVM）管理者およびクラスタ管理者は、ボリュームとアグリゲートの使用量と設定に関する情報を表示して、ボリュームでスペースが不足していないかを確認できます。
- イベント ログを含むボリュームでスペースが不足している場合、SVM管理者およびクラスタ管理者は、いくつかのイベント ログ ファイルを削除するかボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。

> イベント ログ ボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを大きくする前に、アグリゲートのサイズを大きくする必要があります。アグリゲートのサイズを大きくすることができるのは、クラスタ管理者だけです。

- 監査設定を変更して、イベント ログ ファイルのデスティネーション パスを別のボリューム上のディレクトリに変更できます。

> 次の場合はデータへのアクセスが拒否されます。
>
> - デスティネーション ディレクトリが削除されている
> - デスティネーション ディレクトリをホストするボリュームのファイル リミットが最大レベルに達している

詳細については以下を参照してください。

- "ボリュームに関する情報の表示方法とボリュームサイズの拡張方法"です。
- "アグリゲートに関する情報の表示方法とアグリゲートの管理方法"です。

ステージングボリュームに関するスペースの問題のトラブルシューティング

Storage Virtual Machine（SVM）のステージングファイルを含むボリュームのいずれかでスペースが不足すると、監査でログレコードをステージングファイルに書き込むことができなくなります。その結果、クライアントアクセスが失敗します。この問題のトラブルシューティングを行うには、ボリュームの使用量に関する情報を表示して、SVMで使用されているステージングボリュームのいずれかがいっぱいになっていないかを確認する必要があります。

統合イベントログファイルを含むボリュームに十分なスペースがあるにもかかわらず、スペース不足が原因でクライアントアクセスに失敗する場合は、ステージングボリュームのスペースが不足している可能性があります。SVM管理者は、ユーザに問い合わせて、SVMのステージングファイルを含むステージングボリュームでスペースが不足していないかどうかを確認する必要があります。ステージングボリュームのスペース不足が原因で監査イベントを生成できない場合は、監査サブシステムによってEMSイベントが生成されます。次のメッセージが表示されます。 `No space left on device`ステージングボリュームに関する情報を表示できるのは、管理者だけです。SVM管理者はこの操作を実行できません。

すべてのステージングボリューム名はで始まり `MDV_aud_`、そのあとにステージングボリュームを含むアグリゲートのUUIDが続きます。次の例は、管理SVM上にある4つのシステムボリュームを示しています。これらのボリュームは、クラスタ内でデータSVMのファイルサービスの監査の設定が作成されたときに自動的に作成されたものです。

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

ステージングボリュームでスペースが不足している場合は、ボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。

> ステージングボリュームを含むアグリゲートがいっぱいの場合は、ボリュームのサイズを拡張する前に、アグリゲートのサイズを拡張する必要があります。アグリゲートのサイズを拡張できるのは、クラスタ管理者だけです。SVM管理者はこの操作を実行できません。

2GB未満（ONTAP 9.14.1以前）または5GB（ONTAP 9.151以降）の使用可能なスペースがあるアグリゲートが1つ以上あると、SVMの監査の作成が失敗します。SVMの監査の作成に失敗すると、作成されていたステージングボリュームが削除されます。

SVMでのファイルの監視と管理にFPolicyを使用する

FPolicyについて

2つの部分から成るONTAP FPolicyソリューションについて学ぶ

FPolicyは、パートナーソリューションを通じてStorage Virtual Machine（SVM）上のファイルアクセスイベントの監視と管理に使用されるファイルアクセス通知フレームワークです。パートナーソリューションは、データガバナンスとコンプライアンス、ランサムウェア対策、データモビリティなど、さまざまなユースケースへの対応を支援します。

パートナーソリューションには、NetAppがサポートするサードパーティソリューションと、NetApp製品のワークロードセキュリティとCloud Data Senseの両方が含まれます。

FPolicyソリューションには2つの要素があります。ONTAP FPolicyフレームワークは、クラスタでのアクティビティを管理し、パートナーアプリケーション（外部FPolicyサーバ）に通知を送信します。外部FPolicyサーバは、お客様のユースケースに対応するために、ONTAP FPolicyから送信された通知を処理します。

ONTAPフレームワークでは、FPolicyの設定の作成と管理、ファイルイベントの監視、および外部FPolicyサーバへの通知の送信を行います。ONTAP FPolicy は、外部 FPolicy サーバと Storage Virtual Machine （ SVM ）ノードの間の通信を可能にするインフラを提供します。

FPolicyフレームワークは、外部FPolicyサーバに接続し、クライアントアクセスの結果として特定のファイルシステムイベントが発生した場合にFPolicyサーバに通知を送信します。外部FPolicyサーバは、これらの通知を処理し、ノードに応答を送信します。通知処理の結果として実行される処理は、アプリケーション、およびノードと外部サーバの間の通信が非同期であるか同期であるかによって異なります。

ONTAP FPolicyの同期および非同期通知

FPolicyは、FPolicyインターフェイスを介して外部FPolicyサーバに通知を送信します。通知は同期モードまたは非同期モードで送信されます。通知モードによって、FPolicyサーバに通知を送信したあとのONTAPの動作が決まります。

- * 非同期通知 *

  非同期通知では、ノードはFPolicyサーバからの応答を待たずに済むため、システムの全体的なスループットが向上します。このタイプの通知は、通知を評価した結果としてFPolicyサーバで処理する必要がないアプリケーションに適しています。たとえば、Storage Virtual Machine（SVM）管理者がファイルアクセスのアクティビティを監視および監査する場合などに使用します。

  FPolicyサーバが非同期モードで動作している場合にネットワークが停止すると、停止中に生成されたFPolicy通知がストレージノードに格納されます。FPolicyサーバがオンラインに戻ると、格納されている通知に関するアラートが通知され、ストレージノードから通知を取得できます。停止中に通知を保存できる期間は、最大10分まで設定できます。

  14.1以降では、ONTAP 9の必須ではない非同期ポリシーのファイルアクセスイベントをキャプチャする永続的ストアを設定できます。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期（必須または必須でない）および非同期の必須構成はサポートされていません。

- * 同期通知 *

同期モードで実行するように設定した場合、クライアント処理を続行するには、すべての通知をFPolicyサーバが確認応答する必要があります。このタイプの通知は、通知評価の結果に基づいてアクションが必要な場合に使用されます。たとえば、SVM管理者が要求を許可するか拒否するかを外部FPolicyサーバで指定された条件に基づいて判断する場合などに使用されます。

同期アプリケーションおよび非同期アプリケーション

FPolicyアプリケーションには、非同期と同期の両方でさまざまな用途があります。

非同期アプリケーションとは、ファイルやディレクトリへのアクセスやStorage Virtual Machine（SVM）上のデータが外部FPolicyサーバによって変更されないアプリケーションです。例：

- ファイルアクセスと監査ログ
- ストレージリソース管理

同期アプリケーションとは、データアクセスが変更されたり、外部FPolicyサーバによってデータが変更されたりするアプリケーションです。例：

- クォータの管理
- ファイルアクセスブロッキング
- ファイルのアーカイブと階層型ストレージ管理
- 暗号化サービスと復号化サービス
- 圧縮サービスと展開サービス

ONTAP FPolicy 永続ストア

永続的ストアは、クライアントI/O処理をFPolicy通知処理から分離して、クライアントのレイテンシを低減するのに役立ちます。ONTAP 9.14.1以降では、FPolicyの永続的ストアを作成し、SVM内の非同期で必須でないポリシーのファイル アクセス イベントをキャプチャできます。同期（必須かどうかは問わない）および非同期で必須の設定はサポートされていません。

この機能は、FPolicy外部モードでのみ使用できます。使用するパートナー アプリケーションが、この機能をサポートしている必要があります。パートナーと協力して、このFPolicy設定がサポートされていることを確認するようにしてください。

ONTAP 9.15.1以降では、FPolicyの永続的ストア設定が簡易化されています。 `persistent-store create`コマンドは、SVMのボリューム作成を自動化し、永続的ストアのベストプラクティスに従ってボリュームを設定します。

永続的ストアのベストプラクティスの詳細については、を参照してください"FPolicyの設定に関する要件、考慮事項、およびベストプラクティス"。

永続ストアの追加については、を参照してください"永続ストアの作成"。

ONTAP FPolicy設定タイプ

FPolicyの基本設定には2つのタイプがあります。一方の設定では、外部FPolicyサーバを

使用して通知の処理と対応を行います。もう一方の設定では外部FPolicyサーバを使用しません。代わりに、ONTAP内部のネイティブFPolicyサーバを使用して、拡張子に基づく単純なファイルブロッキングを行います。

- * 外部 FPolicy サーバ構成 *

  FPolicyサーバに通知が送信され、FPolicyサーバが要求をスクリーニングし、要求されたファイル操作をノードで許可するかどうかを決定するルールを適用します。同期ポリシーの場合、FPolicyサーバは要求されたファイル操作を許可またはブロックする応答をノードに送信します。

- * ネイティブ FPolicy サーバ構成 *

  通知は内部的にスクリーニングされます。要求は、FPolicyスコープで設定されているファイル拡張子に基づいて許可または拒否されます。

  *注：拒否されたファイル拡張子要求はログに記録されません。

ネイテイフ**FPolicy**セツテイヲサクセイスルシヨウコウ

ネイティブFPolicyの設定では、ONTAP内部のFPolicyエンジンを使用して、ファイルの拡張子に基づいてファイル操作を監視およびブロックします。このソリューションでは、外部FPolicyサーバ（FPolicyサーバ）は必要ありません。このシンプルなソリューションが必要な場合は、ネイティブファイルブロッキング構成を使用することをお勧めします。

ネイティブファイルブロッキングを使用すると、設定された処理およびフィルタリングイベントに一致するすべてのファイル操作を監視し、特定の拡張子を持つファイルへのアクセスを拒否できます。これがデフォルトの設定です。

この設定では、ファイルの拡張子のみに基づいてファイルへのアクセスをブロックすることができます。たとえば、拡張子を含むファイルをブロックするには `mp3`、拡張子がのファイルをターゲットとする特定の処理について通知を送信するようにポリシーを設定し `mp3`ます。このポリシーは、通知を生成する操作のファイル要求を拒否するように設定されて `mp3`います。

ネイティブFPolicy設定には次の事項が適用されます。

- FPolicyサーバベースのファイルスクリーニングでサポートされているフィルタとプロトコルのセットが、ネイティブファイルブロッキングでもサポートされます。
- ネイティブファイルブロッキングとFPolicyサーバベースファイルスクリーニングアプリケーションは同時に設定できます。

  そのためには、Storage Virtual Machine（SVM）に2つのFPolicyポリシーを設定します。1つはネイティブファイルブロッキング用に設定されたポリシー、もう1つはFPolicyサーバベースのファイルスクリーニング用に設定されたポリシーです。

- ネイティブファイルブロッキング機能は、ファイルの内容ではなく、拡張子に基づいてファイルをスクリーニングするだけです。
- シンボリックリンクの場合、ネイティブファイルブロッキングはルートファイルのファイル拡張子を使用します。

詳細については、をご覧ください "FPolicy：ネイティブファイルブロッキング"。

外部**FPolicy**サーバを使用する設定を作成する状況

通知の処理と管理に外部FPolicyサーバを使用するFPolicy設定は、ファイル拡張子に基づく単純なファイルブロッキング以上のことが必要なユースケースに、堅牢なソリューションを提供します。

ファイルアクセスイベントの監視と記録、クォータサービスの提供、単純なファイル拡張子以外の条件に基づくファイルブロッキングの実行、階層型ストレージ管理アプリケーションを使用したデータ移行サービスの提供、Storage Virtual Machine（SVM）のデータのサブセットのみを監視するきめ細かなポリシーセットの提供などを行う場合は、外部FPolicyサーバを使用する設定を作成する必要があります。

ONTAP FPolicy実装におけるクラスタコンポーネントの役割

FPolicyの実装では、クラスタ、それに含まれるStorage Virtual Machine（SVM）、およびデータLIFのすべてが役割を果たします。

- * クラスタ *

  クラスタにはFPolicyの管理フレームワークが含まれており、クラスタ内のすべてのFPolicyの設定に関する情報の保守と管理を行っています。

- * SVM *

  FPolicyの設定はSVMレベルで定義されます。設定の範囲はSVMで、SVMリソースに対してのみ機能します。あるSVMの設定で、別のSVMにあるデータに対するファイルアクセス要求を監視して通知を送信することはできません。

  FPolicyの設定は管理SVMで定義できます。管理SVMで定義した設定は、すべてのSVMで表示および使用できます。

- * データ LIF *

  FPolicyサーバへの接続は、FPolicyの設定が格納されたSVMに属するデータLIFを介して行われます。これらの接続に使用されるデータLIFは、通常のクライアントアクセスに使用されるデータLIFと同じ方法でフェイルオーバーできます。

ONTAP FPolicyと外部**FPolicy**サーバの連携

Storage Virtual Machine（SVM）でFPolicyを設定して有効にすると、SVMに含まれているすべてのノードでFPolicyが実行されます。FPolicyは、外部FPolicyサーバ（FPolicyサーバ）との接続の確立と維持、通知の処理、およびFPolicyサーバとの間の通知メッセージの管理を行います。

また、接続管理の一環として、 FPolicy は次の役割を果たします。

- ファイル通知が正しいLIFを経由してFPolicyサーバに送信されるようにします。
- ポリシーに複数のFPolicyサーバが関連付けられている場合に、FPolicyサーバへの通知の送信時にロードバランシングが実行されるようにします。
- FPolicyサーバへの接続が切断された場合、接続の再確立が試行されます。
- 認証されたセッションを介してFPolicyサーバに通知を送信します。

- パススルーリードが有効になっている場合にクライアント要求を処理するためにFPolicyサーバによって確立されたパススルーリードデータ接続を管理します。

FPolicyツウシンニセイギョチャネルヲシヨウスルホウホウ

FPolicyは、Storage Virtual Machine（SVM）に含まれている各ノードのデータLIFから外部FPolicyサーバへの制御チャネル接続を開始します。FPolicyは制御チャネルを使用してファイル通知を送信するため、FPolicyサーバでは、SVMのトポロジに基づいて複数の制御チャネル接続が認識される場合があります。

ケンゲンツキツウシンテノデータアクセスチャネルノシヨウホウホウ

同期ユースケースでは、FPolicyサーバは権限付きデータアクセスパスを介してStorage Virtual Machine（SVM）上のデータにアクセスします。権限付きパスを介してアクセスすると、ファイルシステム全体がFPolicyサーバに公開されます。データファイルにアクセスして、情報の収集、ファイルのスキャン、ファイルの読み取り、ファイルへの書き込みを行うことができます。

外部FPolicyサーバが権限付きデータチャネルを介してSVMのルートからファイルシステム全体にアクセスできるため、権限付きデータチャネル接続はセキュアである必要があります。

権限付きデータアクセスチャネルでのFPolicy接続クレデンシャルの使用方法

FPolicyサーバは、FPolicy設定で保存されている特定のWindowsユーザクレデンシャルを使用して、クラスタノードへの権限付きデータアクセス接続を確立します。権限付きデータアクセスチャネル接続の確立用にサポートされているプロトコルはSMBだけです。

FPolicyサーバで権限付きデータアクセスが必要な場合は、次の条件を満たしている必要があります。

- クラスタでSMBライセンスが有効になっている必要があります。
- FPolicyサーバは、FPolicyの設定で設定されたクレデンシャルで実行されている必要があります。

FPolicyでは、データチャネル接続を確立する際に、指定したWindowsユーザ名のクレデンシャルを使用します。データアクセスは、管理共有ONTAP _ ADMIN$を介して行われます。

ケンゲンツキデータアクセスヨウノスーパーユーザクレデンシャルノフヨトハ

ONTAPでは、FPolicy設定で設定されたIPアドレスとユーザクレデンシャルを組み合わせて、FPolicyサーバにスーパーユーザクレデンシャルを付与します。

スーパーユーザのステータスは、FPolicyサーバがデータにアクセスするときに次のPrivilegesに付与されます。

- 権限チェックの省略

  ユーザは、ファイルおよびディレクトリへのアクセスのチェックを回避します。

- 特殊ロックPrivileges

  ONTAPは、ロックが設定されているかどうかに関係なく、すべてのファイルに対して読み取り、書き込み、変更アクセスを許可します。FPolicyサーバがファイルに対してバイト範囲ロックを取得すると、そのファイルに対する既存のロックがただちに削除されます。

- FPolicyチェックのバイパス

アクセスではFPolicy通知は生成されません。

FPolicyによるポリシーの処理の管理方法

Storage Virtual Machine（SVM）には、優先度が異なる複数のFPolicyポリシーが割り当てられる場合があります。SVMで適切なFPolicyの設定を作成するには、FPolicyによるポリシーの処理の管理方法を理解しておくことが重要です。

各ファイルアクセス要求が最初に評価され、このイベントを監視しているポリシーが特定されます。監視対象イベントの場合は、関連するポリシーとともに監視対象イベントに関する情報が評価対象のFPolicyに渡されます。各ポリシーは、割り当てられた優先度の順に評価されます。

ポリシーを設定する際には、次の推奨事項を考慮する必要があります。

- ポリシーが常に他のポリシーよりも先に評価されるようにするには、そのポリシーの優先度を高く設定します。
- 監視対象イベントで要求されたファイルアクセス処理が成功することが、別のポリシーに照らして評価されるファイル要求の前提条件である場合は、最初のファイル処理の成功または失敗を制御するポリシーの優先度を高くします。

  たとえば、FPolicyのファイルのアーカイブおよびリストア機能を1つのポリシーで管理し、オンラインファイルでのファイルアクセス操作を2つ目のポリシーで管理している場合は、ファイルのリストアを管理するポリシーの優先度を高くしてから、2つ目のポリシーの管理操作を許可する必要があります。

- ファイルアクセス処理に適用される可能性のあるすべてのポリシーを評価する場合は、同期ポリシーの優先度を低くします。

既存のポリシーの優先度を変更するには、ポリシーのシーケンス番号を変更します。ただし、変更した優先順位に基づいてFPolicyでポリシーが評価されるようにするには、変更したシーケンス番号のポリシーを無効にしてから再度有効にする必要があります。

ノードと外部の **ONTAP FPolicy** サーバ間の通信プロセス

FPolicyの設定を適切に計画するには、ノードと外部FPolicyサーバの間の通信プロセスについて理解しておく必要があります。

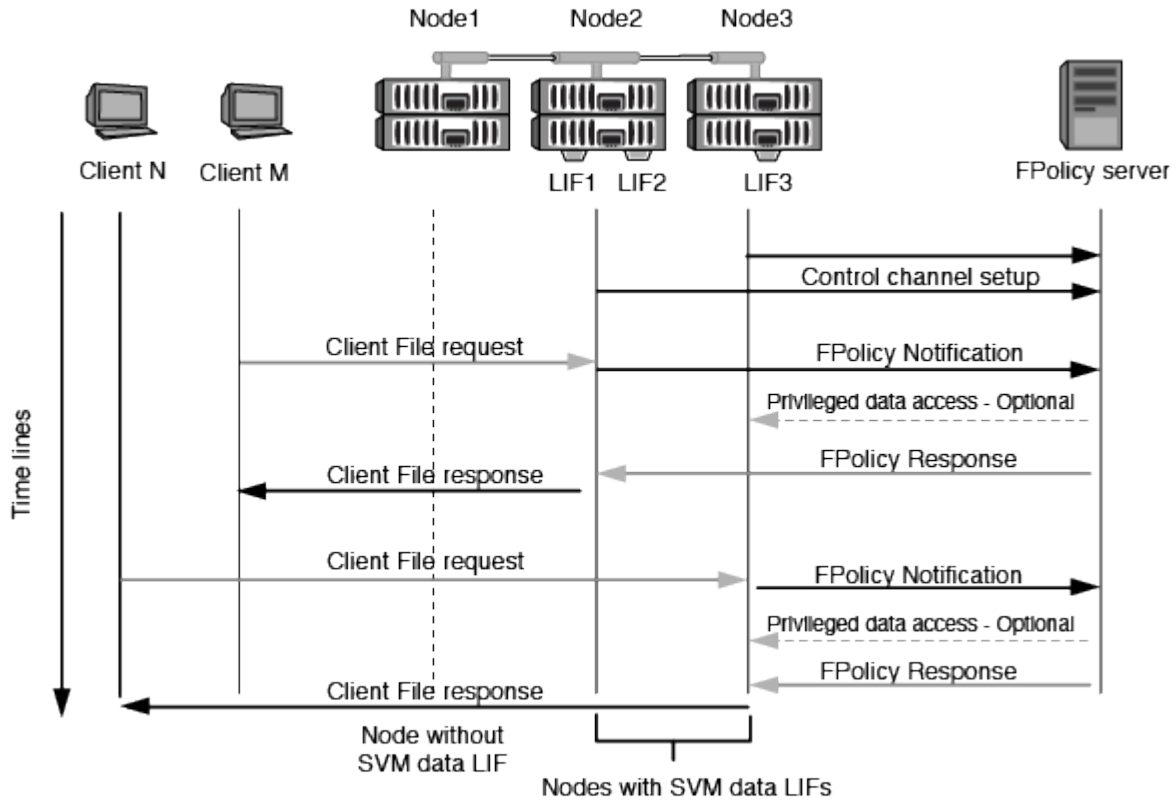
Storage Virtual Machine（SVM）に属しているすべてのノードは、TCP/IPを使用して外部FPolicyサーバへの接続を開始します。FPolicyサーバへの接続のセットアップには、ノードのデータLIFを使用します。そのため、接続のセットアップは、ノードでSVMのデータLIFが稼働している場合にのみ実行できます。

ポリシーが有効になっている場合、各ノードの各FPolicyプロセスでは、FPolicyサーバとの接続の確立が試行されます。ポリシー設定で指定されたFPolicy外部エンジンのIPアドレスとポートが使用されます。

この接続により、SVMに属する各ノードからFPolicyサーバへのデータLIFを介した制御チャネルが確立されます。さらに、データLIFのアドレスが同じノードでIPv4とIPv6の両方で設定されている場合、FPolicyはIPv4とIPv6の両方の接続の確立を試みます。したがって、SVMが複数のノードに展開されている場合、またはIPv4アドレスとIPv6アドレスの両方が設定されている場合は、SVMでFPolicyポリシーを有効にしたあとに、クラスタからの複数の制御チャネルのセットアップ要求に対応する必要があります。

たとえば、クラスタに3つのノード（ノード1、ノード2、およびノード3）があり、SVMのデータLIFがノード2とノード3だけで設定されている場合、データボリュームの配置に関係なく、制御チャネルはノード2とノード3からのみ開始されます。ノード2にSVMに属するデータLIFが2つ（LIF1とLIF2）あり、最初にLIF1から

接続を行うとします。FPolicyは、LIF1で障害が発生した場合、LIF2からの制御チャネルの確立を試みます。



LIFの移行時またはフェイルオーバー時の**FPolicy**による外部通信の管理方法

データLIFは、同じノードのデータポート、またはリモートノードのデータポートに移行できます。

データLIFがフェイルオーバーまたは移行されると、FPolicyサーバへの新しい制御チャネル接続が確立されます。その後、FPolicyはSMBクライアントおよびNFSクライアントのタイムアウトした要求を再試行でき、新しい通知が外部FPolicyサーバに送信されます。ノードは、SMBおよびNFSの元のタイムアウトした要求に対するFPolicyサーバの応答を拒否します。

ノードのフェイルオーバー時の**FPolicy**による外部通信の管理方法

FPolicy通信に使用されるデータポートをホストするクラスタノードで障害が発生すると、ONTAPはFPolicyサーバとノードの間の接続を切断します。

クラスタフェイルオーバーがFPolicyサーバに及ぼす影響は、FPolicy通信に使用されるデータポートを別のアクティブノードに移行するようにフェイルオーバーポリシーを設定することで軽減できます。移行が完了すると、新しいデータポートを使用して新しい接続が確立されます。

データポートを移行するようにフェイルオーバーポリシーが設定されていない場合、FPolicyサーバは障害が発生したノードが稼働するまで待機する必要があります。ノードが稼働すると、そのノードから新しいSession IDを使用して新しい接続が開始されます。

FPolicyサーバは、切断された接続をキープアライブプロトコルメッセージで検出します。Session IDをパージするタイムアウトは、FPolicyの設定時に決定されます。デフォルトのキープアライブタイムアウトは2分です。

SVMネームスペース全体にわたるONTAP FPolicyサービスについて学ぶ

ONTAP は、統合 Storage Virtual Machine （ SVM ）ネームスペースを提供します。ジャンクションによってクラスタ全体のボリュームを統合し、単一の論理ファイルシステムを実現します。FPolicy サーバはネームスペーストポロジを認識し、ネームスペース全体に FPolicy サービスを提供します。

ネームスペースは SVM に固有のもので、その内部に含まれています。したがって、ネームスペースは SVM コンテキストからのみ表示できます。ネームスペースには次のような特徴があります。

- 各 SVM には単一のネームスペースが存在します。ネームスペースのルートはルートボリュームで、ネームスペース内ではスラッシュ（ / ）で表されます。
- それ以外のボリュームには、ルート（ / ）より下のジャンクションポイントがあります。
- ボリュームジャンクションは、クライアントに対して透過的です。
- 単一の NFS エクスポートは、ネームスペース全体へのアクセスを提供できます。あるいは、エクスポートポリシーで特定のボリュームをエクスポートできます。
- ネームスペース内のボリューム、ボリューム内の qtree 、またはディレクトリに SMB 共有を作成できます。
- ネームスペースアーキテクチャは柔軟です。

  一般的なネームスペースアーキテクチャの例を次に示します。

  - ルートからの分岐が 1 つだけのネームスペース
  - ルートからの分岐が複数あるネームスペース
  - ルートから分岐していないボリュームが複数あるネームスペース

ONTAP FPolicyパススルーリードが階層型ストレージ管理の使いやすさを向上させる仕組み

パススルーリードを使用すると、オフラインファイルに対する読み取りアクセスを（階層型ストレージ管理（HSM）サーバとして機能している）FPolicyサーバから提供できます。セカンダリストレージシステムからプライマリストレージシステムにファイルをリコールする必要はありません。

SMBサーバ上にあるファイルにHSMを提供するようにFPolicyサーバが設定されている場合、ポリシーベースのファイル移行が実行されます。この場合、ファイルはセカンダリストレージにオフラインで保存され、スタブファイルのみがプライマリストレージに残ります。スタブファイルはクライアントからは通常のファイルとして認識されますが、実際には元のファイルと同じサイズのスパースファイルです。スパースファイルにはSMBオフラインビットが設定されており、セカンダリストレージに移行された実際のファイルを参照しています。

通常、オフラインファイルの読み取り要求を受信した場合は、要求されたコンテンツをプライマリストレージにリコールしてから、プライマリストレージ経由でアクセスする必要があります。データをプライマリストレージにリコールする必要があるため、望ましくない影響がいくつかあります。望ましくない影響としては、コンテンツをリコールしてから要求に応答する必要があることが原因でクライアント要求に対するレイテンシが増加したり、プライマリストレージでリコールされるファイルに必要なスペースが増加したりすることがあります。

FPolicyパススルーリードを使用すると、移行されたオフラインファイルに対する読み取りアクセスをHSMサ

ーバ（FPolicyサーバ）が提供できます。セカンダリストレージシステムからプライマリストレージシステムにファイルをリコールする必要はありません。プライマリストレージにファイルをリコールする代わりに、読み取り要求をセカンダリストレージから直接処理できます。

FPolicyのパススルーリード処理では、コピーオフロード（ODX）はサポートされません。

パススルーリードには次のような利点があり、ユーザビリティが向上します。

- 要求されたデータをリコールするための十分なスペースがプライマリストレージにない場合でも、読み取り要求を処理できます。
- スクリプトやバックアップソリューションで多数のオフラインファイルにアクセスする必要がある場合など、データリコールが急増する可能性がある場合は、容量とパフォーマンスの管理が向上します。
- Snapshot内のオフラインファイルに対する読み取り要求を処理できます。

  Snapshotは読み取り専用であるため、スタブファイルがSnapshot内にある場合、FPolicyサーバは元のファイルをリストアできません。パススルーリードを使用すると、この問題が解消されます。

- 読み取り要求をセカンダリストレージ上のファイルにアクセスして処理するタイミングと、オフラインファイルをプライマリストレージにリコールするタイミングを制御するポリシーを設定できます。

  たとえば、オフラインファイルがプライマリストレージに移行されるまでに、指定した期間内にオフラインファイルにアクセスできる回数を指定するポリシーをHSMサーバ上に作成できます。このタイプのポリシーにより、滅多にアクセスされないファイルのリコールを回避できます。

FPolicyパススルーリードが有効になっている場合の読み取り要求の管理方法

Storage Virtual Machine（SVM）とFPolicyサーバ間の接続を最適な形で設定できるように、FPolicyパススルーリードが有効になっている場合の読み取り要求の管理方法を理解しておく必要があります。

FPolicyパススルーリードが有効になっている場合にSVMがオフラインのファイルに対する要求を受信すると、FPolicyは標準の接続チャネルを介してFPolicyサーバ（HSMサーバ）に通知を送信します。

通知を受信すると、FPolicyサーバは通知で送信されたファイルパスからデータを読み取り、要求されたデータをSVMとFPolicyサーバの間に確立されたパススルーリード権限付きデータ接続を介してSVMに送信します。

データが送信されると、FPolicyサーバは読み取り要求にallowまたはdenyとして応答します。読み取り要求が許可されたか拒否されたかに基づいて、ONTAPは要求された情報またはエラーメッセージをクライアントに送信します。

FPolicy設定を計画する

ONTAP FPolicy を構成するための要件、考慮事項、およびベストプラクティス

Storage Virtual Machine（SVM）でFPolicyの設定を作成して設定する前に、FPolicyの設定に関する一定の要件、考慮事項、およびベストプラクティスについて確認しておく必要があります。

FPolicy機能は、コマンドラインインターフェイス（CLI）またはREST APIを使用して設定します。

FPolicyを設定するための要件

Storage Virtual Machine（SVM）でFPolicyを設定して有効にする前に、一定の要件について確認しておく必要があります。

- クラスタ内のすべてのノードで、FPolicyがサポートされているバージョンのONTAPが実行されている必要があります。
- ONTAPの標準のFPolicyエンジンを使用しない場合は、外部FPolicyサーバ（FPolicyサーバ）をインストールしておく必要があります。
- FPolicyポリシーが有効になっているSVMのデータLIFからアクセスできるサーバに、FPolicyサーバがインストールされている必要があります。

> ONTAP 9 .8以降では、ONTAPは `data-fpolicy-client`サービスを追加することでアウトバウンドFPolicy接続用のクライアントLIFサービスを提供しています。"LIFとサービスポリシーの詳細については、こちらをご覧ください"です。

- FPolicyポリシーの外部エンジンの設定で、FPolicyサーバのIPアドレスがプライマリサーバまたはセカンダリサーバとして設定されている必要があります。
- FPolicyサーバが権限付きデータチャネルを使用してデータにアクセスする場合は、次の追加要件を満たす必要があります。
  - クラスタでSMBのライセンスが有効になっている必要があります。

    権限付きデータアクセスはSMB接続を使用して実行されます。
  - 権限付きデータチャネル経由でファイルにアクセスするためのユーザクレデンシャルが設定されている必要があります。
  - FPolicyサーバは、FPolicyの設定で設定されたクレデンシャルで実行されている必要があります。
  - FPolicyサーバとの通信に使用されるすべてのデータLIFが、許可されているプロトコルの1つとして設定されている必要があります `cifs`。

    これには、パススルーリード接続に使用されるLIFも含まれます。

FPolicyを設定する際のベストプラクティスと推奨事項

Storage Virtual Machine（SVM）でFPolicyを設定する場合は、FPolicyの設定によって監視のパフォーマンスが向上し、要件を満たす結果が得られるようにするために、設定に関する一般的なベストプラクティスと推奨事項を理解してください。

パフォーマンス、サイジング、および設定に関する具体的なガイドラインについては、FPolicyパートナーアプリケーションを参照してください。

永続的ストア

ONTAP 9.14.1以降では、FPolicyを使用して永続的ストアを作成し、SVM内の非同期で必須でないポリシーのファイル アクセス イベントをキャプチャできます。永続的ストアは、クライアントI/O処理をFPolicy通知処理から分離して、クライアントのレイテンシを低減するのに役立ちます。同期（必須かどうかは問わない）および非同期で必須の設定はサポートされていません。

- 永続的ストア機能を使用する前に、この設定がパートナー アプリケーションでサポートされていることを

確認してください。

- FPolicyが有効になっているSVMごとに永続的ストアが1つ必要です。
  - 各SVMに設定できる永続的ストアは1つだけです。ポリシーが別 々 のパートナーのものであっても、この単一の永続的ストアをそのSVM上のすべてのFPolicy設定に使用する必要があります。
- ONTAP 9.15.1以降：
  - 永続的ストア、そのボリューム、およびボリューム設定は、永続的ストアの作成時に自動的に処理されます。
- ONTAP 9.14.1：
  - 永続的ストア、そのボリューム、およびボリューム設定は手動で処理します。
- 永続的ストアのボリュームは、FPolicyによって監視されるトラフィック量が最大になると想定されるLIFがあるノードに作成します。
  - ONTAP 9.15.1以降：永続的ストアの作成時にボリュームが自動的に作成および設定されます。
  - ONTAP 9.14.1：クラスタ管理者は、FPolicyが有効になっている各SVMで永続的ストア用のボリュームを作成し、設定する必要があります。
- 永続的ストアに蓄積された通知がプロビジョニングされたボリュームのサイズを超えると、FPolicyは適切なEMSメッセージを含む受信通知を破棄し始めます。
  - ONTAP 9 .15.1以降：パラメータに加えて `size`、 `autosize-mode`パラメータを使用すると、使用済みスペースの量に応じてボリュームを拡張または縮小できます。
  - ONTAP 9 .14.1：この `size`パラメータは、ボリュームの作成時に最大数を指定するように設定されます。
- 永続的ストアボリュームのSnapshotポリシーをではなくに `default`設定します `none`。これは、Snapshotが誤ってリストアされて現在のイベントが失われることがないようにし、イベント処理が重複しないようにするためです。
  - ONTAP 9 .15.1以降： `snapshot-policy`永続ストアの作成時に、パラメータは自動的にnoneに設定されます。
  - ONTAP 9 .14.1： `snapshot-policy`ボリュームの作成時にパラメータがに設定されます `none`。
- 永続的なイベントレコードが誤って破損したり削除されたりしないように、外部ユーザプロトコルアクセス（CIFS / NFS）で永続的ストアボリュームにアクセスできないようにします。
  - ONTAP 9.15.1以降：ONTAPは、永続的ストアの作成時に外部ユーザプロトコルアクセス（CIFS / NFS）からボリュームを自動的にブロックします。
  - ONTAP 9.14.1：FPolicyを有効にしたら、ONTAPでボリュームをアンマウントしてジャンクションパスを削除します。これにより、外部ユーザプロトコルによるアクセス（CIFS / NFS）ができなくなります。

詳細については、およびを参照して "FPolicyの永続的ストア" "永続ストアの作成"ください。

永続的ストアのフェイルオーバーとギブバック

永続ストアは、最後のイベントを受信したとき、予期しないリブートが発生したとき、またはFPolicyを無効にして再度有効にしたときのままです。テイクオーバー処理が完了すると、新しいイベントがパートナーノードに格納されて処理されます。ギブバック処理のあと、ノードのテイクオーバーの発生時に残っている可能性がある未処理のイベントの処理が永続的ストアで再開されます。ライブイベントは、未処理のイベントよりも優先されます。

永続的ストアのボリュームが、あるノードから同じSVM内の別のノードに移動された場合、まだ処理されていない通知も新しいノードに移動します。再度実行する必要があります `fpolicy persistent-store create`保留中の通知が外部サーバーに配信されるようにするには、ボリュームの移動後にどちらかのノードでコマンドを実行します。

詳細はこちら `fpolicy persistent-store create`の中で"ONTAPコマンド リファレンス" 。

ポリシー設定

FPolicy外部エンジン、イベント、SVM用のスコープを設定することで、全体的なエクスペリエンスとセキュリティが向上する可能性があります。

- SVM用のFPolicy外部エンジンの設定：
  - セキュリティを強化するには、パフォーマンスコストがかかります。Secure Sockets Layer（SSL）通信を有効にすると、共有へのアクセスのパフォーマンスに影響します。
  - FPolicyサーバの通知処理の耐障害性と高可用性を確保するには、FPolicy外部エンジンに複数のFPolicyサーバを設定する必要があります。
- SVMのFPolicyイベントの設定

  ファイル操作の監視は、エクスペリエンス全体に影響します。たとえば、ストレージ側で不要なファイル操作をフィルタリングすると、操作性が向上します。NetAppでは、次の設定を推奨しています。
  - ユースケースを壊さずに、最小タイプのファイル処理を監視し、最大数のフィルタを有効にする。
  - 属性取得、読み取り、書き込み、オープン、クローズの各処理にフィルタを使用する。SMBおよびNFSホームディレクトリ環境では、これらの処理の割合が高くなっています。
- SVMのFPolicyスコープの設定

  ポリシーの範囲を、SVM全体ではなく、関連するストレージオブジェクト（共有、ボリューム、エクスポートなど）に制限します。NetAppでは、ディレクトリ拡張子の確認を推奨していますパラメータがに設定されて `true`いる場合 `is-file-extension-check-on-directories-enabled`、ディレクトリオブジェクトには通常のファイルと同じ拡張子チェックが実行されます。

ネットワーク設定

FPolicyサーバとコントローラの間のネットワーク接続のレイテンシを低くする必要があります。NetAppでは、プライベートネットワークを使用してFPolicyトラフィックをクライアントトラフィックから分離することを推奨しています。

また、レイテンシを最小限に抑え、広帯域接続を実現するために、外部FPolicyサーバ（FPolicyサーバ）を広帯域接続が可能なクラスタの近くに配置する必要があります。

> FPolicyトラフィック用のLIFがクライアントトラフィック用のLIFとは別のポートに設定されている場合、ポートの障害が原因でFPolicy LIFがもう一方のノードにフェイルオーバーすることがあります。その結果、ノードからFPolicyサーバに到達できなくなり、ノードでのファイル操作に関するFPolicy通知は失敗します。この問題を回避するには、ノード上の少なくとも1つのLIFからFPolicyサーバにアクセスして、そのノードで実行されるファイル操作のFPolicy要求を処理できることを確認します。

ハードウェア構成

FPolicyサーバは、物理サーバと仮想サーバのどちらにも配置できます。FPolicyサーバが仮想環境にある場合は、仮想サーバに専用のリソース（CPU、ネットワーク、メモリ）を割り当てる必要があります。

SVMがクライアント要求に応答する際のレイテンシの原因となる可能性があるFPolicyサーバの過負荷状態を防ぐために、クラスタ ノードとFPolicyサーバの比率を最適化する必要があります。最適な比率は、FPolicyサーバが使用されているパートナー アプリケーションによって異なります。NetAppは、適切な値を見極めるためにパートナーと協力することを推奨しています。

複数ポリシーの設定

ネイティブ ブロッキング用のFPolicyポリシーはシーケンス番号に関係なく最優先され、決定変更ポリシーは他のポリシーよりも優先されます。ポリシーの優先度は、ユースケースによって異なります。NetAppは、適切な優先度を見極めるためにパートナーと協力することを推奨しています。

サイズに関する考慮事項

FPolicyは、SMB処理とNFS処理のインライン監視を実行し、外部サーバに通知を送信し、外部エンジンの通信モード（同期または非同期）に基づいて応答を待ちます。このプロセスは、SMBとNFSのアクセスとCPUリソースのパフォーマンスに影響します。

何らかの問題につながる可能性を抑えるため、NetAppは、FPolicyを有効にする前にパートナーと協力して環境の評価とサイジングを行うことを推奨しています。パフォーマンスは、ユーザ数、ユーザあたりの処理数やデータ サイズなどのワークロード特性、ネットワーク レイテンシ、障害やサーバの速度低下など、複数の要因から影響を受けます。

パフォーマンスの監視

FPolicyは、通知ベースのシステムです。通知は外部サーバに送信され、そこで処理され、生成された応答がONTAPに返されます。この往復プロセスにより、クライアント アクセスのレイテンシが増加します。

FPolicyサーバとONTAPのパフォーマンス カウンタを監視することで、ソリューション内のボトルネックを特定し、必要に応じてパラメータを調整してソリューションを最適化できます。たとえば、FPolicyのレイテンシの増加は、連鎖的にSMBとNFSのアクセス レイテンシに影響を及ぼします。そのため、ワークロード（SMBとNFS）とFPolicyのレイテンシのどちらも監視する必要があります。加えて、ONTAPのサービス品質（QoS）ポリシーを使用して、FPolicyが有効になっているボリュームやSVMごとにワークロードの設定を行えます。

NetAppでは、コマンドを実行してワークロードの統計情報を表示することを推奨 `statistics show –object workload`さらに、次のパラメータを監視する必要があります。

- 平均レイテンシ、読み取りレイテンシ、書き込みレイテンシ
- 処理の総数
- 読み取り / 書き込みカウンタ

FPolicyサブシステムのパフォーマンスを監視するために、次のFPolicyカウンタを使用できます。

FPolicyに関連する統計を収集するには、診断モードにする必要があります。

手順

1. FPolicyカウンタを収集します。
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. FPolicyカウンタを表示します。
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   `fpolicy`カウンタと`fpolicy_server`カウンタには、次の表に示す複数のパフォーマンスパラメータに関する情報が表示されます。

カウンタ	説明
• fpolicyカウンタ*	aborted_requests
SVMで処理が中止されたスクリーニング要求の数	event_count
通知の原因になったイベントのリスト	max_request_latency
スクリーニング要求の最大レイテンシ	outstanding_requests
処理中のスクリーン要求の総数	processed_requests
SVMでFPolicyの処理が完了したスクリーニング要求の総数	request_latency_hist
スクリーニング要求のレイテンシのヒストグラム	requests_dispatched_rate
送信されたスクリーニング要求の1秒あたりの数	requests_received_rate
受信したスクリーニング要求の1秒あたりの数	• fpolicy_serverカウンタ*
max_request_latency	画面要求の最大遅延
outstanding_requests	応答を待機している画面要求の総数
request_latency	スクリーニング要求の平均レイテンシ
request_latency_hist	スクリーニング要求のレイテンシのヒストグラム

カウンタ	説明
request_sent_rate	FPolicyサーバに送信されたスクリーニング要求の1秒あたりの数
response_received_rate	FPolicyサーバから受信したスクリーニング応答の1秒あたりの数

および `statistics show`の詳細については `statistics start`、を"ONTAPコマンド リファレンス"参照してください。

FPolicyのワークフローと他のテクノロジへの依存の管理

NetAppは、設定を変更する前にFPolicyポリシーを無効にすることを推奨しています。たとえば、有効になっているポリシーに設定された外部エンジンのIPアドレスを追加または変更する場合は、まずポリシーを無効にします。

NetApp FlexCacheボリュームを監視するようにFPolicyを設定する場合、NetAppは、読み取りと属性取得のファイル処理を監視するようにFPolicyを設定しないことを推奨しています。これらの処理をONTAPで監視するには、Inode-to-Path（I2P）データを取得する必要があります。I2Pデータは、FlexCacheボリュームからは取得できないため、元のボリュームから取得する必要があります。そのため、これらの処理を監視することで、FlexCacheで得られるパフォーマンス上のメリットが帳消しになってしまいます。

FPolicyと外部のウイルス対策ソリューションを両方とも導入している場合、最初にウイルス対策ソリューションが通知を受信します。FPolicyの処理は、ウイルス対策スキャンの完了後に開始されます。ウイルス対策スキャナが低速だと全体的なパフォーマンスに影響する可能性があるため、ウイルス対策ソリューションの適切なサイジングが重要になります。

パススルー リードのアップグレードとリバートに関する考慮事項

パススルー リードをサポートしているONTAPリリースへのアップグレードまたはパススルー リードをサポートしていないリリースへのリバートを行う前に、アップグレードおよびリバートに関する考慮事項を把握しておく必要があります。

アップグレード

FPolicyパススルー リードをサポートしているONTAPのバージョンにすべてのノードをアップグレードしたあと、クラスタはパススルー リードを使用できるようになります。ただし、既存のFPolicy設定ではパススルー リードがデフォルトで無効になっています。既存のFPolicy設定でパススルー リードを使用するには、FPolicyポリシーを無効にして設定を変更したうえで、設定を再び有効にする必要があります。

リバート

FPolicyをサポートしていないONTAPのバージョンにリバートする前に、以下の条件を満たす必要があります。

- パススルー リードを使用しているすべてのポリシーを無効にしたうえで、影響を受ける設定を変更してパススルー リードを使用しないようにする必要があります。
- クラスタ上のすべてのFPolicyポリシーを無効にして、クラスタのFPolicy機能を無効にします。

永続的ストアをサポートしないバージョンのONTAPにリバートする前に、FPolicyポリシーに永続的ストアが設定されていないことを確認してください。永続ストアが設定されている場合、リバートは失敗します。

関連情報

- "statistics show"
- "statistics start"

ONTAP FPolicy設定をセットアップする

FPolicyでファイルアクセスを監視するには、FPolicyの設定を作成し、FPolicyサービスが必要なStorage Virtual Machine（SVM）で有効にする必要があります。

SVMでFPolicy設定をセットアップして有効にする手順は次のとおりです。

1. FPolicy外部エンジンを作成します。

   FPolicy外部エンジンは、特定のFPolicyの設定に関連付けられた外部FPolicyサーバ（FPolicyサーバ）を識別します。内部の「ネイティブ」 FPolicy エンジンを使用してネイティブ・ファイル・ブロッキング構成を作成する場合は、 FPolicy 外部エンジンを作成する必要はありません。

   ONTAP 9 .15.1以降では、エンジン形式を使用できます `protobuf`。に設定する `protobuf`と、通知メッセージはGoogle Protobufを使用してバイナリ形式でエンコードされます。エンジン形式をに設定する前に、 `protobuf`FPolicyサーバでもデシリアライゼーションがサポートされていることを確認して `protobuf`ください。詳細については、を参照してください。 "FPolicy外部エンジンの設定を計画する"

2. FPolicyイベントを作成します。

   FPolicyイベントは、FPolicyポリシーで監視する対象を定義します。イベントは監視対象のプロトコルとファイル操作で構成され、一連のフィルタを含めることができます。イベントでは、フィルタを使用して、FPolicy外部エンジンから通知を送信する必要がある監視対象イベントのリストを絞り込みます。イベントは、ポリシーがボリューム操作を監視するかどうかも指定します。

3. FPolicy永続ストアを作成します（オプション）。

   14.1以降では、ONTAP 9の必須ではない非同期ポリシーのファイルアクセスイベントをキャプチャするようにを設定でき"永続的ストア"ます。同期（必須または非必須）および非同期の必須構成はサポートされていません。

   永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。

   ONTAP 9 .15.1以降では、FPolicyの永続的ストアの設定が簡素化されています。 `persistent-store-create`コマンドは、SVM用のボリュームの作成を自動化し、永続的ストア用のボリュームを設定します。

4. FPolicyポリシーを作成します。

   FPolicyポリシーでは、監視する必要がある一連のイベントと、指定のFPolicyサーバ（FPolicyサーバが設定されていない場合は標準のエンジン）に通知を送信する必要がある監視対象イベントを、適切な範囲で関連付けます。また、通知を受信するデータへの権限付きアクセスをFPolicyサーバに許可するかどうかも定義します。FPolicyサーバからデータにアクセスする必要がある場合は、権限付きアクセスが必要になります。権限付きアクセスが必要な一般的なユースケースには、ファイルブロッキング、クォータ管理、階層型ストレージ管理などがあります。ポリシーは、このポリシーの設定で FPolicy サーバを使用するか、内部の「ネイティブ」 FPolicy サーバを使用するかを指定します。

   スクリーニングを必須にするかどうかはポリシーで指定します。スクリーニングを必須にすると、すべてのFPolicyサーバが停止した場合や定義された時間内にFPolicyサーバからの応答を得られない場合に、フ

ァイル アクセスが拒否されます。

ポリシーはSVM単位で適用されます。1つのポリシーを複数のSVMに適用することはできません。ただし、ある特定のSVMに複数のFPolicyポリシーを含めることは可能で、範囲、イベント、外部サーバの設定を同じ組み合わせにすることも、それぞれで異なる組み合わせにすることもできます。

5. ポリシーの範囲を設定します。

   FPolicyスコープでは、ボリューム、共有、またはエクスポート ポリシーについて、ポリシーで監視するものと除外するものを指定します。また、ファイル拡張子についても、FPolicyの監視対象に含めるものと除外するものを指定します。

   除外リストの方が対象リストよりも優先されます。

6. FPolicyポリシーを有効にします。

   ポリシーを有効にすると、制御チャネルおよび特権データ チャネル（オプション）の接続が確立されます。SVMが属するノードのFPolicyプロセスで、ファイルおよびフォルダに対するアクセスの監視が開始され、設定された条件に当てはまるイベントが見つかると、FPolicyサーバ（FPolicyサーバが設定されていない場合は標準のエンジン）に通知が送信されます。

ポリシーでネイティブ ファイル ブロッキングを使用する場合は、外部エンジンは設定されず、関連付けられることもありません。

FPolicy外部エンジンの設定を計画する

ONTAP FPolicy外部エンジン構成を計画する

FPolicy外部エンジンを設定する前に、外部エンジンを作成することの意味と、使用可能な設定パラメータを理解する必要があります。この情報は、各パラメータに設定する値を決定するのに役立ちます。

FPolicy外部エンジンの作成時に定義される情報

外部エンジンの設定では、外部FPolicyサーバへの接続を作成および管理するためにFPolicyが必要とする次のような情報を定義します。

- SVM名
- エンジン名
- FPolicyサーバへの接続時に使用するプライマリおよびセカンダリFPolicyサーバのIPアドレスとTCPポート番号
- エンジンタイプが非同期か同期か
- エンジンフォーマットがまたは `protobuf`かどうか `xml`

  ONTAP 9 .15.1以降では、エンジン形式を使用できます `protobuf`。に設定する `protobuf`と、通知メッセージはGoogle Protobufを使用してバイナリ形式でエンコードされます。エンジン形式をに設定する前に、 `protobuf`FPolicyサーバでもデシリアライゼーションがサポートされていることを確認して `protobuf`ください。

protobuf形式はONTAP 9 .15.1以降でサポートされているため、以前のリリースのONTAPにリバートする前に外部エンジン形式を考慮する必要があります。ONTAP 9.15.1より前のリリースにリバートする場合は、FPolicyパートナーと協力して次のいずれかを実行します。

  - 各エンジンフォーマットをからに `xml`変更します。 `protobuf`
  - エンジンフォーマットがのエンジンを削除します。 `protobuf`

- ノードとFPolicyサーバ間の接続を認証する方法

  相互SSL認証を設定する場合は、SSL証明書情報を提供するパラメータも設定する必要があります。

- 各種の高度な権限設定を使用して接続を管理する方法

  これには、タイムアウト値、リトライ値、キープアライブ値、最大要求値、送信および受信バッファ サイズ値、セッション タイムアウト値などを定義するパラメータが含まれます。

コマンドは、 `vserver fpolicy policy external-engine create`FPolicy外部エンジンの作成に使用します。

外部エンジンの基本パラメータ

次に示すFPolicy基本設定パラメータの一覧は、設定を計画するのに役立ちます。

情報の種類	オプション
SVM この外部エンジンに関連付けるSVMの名前を指定します。 各FPolicy設定は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。	`-vserver vserver_name`

_ エンジン名 _ 外部エンジンの設定に割り当てる名前を指定します。FPolicyポリシーを作成した場合、あとで外部エンジンの名前を指定する必要があります。こうすることで、外部エンジンがポリシーに関連付けられます。 名前の最大文字数は256文字です。 MetroClusterまたはSVMディザスタリカバリ設定で外部エンジン名を設定する場合、この名前は最大200文字にする必要があります。 名前には、次のASCII文字の任意の組み合わせを含めることができます。 • a`から `z • A`から `Z • 0`から `9 • “_”、“.”-", and "	-engine-name engine_name
プライマリ FPolicy サーバ _ 所定のFPolicyポリシーに関してノードが送信する通知の宛先となるプライマリFPolicyサーバを指定します。IPアドレスの値をカンマで区切って指定します。 複数のプライマリサーバのIPアドレスを指定した場合、SVMが参加しているすべてのノードに、ポリシーが有効になったときに指定されたすべてのプライマリFPolicyサーバへの制御接続が作成されます。複数のプライマリFPolicyサーバを設定した場合、通知はラウンドロビン方式でFPolicyサーバに送信されます。 外部エンジンがMetroClusterまたはSVMディザスタリカバリ設定で使用されている場合は、ソースサイトでのFPolicyサーバのIPアドレスをプライマリサーバとして指定する必要があります。デスティネーションサイトのFPolicyサーバのIPアドレスは、セカンダリサーバとして指定する必要があります。	-primary-servers `IP_address`はい。
ポート番号 _ FPolicyサービスのポート番号を指定します。	-port integer

_ セカンダリ FPolicy サーバ _ 所定のFPolicyポリシーに関して、ファイルアクセスイベントの送信先となるセカンダリFPolicyサーバを指定します。IPアドレスの値をカンマで区切って指定します。 セカンダリサーバは、いずれのプライマリサーバにも到達できない場合にのみ使用されます。ポリシーを有効にすると、セカンダリサーバへの接続が確立されますが、通知がセカンダリサーバに送信されるのは、いずれのプライマリサーバにも到達できない場合だけです。複数のセカンダリサーバを設定した場合、通知はラウンドロビン方式でFPolicyサーバに送信されます。	`-secondary-servers` `IP_address`はい。
_ 外部エンジンタイプ _ 外部エンジンが同期モードで動作するか非同期モードで動作するかを指定します。デフォルトでは、FPolicyは同期モードで動作します。 に設定する `synchronous`と、ファイル要求処理によって通知がFPolicyサーバに送信されますが、その後FPolicyサーバから応答を受信するまでは通知は送信されません。この時点で、要求されたアクションがFPolicyサーバからの応答で許可されるかどうかに応じて、要求フローが続行されるか処理が拒否されます。 に設定する `asynchronous`と、ファイル要求処理はFPolicyサーバに通知を送信したあとも続行します。	`-extern-engine-type` `external_engine_type`このパラメータには、次のいずれかの値を指定できます。 • `synchronous` • `asynchronous`
外部エンジンフォーマット 外部エンジン形式がXMLかprotobufかを指定します。 ONTAP 9 .15.1以降では、protobufエンジン形式を使用できます。protobufに設定すると、通知メッセージはGoogle Protobufを使用してバイナリ形式でエンコードされます。エンジン形式をprotobufに設定する前に、FPolicyサーバでもprotobufデシリアライゼーションがサポートされていることを確認してください。	`- extern-engine-format` {`protobuf` または `xml`}

_SSL オプションを使用して FPolicy サーバと通信します FPolicyサーバとの通信に使用するSSLオプションを指定します。これは必須パラメータです。次の情報に基づいて、いずれかのオプションを選択できます。 • に設定する `no-auth`と、認証は行われません。 通信リンクはTCPを介して確立されます。 • に設定する `server-auth`と、SVMはSSLサーバ認証を使用してFPolicyサーバを認証します。 • に設定する `mutual-auth`と、SVMとFPolicyサーバの間で相互認証が行われ、SVMはFPolicyサーバを認証し、FPolicyサーバはSVMを認証します。 相互SSL認証を設定する場合は、、 `-certificate-serial`、の `-certifcate-ca`各パラメータも設定する必要があります `-certificate-common-name`。	`-ssl-option{no-auth`
`server-auth`	`mutual-auth}`
_ 証明書 FQDN またはカスタム共通名 _ SVMとFPolicyサーバ間のSSL認証が設定されている場合に使用される証明書の名前を指定します。証明書の名前は、FQDNまたはカスタム共通名で指定できます。 パラメータに `-ssl-option`を指定する場合 `mutual-auth`は、パラメータの値を指定する必要があります `-certificate-common-name`。	`-certificate-common-name text`
証明書シリアル番号 _ SVMとFPolicyサーバ間のSSL認証が設定されている場合に認証に使用される証明書のシリアル番号を指定します。 パラメータに `-ssl-option`を指定する場合 `mutual-auth`は、パラメータの値を指定する必要があります `-certificate-serial`。	`-certificate-serial text`
_ 認証局 _ SVMとFPolicyサーバ間のSSL認証が設定されている場合に認証に使用される証明書のCA名を指定します。 パラメータに `-ssl-option`を指定する場合 `mutual-auth`は、パラメータの値を指定する必要があります `-certificate-ca`。	`-certificate-ca text`

外部エンジンの詳細オプションとは

次の高度なFPolicy設定パラメータの表は、高度なパラメータを使用して設定をカスタマイズするかどうかを計画する際に使用できます。これらのパラメータを使用して、クラスタノードとFPolicyサーバ間の通信動作を変更します。

情報の種類	オプション
_ リクエストをキャンセルするためのタイムアウト _ (s`ノードがFPolicyサーバからの応答を待機する時間間隔（時間(`h）、分(m、または秒）を指定します。 タイムアウト間隔が経過すると、ノードはFPolicyサーバにキャンセル要求を送信します。その後、ノードから代替FPolicyサーバに通知が送信されます。このタイムアウトは、応答していないFPolicyサーバを処理するのに役立ちます。これにより、SMB / NFSクライアントの応答を改善できます。また、通知要求が停止している、または無効なFPolicyサーバから代替FPolicyサーバに移動されるため、タイムアウト時間後に要求をキャンセルすると、システムリソースを解放するのに役立ちます。 この値の範囲は~ 100`です `0。値がに設定されている場合 0、オプションは無効になり、キャンセル要求メッセージはFPolicyサーバに送信されません。デフォルトはです 20s。	-reqs-cancel-timeout integer[h
m	s]
_ 要求を破棄するためのタイムアウト _ (s`要求を中止するタイムアウト（時間）(`h、分(m、または秒）を指定します。 この値の範囲は~ 200`です `0。	-reqs-abort-timeout ` `integer[h
m	s]
ステータス要求の送信間隔 _ (s`FPolicyサーバにステータス要求を送信する間隔（時間(`h）、分）(m、または秒）を指定します。 この値の範囲は~ 50`です `0。値がに設定されている場合 0、オプションは無効になり、ステータス要求メッセージはFPolicyサーバに送信されません。デフォルトはです 10s。	-status-req-interval integer[h
m	s]
FPolicy サーバの未処理要求の最大数 _ FPolicyサーバのキューに登録できる未処理要求の最大数を指定します。 この値の範囲は~ 10000`です `1。デフォルトはです 500。	-max-server-reqs integer

_ 応答しない FPolicy サーバを切断するタイムアウト _ (s`FPolicyサーバへの接続を終了するまでの時間間隔（時間(`h）、分）(m、または秒を指定します。 FPolicyサーバのキューに許容される最大要求数が含まれていて、タイムアウト期間内に応答がない場合にのみ、タイムアウト期間後に接続を終了します。許可される最大要求数は、（デフォルト）またはパラメータで指定された数 max-server-reqs-`です `50。 この値の範囲は~ 100`です `1。デフォルトはです 60s。	-server-progress -timeout integer[h
m	s]
FPolicy サーバにキープアライブメッセージを送信する間隔 _ (s`FPolicyサーバにキープアライブメッセージを送信する時間間隔を時間(`h、分(m、または秒で指定します。 キープアライブメッセージはハーフオープン接続を検出します。 この値の範囲は~ 600`です `10。値がに設定されている場合 0、オプションは無効になり、キープアライブメッセージはFPolicyサーバに送信されません。デフォルトはです 120s。	-keep-alive-interval-integer[h
m	s]
最大再接続試行回数 _ 接続が切断されたあと、SVMがFPolicyサーバへの再接続を試行する最大回数を指定します。 この値の範囲は~ 20`です `0。デフォルトはです 5。	-max-connection-retries integer
受信バッファサイズ _ FPolicyサーバの接続ソケットの受信バッファサイズを指定します。 デフォルト値は256KBに設定されています。値が0に設定されている場合、受信バッファのサイズはシステムによって定義された値に設定されます。 たとえば、ソケットのデフォルトの受信バッファサイズが65536バイトの場合、調整可能な値を0に設定すると、ソケットバッファサイズは65536バイトに設定されます。デフォルト値以外の任意の値を使用して、受信バッファのサイズ（バイト単位）を設定できます。	-recv-buffer-size integer

送信バッファサイズ _ FPolicyサーバの接続ソケットの送信バッファサイズを指定します。 デフォルト値は256KBに設定されています。値が0に設定されている場合、送信バッファのサイズはシステムによって定義された値に設定されます。 たとえば、ソケットのデフォルトの送信バッファサイズが65536バイトに設定されている場合、調整可能な値を0に設定すると、ソケットバッファサイズは65536バイトに設定されます。デフォルト値以外の任意の値を使用して、送信バッファのサイズ（バイト単位）を設定できます。	`-send-buffer-size integer`
_ 再接続中にセッション ID を消去するためのタイムアウト _ (s`再接続の試行時に`FPolicy`サーバに新しい`Session ID`が送信されるまでの間隔（時間`(`h`）、分）(`m、または秒を指定します。  ストレージコントローラとFPolicyサーバの間の接続が終了し、その期間内に再接続が行われる `-session-timeout`と、古い通知に対する応答を送信できるように、古いSession IDがFPolicyサーバに送信されます。 デフォルト値は10秒に設定されています。	`-session-timeout [h][m]integerintegerinteger`

SSL認証接続を使用するように**ONTAP FPolicy**外部エンジンを構成する方法の追加情報

FPolicyサーバへの接続時にSSLを使用するようにFPolicy外部エンジンを設定する場合は、いくつかの追加情報を確認しておく必要があります。

SSLサーバ認証

SSL サーバ認証用の FPolicy 外部エンジンを設定する場合には、外部エンジンを作成する前に、 FPolicy サーバ証明書の署名を行った認証局（ CA ）のパブリック証明書をインストールする必要があります。

相互認証

Storage Virtual Machine（SVM）のデータLIFを外部FPolicyサーバに接続するときにSSL相互認証を使用するようにFPolicy外部エンジンを設定する場合は、外部エンジンを作成する前に、FPolicyサーバ証明書の署名を行ったCAのパブリック証明書を、SVMの認証用のパブリック証明書およびキーファイルとともにインストールする必要があります。インストールされている証明書をFPolicyポリシーが使用している間は、この証明書を削除しないでください。

FPolicyが相互認証に証明書を使用しているときに証明書を削除した場合、その証明書を使用する無効になっているFPolicyポリシーを再度有効にすることはできません。この状況では、同じ設定で証明書を新規作成して SVM にインストールしても、 FPolicy ポリシーを再度有効にすることはできません。

証明書が削除されている場合は、新しい証明書をインストールし、その証明書を使用する新しいFPolicy外部エンジンを作成し、FPolicyポリシーを変更して再度有効にするFPolicyポリシーに新しい外部エンジンを関連付ける必要があります。

SSL用の証明書のインストール

FPolicyサーバ証明書に署名したCAのパブリック証明書をインストールするには、コマンドで `-type`パラメータをに設定 `client-ca`し `security certificate install`ます。SVMの認証に必要な秘密鍵とパブリック証明書をインストールするには、コマンドを `-type`使用して、 `security certificate install`パラメータをに設定 `server`します。

関連情報

- "セキュリティ証明書のインストール"

ONTAP FPolicy証明書は、**ID**保持なしの構成の**SVM**災害復旧関係では複製されません。

FPolicyサーバへの接続時にSSL認証に使用されるセキュリティ証明書は、IDが保持されない設定のSVMディザスタリカバリ先にレプリケートされません。SVM上のFPolicy外部エンジンの設定はレプリケートされますが、セキュリティ証明書はレプリケートされません。セキュリティ証明書をデスティネーションに手動でインストールする必要があります。

SVMディザスタリカバリ関係の設定時にコマンドのオプション `snapmirror create`に選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

このオプションを（ID保持）に `true`設定する `-identity-preserve`と、セキュリティ証明書の情報を含むすべてのFPolicy設定の詳細がレプリケートされます。セキュリティ証明書をデスティネーションにインストールする必要があるのは、オプションを（ID保持なし）に設定した場合だけ `false`です。

関連情報

- "スナップミラー作成"

MetroClusterおよび**SVM**ディザスタリカバリ構成におけるクラスタスコープの**ONTAP FPolicy**外部エンジンの制限

クラスタを対象としたFPolicy外部エンジンを作成するには、クラスタStorage Virtual Machine（SVM）をそのエンジンに割り当てます。ただし、MetroClusterまたはSVMディザスタリカバリ設定でクラスタ対象の外部エンジンを作成する場合は、SVMがFPolicyサーバとの外部通信に使用する認証方式を選択する際に一定の制限事項があります。

外部FPolicyサーバの作成時に選択できる認証オプションには、認証なし、SSLサーバ認証、およびSSL相互認証の3つがあります。外部FPolicyサーバがデータSVMに割り当てられている場合に認証オプションを選択する際の制限事項はありませんが、クラスタ対象のFPolicy外部エンジンを作成する際には制限事項があります。

構成	許可されるかどうか
MetroClusterまたはSVMディザスタリカバリと、認証を行わないクラスタ対象FPolicy外部エンジン（SSL未設定）	○
MetroClusterまたはSVMディザスタリカバリと、SSLサーバまたはSSL相互認証を備えたクラスタ対象FPolicy外部エンジン	いいえ

- SSL認証を使用するクラスタ対象FPolicy外部エンジンが存在し、MetroClusterまたはSVMディザスタリカバリ設定を作成する場合は、認証を使用しないようにこの外部エンジンを変更するか、MetroClusterまた

はSVMディザスタリカバリ設定を作成する前に外部エンジンを削除する必要があります。

- MetroClusterまたはSVMディザスタリカバリ設定がすでに存在する場合、ONTAPにより、SSL認証を使用するクラスタ対象FPolicy外部エンジンの作成が阻止されます。

ONTAP FPolicy外部エンジン構成ワークシートの完成

このワークシートを使用して、FPolicy外部エンジンの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、外部エンジンを設定する前に、それらのパラメータに使用する値を決定する必要があります。

外部エンジンの基本設定に関する情報

外部エンジンの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報の種類	必須	含める	自分の価値観
Storage Virtual Machine（SVM）名	○	○	
エンジン名	○	○	
フライマリFPolicyサアハ	○	○	
ポート番号	○	○	
セカンダリFPolicyサーバ	いいえ		
外部エンジンタイプ	いいえ		
外部FPolicyサーバとの通信のためのSSLオプション	○	○	
証明書のFQDNまたはカスタム共通名	いいえ		
証明書のシリアル番号	いいえ		
認証局	いいえ		

外部エンジンの詳細パラメータに関する情報

外部エンジンに高度なパラメータを設定するには、advanced権限モードで設定コマンドを入力する必要があります。

情報の種類	必須	含める	自分の価値観
タイムアウトによる要求のキャンセル	いいえ		

タイムアウトによる要求の破棄	いいえ		
ステータス要求の送信間隔	いいえ		
FPolicyサーバの未処理要求の最大数	いいえ		
応答しないFPolicyサーバを切断するタイムアウト	いいえ		
FPolicyサーバへのキープアライブメッセージの送信間隔	いいえ		
再接続の最大試行回数	いいえ		
受信バッファサイズ	いいえ		
送信バッファサイズ	いいえ		
再接続中にSession IDをパージするためのタイムアウト	いいえ		

FPolicyイベントの設定を計画する

ONTAP FPolicyイベント設定の詳細

FPolicyイベントを設定する前に、FPolicyイベントを作成することの意味を理解する必要があります。イベントで監視するプロトコル、監視するイベント、および使用するイベントフィルタを決定する必要があります。この情報は、設定する値を計画するのに役立ちます。

FPolicyイベントを作成することの意味

FPolicyイベントを作成することは、どのファイルアクセス操作を監視するか、またどの監視対象イベント通知を外部FPolicyサーバに送信するかを決定するためにFPolicyプロセスで必要となる情報を定義することを意味します。FPolicyイベントの設定では、次の設定情報を定義します。

- Storage Virtual Machine（SVM）名
- イベント名
- 監視するプロトコル

  FPolicyでは、SMB、NFSv3、NFSv4、およびONTAP 9.15.1以降のNFSv4.1のファイルアクセス処理を監視できます。

- 監視するファイル処理

  すべてのファイル処理が、各プロトコルに対して有効とは限りません。

- 構成するファイル フィルタ

  ファイル処理とフィルタの特定の組み合わせだけが有効です。プロトコルごとに、サポートされる独自の組み合わせがあります。

- ボリュームのマウントおよびアンマウント操作を監視するかどうか

> 3つのパラメータ(`-protocol`、、 `-file-operations`、 `-filters`）との依存関係があります。3つのパラメータの有効な組み合わせは次のとおりです。
>
> - パラメータと `-file-operations`パラメータを指定できます `-protocol`。
> - 3つのパラメータをすべて指定できます。
> - パラメータはどれも指定できません。

FPolicyイベントの設定内容

次に示す使用可能なFPolicyイベント設定パラメータの一覧は、設定を計画するのに役立ちます。

情報の種類	オプション
SVM このFPolicyイベントに関連付けるSVMの名前を指定します。 各FPolicy設定は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。	`-vserver vserver_name`
_ イベント名 _ FPolicyイベントに割り当てる名前を指定します。FPolicyポリシーを作成するときは、イベント名を使用してFPolicyイベントをポリシーに関連付けます。 名前の最大文字数は256文字です。 MetroClusterまたはSVMディザスタリカバリ設定でイベントを設定する場合、この名前は最大200文字にする必要があります。 名前には、次のASCII文字の任意の組み合わせを含めることができます。 - a`から `z - A`から `Z - 0`から `9 - _`""、""、""。""-`", and "	`-event-name event_name`

プロトコル _ FPolicyイベントに設定するプロトコルを指定します。のリスト `-protocol` には、次のいずれかの値を指定できます。 • `cifs` • `nfsv3` • `nfsv4` を指定する場合は `-protocol`、パラメータに有効な値を指定する必要があります `-file-operations`。プロトコルのバージョンが変わると、有効な値が変わることがあります。 ONTAP 9.15.1以降では、NFSv4でNFSv4.0およびNFSv4.1イベントをキャプチャできます。	`-protocol protocol`

_ ファイル操作 _ FPolicyイベントのファイル操作のリストを指定します。 このイベントは、パラメータで指定したプロトコルを使用して、すべてのクライアント要求からこのリストに指定された操作をチェックします `-protocol`。1つ以上のファイル操作をカンマで区切って指定できます。のリスト `-file-operations`には、次の値を1つ以上指定できます。 • `close`ファイルクローズソウサ • `create`ファイルサクセイソウサ • `create-dir`ディレクトリサクセイソウサ • `delete`ファイルサクジョソウサ • `delete_dir`ディレクトリサクジョソウサ • `getattr`属性取得操作 • `link`リンクソウサ • `lookup`ケンサクソウサ • `open`ファイルオープンソウサ • `read`フアイルヨミトリソウサ • `write`フアイルカキコミソウサ • `rename`ファイルメイヘンコウソウサ • `rename_dir`ディレクトリメイヘンコウソウサ • `setattr`属性設定操作用 • `symlink`シンホリツクリンクソウサ を指定する場合は `-file-operations`、パラメータに有効なプロトコルを指定する必要があります `-protocol`。	`-file-operations` `file_operations`はい。

_ フィルタ _ 指定したプロトコルの指定したファイル操作に対するフィルタのリストを指定します。パラメータの値 `-filters`は、クライアント要求をフィルタリングするために使用されます。このリストには、次の1つ以上を指定できます。 パラメータを指定する場合 `-filters`は、パラメータと `-protocol`パラメータに有効な値も指定する必要があります `-file-operations`。 • `monitor-ads`代替データストリームを要求するクライアント要求をフィルタリングするオプション。 • `close-with-modification`変更してクローズ操作を要求するクライアント要求をフィルタリングするオプション。 • `close-without-modification`変更せずにクローズ操作を要求するクライアント要求をフィルタリングするオプション。 • `first-read`初回の読み取りを要求するクライアント要求をフィルタリングするオプション。 • `first-write`初回の書き込みを要求するクライアント要求をフィルタリングするオプション。 • `offline-bit`オフラインビットの設定を要求するクライアント要求をフィルタリングするオプション。 このフィルタを設定すると、オフラインのファイルがアクセスされたときにのみFPolicyサーバが通知を受信します。 • `open-with-delete-intent`削除するためにファイルのオープンを要求するクライアント要求をフィルタリングするオプション。 このフィルタを設定すると、削除するためにファイルを開こうとした場合にのみFPolicyサーバが通知を受信します。これは、フラグが指定されたときにファイルシステムによって使用されます `FILE_DELETE_ON_CLOSE`。 • `open-with-write-intent`書き込み目的でのオープン操作を要求するクライアント要求をフィルタリングするオプション。 このフィルタを設定すると、書き込むためにファイルを開こうとした場合にのみFPolicyサーバが通知を受信します。 • `write-with-size-change`書き込みと同時にサイズの変更を要求するクライアント要求をフィルタリングするオプション。 • `setattr-with-owner-change`ファイルまたはディレクトリの所有者を変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-group-change`ファイルまたはディレクトリのグループを変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-sacl-change`ファイルまたはディレクトリのSACLを変更するクライアント属性設定要求をフィルタリングします。	`-filters` `filter`はい。

2606 このフィルタは、SMBプロトコルとNFSv4プロトコルでのみ使用できます。

は、ボリューム処理が必要です _ ボリュームのマウントおよびアンマウント操作に対して監視が必要かどうかを指定します。デフォルトはです `false`。	`-volume-operation{true`
`false`} `-filters` `filter`はい。	*FPolicy*アクセスが通知を拒否しました ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。これらの通知は、セキュリティ、ランサムウェア対策、ガバナンスに役立ちます。権限不足でファイル処理が失敗した場合、次のメッセージを含む通知が生成されます。 • Failures due to NTFS permissions. • Failures due to Unix mode bits. • Failures due to NFSv4 ACLs.
`-monitor-fileop-failure{true`	`false`}

SMB用のONTAP FPolicyモニタリングでサポートされるファイル操作とフィルタの組み合わせ

ィルタリングするオプション。

FPolicyイベントを設定する場合、SMBのファイルアクセス操作の監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることに注意する必要があります。

このフィルタを指定すると、ほかの操作は監視されません。

次の表に、FPolicyによるSMBファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
閉じる	monitor-ads、offline-bit、close-with-modification、close-with-modification、close-with-read、exclude-directory
作成	モニター広告、オフラインビット
create_dir	現在、このファイル処理でサポートされるフィルタはありません。
delete	モニター広告、オフラインビット

delete_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の取得	オフラインビット、exclude-dir
オープン	monitor-ads、offline-bit、open-with-delete-intent、open-with-write-intent、exclude-dir
読み取り	モニター広告、オフラインビット、初回読み取り
書き込み	monitor-ads、offline-bit、first-write、write-with-size-change
rename	モニター広告、オフラインビット
rename_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の設定	monitor-ads、offline-bit、setattr_with_owner_change、setattr_with_group_change、setattr_with_sacl_change、setattr_with_modify_time_change、setattr_with_access_time_change、setattr_with_creation_time_change、setattr_with_exclude、

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。以下の表に、FPolicyによるSMBファイル アクセス イベントの監視でアクセス拒否時にサポートされるファイル処理とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
オープン	NA

ONTAP FPolicyが**NFSv3**で監視するサポートされているファイル操作とフィルタの組み合わせ

FPolicyイベントを設定する場合、NFSv3のファイルアクセス操作の監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることに注意する必要があります。

次の表に、FPolicyによるNFSv3ファイルアクセスイベントの監視でサポートされるファイル処理とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
作成	オフラインビット
create_dir	現在、このファイル処理でサポートされるフィルタはありません。

delete	オフラインビット
delete_dir	現在、このファイル処理でサポートされるフィルタはありません。
リンク	オフラインビット
検索	オフラインビット、exclude-dir
読み取り	オフラインビット、初回読み取り
書き込み	オフラインビット、first-write、write-with-size-change
rename	オフラインビット
rename_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の設定	オフラインビット、setattr_with_owner_change、setattr_with_group_change、setattr_with_mode_change、setattr_with_modify_time_change、setattr_with_access_time_change、setattr_with_size_change、exclude_directory
シンボリックリンク	オフラインビット

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるNFSv3ファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル処理とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
アクセス	NA
作成	NA
create_dir	NA
delete	NA
delete_dir	NA
リンク	NA
読み取り	NA

rename	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

ONTAP FPolicyが**NFSv4**で監視するサポートされているファイル操作とフィルタの組み合わせ

FPolicyイベントを設定する際には、NFSv4のファイル アクセス処理の監視では特定のファイル処理とフィルタの組み合わせだけがサポートされることを考慮する必要があります。

ONTAP 9 .15.1以降では、FPolicyはNFSv4.1プロトコルをサポートしています。

次の表に、FPolicyによるNFSv4またはNFSv4.1のファイルアクセスイベントの監視でサポートされるファイル処理とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
閉じる	オフラインビット、exclude-directory
作成	オフラインビット
create_dir	現在、このファイル処理でサポートされるフィルタはありません。
delete	オフラインビット
delete_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の取得	オフラインビット、exclude-directory
リンク	オフラインビット
検索	オフラインビット、exclude-directory
オープン	オフラインビット、exclude-directory
読み取り	オフラインビット、初回読み取り
書き込み	オフラインビット、first-write、write-with-size-change

rename	オフラインビット
rename_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の設定	オフラインビット、setattr_with_owner_change、setattr_with_group_change、setattr_with_mode_change、setattr_with_sacl_change、setattr_with_modify_time_change、setattr_with_access_time_change、setattr_with_size_change、exclude_directory
シンボリックリンク	オフラインビット

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。以下の表に、FPolicyによるNFSv4またはNFSv4.1ファイル アクセス イベントの監視でアクセス拒否時にサポートされるファイル処理とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
アクセス	NA
作成	NA
create_dir	NA
delete	NA
delete_dir	NA
リンク	NA
オープン	NA
読み取り	NA
rename	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

ONTAP FPolicyイベント設定ワークシートを完成させる

このワークシートを使用して、FPolicyイベントの設定プロセス中に必要となる値を記録

できます。パラメータ値が必須の場合は、FPolicyイベントを設定する前に、それらのパラメータに使用する値を決定する必要があります。

FPolicyイベントの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報の種類	必須	含める	自分の価値観
Storage Virtual Machine（SVM）名	○	○	
イベント名	○	○	
プロトコル	いいえ		
ファイルソウサ	いいえ		
フィルタ	いいえ		
ボリューム操作	いいえ		
アクセス拒否イベント+（ONTAP 9.13以降のサポート）	いいえ		

FPolicyポリシーの設定を計画する

ONTAP FPolicyポリシー設定について学ぶ

FPolicyポリシーを設定する前に、ポリシーの作成時に必要なパラメータと、特定のオプションパラメータを設定する理由を理解しておく必要があります。この情報は、各パラメータに設定する値を決定するのに役立ちます。

FPolicyポリシーを作成するときは、このポリシーを次のように関連付けます。

- Storage Virtual Machine（SVM）
- 1つ以上のFPolicyイベント
- FPolicy外部エンジン

いくつかのオプションのポリシー設定を構成することもできます。

FPolicyポリシーの設定内容

FPolicyポリシーの必須パラメータとオプションパラメータを次に示します。これは、設定を計画するのに役立ちます。

情報の種類	オプション	必須	デフォルト

SVM 名 _ FPolicyポリシーを作成するSVMの名前を指定します。	`-vserver vserver_name`	○	なし
_ ポリシー名 _ FPolicyポリシーの名前を指定します。 名前の最大文字数は256文字です。 MetroClusterまたはSVMディザスタリカバリ設定でポリシーを設定する場合、この名前は最大200文字にする必要があります。 名前には、次のASCII文字の任意の組み合わせを含めることができます。 • a`から `z • A`から `Z • 0`から `9 • “_”、“.”-", and "	`-policy-name policy_name`	○	なし
_ イベント名 _ FPolicyポリシーに関連付けるイベントをカンマで区切って指定します。 • 1つのポリシーに複数のイベントを関連付けることができます。 • イベントはプロトコルに固有です。 • 1つのポリシーで複数のプロトコルのファイル アクセス イベントを監視するには、ポリシーで監視する各プロトコルのイベントを作成し、それらのイベントをポリシーに関連付けます。 • 既存のイベントを指定する必要があります。	`-events `event_name`はい。`	○	なし

永続ストア ONTAP 9 .14.1以降では、このパラメータは、SVM内の非同期（必須ではない）ポリシーのファイルアクセスイベントをキャプチャする永続ストアを指定します。	`-persistent -store persistent_store_name`	いいえ	なし
_ 外部エンジン名 _ FPolicyポリシーに関連付ける外部エンジンの名前を指定します。 • 外部エンジンには、ノードからFPolicyサーバに通知を送信するために必要な情報が格納されています。 • 単純なファイルブロッキングを行うためにONTAPの標準の外部エンジンを使用したり、より高度なファイルブロッキングとファイル管理を行うために外部FPolicyサーバ（FPolicyサーバ）を使用するように設定された外部エンジンを使用したりするようにFPolicyを設定できます。 • 標準の外部エンジンを使用する場合は、このパラメータの値を指定しないか、値としてを指定できます `native`。 • FPolicyサーバを使用する場合は、外部エンジンの設定がすでに存在している必要があります。	`-engine engine_name`	○（ポリシーで内部のONTAP標準エンジンを使用しない場合）	`native`
_ は必須のスクリーニングです _ 必須のファイルアクセススクリーニングを要求するかどうかを指定します。 • この必須スクリーニング設定は、プライマリサーバとセカンダリサーバがすべて停止した場合や、指定した時間内にFPolicyサーバからの応答を得られない場合に、ファイルアクセスイベントをどのように処理するかを決定します。 • に設定する `true`と、ファイルアクセスイベントが拒否されます。 • に設定する `false`と、ファイルアクセスイベントが許可されます。	`-is-mandatory {true`	`false}`	いいえ

true	権限付きアクセスを許可する _ 権限付きデータ接続を使用した監視対象のファイルやフォルダに対する権限付きアクセスをFPolicyサーバに許可するかどうかを指定します。 設定されている場合、FPolicyサーバは権限付きデータ接続を使用して、監視対象データが格納されているSVMのルートにあるファイルにアクセスできます。 権限付きデータアクセスの場合は、クラスタでSMBのライセンスが有効になっている必要があり、FPolicyサーバへの接続に使用されるすべてのデータLIFが、許可されているプロトコルの1つとして設定されている必要があり`cifs`ます。 ポリシーで権限付きアクセスを許可する場合は、FPolicyサーバで権限付きアクセスに使用するアカウントのユーザ名も指定する必要があります。	-allow -privileged -access{yes	no}

×（パススルーリードが有効になっていない場合）	no	_ 特権ユーザ名 _ FPolicyサーバが権限付きデータアクセスに使用するアカウントのユーザ名を指定します。 • このパラメータの値は、「ドメイン \ ユーザ名」の形式にする必要があります。 • がに設定されて no`いる場合 `-allow-privileged-access、このパラメータに設定されている値は無視されます。	-privileged-user-name user_name

×（権限付きアクセスが有効になっていない場合）	なし	_allow passthrough-read _ FPolicyサーバによってセカンダリストレージ（オフラインファイル）にアーカイブされたファイルに対して、FPolicyサーバがパススルーリードサービスを提供できるかどうかを指定します。 • パススルーリードは、オフラインファイルのデータをプライマリストレージにリストアすることなく読み取る方法です。 パススルーリードでは、読み取り要求に応答する前にファイルをプライマリストレージにリコールする必要がないため、応答レイテンシが短縮されます。さらに、パススルーリードでは、読み取り要求を満たすためだけにリコールされるファイルによってプライマリストレージスペースを消費する必要がなくなるため、ストレージ効率が最適化されます。 • 有効にすると、FPolicyサーバはパススルーリード専用に開かれた別の権限付きデータチャネルを介してファイルのデータを提供します。 パススルーリー	`-is-passthrough-read-enabled {true`

FPolicyポリシーがネイティブエンジンを使用する場合の**ONTAP FPolicy**スコープ設定の要件

標準のエンジンを使用するように FPolicy ポリシーを設定する場合には、ポリシーで設定される FPolicy スコープの定義方法に関して特定の要件があります。

FPolicy スコープは、 FPolicy 環境で指定されたボリュームや共有など、FPolicyポリシーが適用される範囲の境界を定義します。FPolicy ポリシーが適用されるスコープをさらに制限するためのパラメータが多数あります。これらのパラメータの1つで、 `-is-file-extension-check-on-directories-enabled`ディレクトリのファイル拡張子をチェックするかどうかを指定します。デフォルト値はで `false`、ディレクトリ上のファイル拡張子はチェックされません。

標準のエンジンを使用するFPolicyポリシーが共有またはボリュームで有効になっている場合、 `-is-file-extension-check-on-directories-enabled`ポリシーのスコープでパラメータがに設定されている `false`と、ディレクトリへのアクセスが拒否されます。この設定では、ディレクトリのファイル拡張子はチェックされないため、ポリシーのスコープに該当するディレクトリ操作はすべて拒否されます。

標準のエンジンを使用している場合にディレクトリへのアクセスを成功させるには、スコープの作成時にをに `true`設定する必要があり `-is-file-extension-check-on-directories-enabled parameter`ます。

このパラメータをに設定する `true`と、ディレクトリ操作に対して拡張子のチェックが実行され、アクセスを許可するか拒否するかは、FPolicyスコープ設定に含まれている拡張子または除外されている拡張子に基づいて決定されます。

ONTAP FPolicyポリシーワークシートを完成させる

このワークシートを使用して、FPolicyポリシーの設定プロセス中に必要となる値を記録できます。FPolicyポリシーの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報の種類	含める	自分の価値観
Storage Virtual Machine（SVM）名	○	
ポリシー名	○	
イベント名	○	
永続的ストア		
外部エンジン名		
スクリーニングを必須にするかどうか		
特権アクセスを許可するかどうか		
特権ユーザの名前		
パススルー リードが有効かどうか		

FPolicyスコープの設定を計画する

ONTAP FPolicyスコープ設定について学ぶ

FPolicyスコープを設定する前に、スコープを作成することの意味を理解しておく必要があります。スコープ構成に含まれる内容を理解しておく必要があります。また、スコープの優先規則についても理解しておく必要があります。この情報は、設定する値を計画するのに役立ちます。

FPolicyスコープを作成することの意味

FPolicyスコープを作成することは、FPolicyポリシーが適用される範囲を定義することを意味します。Storage Virtual Machine（SVM）は基本の適用範囲です。FPolicyポリシーのスコープを作成するときは、スコープが適用されるFPolicyポリシーを定義する必要があり、さらにスコープを適用するSVMを指定する必要があります。

指定したSVM内にスコープをさらに制限するためのパラメータが多数あります。スコープに含めるものを指定するか、スコープから除外するものを指定することで、スコープを制限できます。有効なポリシーにスコープを適用すると、ポリシーイベントのチェックがこのコマンドで定義したスコープに適用されます。

「 include 」オプションで一致するファイルアクセスイベントが見つかった場合に、通知が生成されます。「 EXCLUDE 」オプションで一致するファイルアクセスイベントについては、通知は生成されません。

FPolicyスコープの設定では、次の設定情報を定義します。

- SVM名
- ポリシー名
- 監視対象に含める共有または監視対象から除外する共有
- 監視対象に含めるまたは監視対象から除外するエクスポートポリシー
- 監視対象に含めるまたは監視対象から除外するボリューム
- 監視対象に含めるまたは監視対象から除外するファイル拡張子
- ディレクトリオブジェクトに対するファイル拡張子のチェックを実行するかどうか

> クラスタのFPolicyポリシーのスコープには、特別な考慮事項があります。クラスタのFPolicyポリシーは、クラスタ管理者が管理SVM用に作成するポリシーです。クラスタ管理者がそのクラスタのFPolicyポリシーのスコープも作成する場合、SVM管理者はその同じポリシーのスコープを作成することはできません。ただし、クラスタ管理者がクラスタのFPolicyポリシーのスコープを作成しない場合は、すべてのSVM管理者がそのクラスタポリシーのスコープを作成できます。SVM管理者がそのクラスタのFPolicyポリシーのスコープを作成した場合、クラスタ管理者はそれ以降その同じクラスタポリシーのクラスタスコープを作成することはできません。これは、クラスタ管理者が同じクラスタポリシーのスコープを上書きできないためです。

スコープの優先規則とは

スコープ設定には、次の優先規則が適用されます。

- 共有をパラメータに指定し、共有の親ボリュームをパラメータに `-volumes-to-exclude`指定した `-volumes-to-exclude`場合 `-shares-to-include`は、がよりも優先されます `-shares-to-`

include。

- エクスポートポリシーをパラメータに指定し、エクスポートポリシーの親ボリュームをパラメータに指定した -volumes-to-exclude`場合 `-export-policies-to-include`は、が `-volumes-to-exclude`よりも優先されます `-export-policies-to-include。
- 管理者はリストと -file-extensions-to-exclude`リストの両方を指定できます `-file-extensions-to-include。

> `-file-extensions-to-exclude`パラメータは、パラメータがチェックされる前にチェックされ `-file-extensions-to-include`ます。

FPolicyスコープの構成要素

次に示す使用可能なFPolicyスコープ設定パラメータの一覧は、設定を計画するのに役立ちます。

> スコープに含めるか除外する共有、エクスポートポリシー、ボリューム、およびファイル拡張子を設定する際に、includeパラメータとexcludeパラメータにメタ文字（「*」など）を含めることができます?" and "。正規表現の使用はサポートされていません。

情報の種類	オプション
SVM FPolicyスコープを作成するSVMの名前を指定します。 各FPolicy設定は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。	-vserver vserver_name
_ ポリシー名 _ スコープを関連付けるFPolicyポリシーの名前を指定します。FPolicyポリシーがすでに存在している必要があります。	-policy-name policy_name
含める共有 _ カンマで区切って複数の共有を指定し、FPolicyポリシーの監視対象となるスコープに含めます。	-shares-to-include `share_name`はい。
_ 除外する共有 _ カンマで区切って複数の共有を指定し、FPolicyポリシーの監視対象となるスコープから除外します。	-shares-to-exclude `share_name`はい。
対象に含めるボリューム： FPolicy ポリシーの監視対象となるボリュームをカンマで区切って指定します。	-volumes-to-include `volume_name`はい。

除外するボリューム _ カンマで区切って複数のボリュームを指定し、FPolicyポリシーの監視対象となるスコープから除外します。	`-volumes-to-exclude` `volume_name`はい。
ポリシーを含めるには _ をエクスポートします カンマで区切って複数のエクスポートポリシーを指定し、FPolicyポリシーの監視対象となるスコープに含めます。	`-export-policies-to-include` `export_policy_name`はい。
ポリシーを exclude_ にエクスポートします カンマで区切って複数のエクスポートポリシーを指定し、FPolicyポリシーの監視対象となるスコープから除外します。	`-export-policies-to-exclude` `export_policy_name`はい。
_include するファイル拡張子 _ カンマで区切って複数のファイル拡張子を指定し、FPolicyポリシーの監視対象となるスコープに含めます。	`-file-extensions-to-include` `file_extensions`はい。
_ ファイル拡張子を exclude_ に設定します カンマで区切って複数のファイル拡張子を指定し、FPolicyポリシーの監視対象となるスコープから除外します。	`-file-extensions-to-exclude` `file_extensions`はい。
_ ディレクトリのファイル拡張子チェックは有効になっていますか？ _ ファイル名の拡張子の監視をディレクトリオブジェクトにも適用するかどうかを指定します。このパラメータをに設定 `true`すると、通常のファイルと同じ拡張子チェックがディレクトリオブジェクトに適用されます。このパラメータをに設定する `false`と、ディレクトリ名の拡張子は照合されず、名前の拡張子が一致しなくてもディレクトリに関する通知が送信されます。 スコープの割り当て先のFPolicyポリシーが標準のエンジンを使用するように設定されている場合は、このパラメータをに設定する必要があります `true`。	`-is-file-extension-check-on-directories-enabled{true`
	`false}`

ONTAP FPolicyスコープワークシートを完成させる

このワークシートを使用して、FPolicyスコープの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、FPolicyスコープを設定する前に、それらのパラメータに使用する値を決定する必要があります。

FPolicyスコープの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報の種類	必須	含める	自分の価値観
Storage Virtual Machine（SVM）名	○	○	
ポリシー名	○	○	
対象に含める共有	いいえ		
共有を除外する	いいえ		
対象に含めるボリューム	いいえ		
ボリュームを除外する	いいえ		
エクスポートポリシーを含める	いいえ		
対象から除外するエクスポートポリシー	いいえ		
対象に含めるファイル拡張子	いいえ		
対象から除外するファイル拡張子	いいえ		
ディレクトリのファイル拡張子の監視が有効かどうか	いいえ		

FPolicy設定の作成

ONTAP FPolicy外部エンジンを作成する

FPolicy設定の作成を開始するには、外部エンジンを作成する必要があります。外部エンジンは、FPolicyが外部FPolicyサーバへの接続を確立および管理する方法を定義します。内部のONTAPエンジン（標準の外部エンジン）を単純なファイルブロッキングに使用している設定の場合は、FPolicy外部エンジンを別途設定する必要はなく、この手順を実行する必要もありません。

開始する前に

"外部エンジン"ワークシートを完成させる必要があります。

タスクの内容

外部エンジンがMetroCluster設定で使用されている場合は、ソースサイトでFPolicyサーバのIPアドレスをプライマリサーバとして指定する必要があります。デスティネーションサイトのFPolicyサーバのIPアドレスは、セカンダリサーバとして指定する必要があります。

手順

1. コマンドを使用してFPolicy外部エンジンを作成し `vserver fpolicy policy external-engine create`ます。

次のコマンドは、Storage Virtual Machine（SVM）vs1.example.com上に外部エンジンを作成します。FPolicyサーバとの外部通信に認証は必要ありません。

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
no-auth
```

2. コマンドを使用してFPolicy外部エンジンの設定を確認します `vserver fpolicy policy external-engine show`。

   次のコマンドは、SVM vs1.example.comで設定されているすべての外部エンジンに関する情報を表示します。

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                  Primary        Secondary
   External
   Vserver             Engine     Servers        Servers       Port Engine
   Type
   ---------------     ---------- -------------- ----------- ------
   -----------
   vs1.example.com     engine1    10.1.1.2,      -             6789
   synchronous
                                  10.1.1.3
   ```

   次のコマンドは、 SVM vs1.example.com 上の「 engine1 」という外部エンジンに関する詳細情報を表示します。

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

   ```
                               Vserver: vs1.example.com
                                Engine: engine1
                  Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
           Port Number of FPolicy Service: 6789
                Secondary FPolicy Servers: -
                    External Engine Type: synchronous
   SSL Option for External Communication: no-auth
              FQDN or Custom Common Name: -
             Serial Number of Certificate: -
                   Certificate Authority: -
   ```

ONTAP FPolicyイベントを作成する

FPolicyポリシーの設定を作成する手順の一環として、FPolicyイベントを作成する必要があります。FPolicyポリシーの作成時にイベントを関連付けます。イベントは、監視する

プロトコルと、監視およびフィルタリングするファイルアクセスイベントを定義します。

開始する前に

FPolicyイベントを完了する必要があります"ワークシート"。

FPolicyイベントの作成

1. コマンドを使用してFPolicyイベントを作成し `vserver fpolicy policy event create`ます。

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. コマンドを使用してFPolicyイベントの設定を確認します `vserver fpolicy policy event show`。

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                       Event                File                       Is Volume
   Vserver             Name       Protocols Operations    Filters    Operation
   ----------------    ---------- --------- ------------- ---------
   ------------
   vs1.example.com     event1     cifs      open, close,  -          false
                                            read, write
   ```

FPolicyアクセス拒否イベントを作成する

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。これらの通知は、セキュリティ、ランサムウェア対策、ガバナンスに役立ちます。

1. コマンドを使用してFPolicyイベントを作成し `vserver fpolicy policy event create`ます。

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -monitor-fileop-failure true -file-operations open
   ```

ONTAP FPolicy永続ストアを作成する

永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。14.1以降では、ONTAP 9の必須ではない非同期ポリシーのファイルアクセスイベントをキャプチャするようにを設定でき"永続的ストア"ます。同期（必須または非必須）および非同期の必須構成はサポートされていません。

ONTAP 9 .15.1以降では、FPolicyの永続的ストアの設定が簡素化されています。 `persistent-store create`コマンドは、SVM用のボリュームの作成を自動化し、永続的ストア用のボリュームを設定します。

永続ストアを作成するには、ONTAPのリリースに応じて次の2つの方法があります。

- ONTAP 9.15.1以降：永続ストアを作成すると、ONTAPでボリュームが自動的に作成されて設定されます。これにより、FPolicyの永続的ストアの設定が簡素化され、すべてのベストプラクティスが実装されま

す。

- ONTAP 9.14.1：ボリュームを手動で作成して設定し、新しく作成したボリューム用の永続的ストアを作成します。

各SVMに設定できる永続的ストアは1つだけです。ポリシーが別 々 のパートナーのものであっても、この単一の永続的ストアをそのSVM上のすべてのFPolicy設定に使用する必要があります。

永続ストアの作成（**ONTAP 9 .15.1**以降）

開始する前に

- 永続的ストアを作成するSVMには、アグリゲートが少なくとも1つ必要です。
- SVMで使用可能なアグリゲートへのアクセスと、ボリュームを作成するための十分な権限が必要です。

手順

1. 永続的ストアを作成します。これにより、ボリュームが自動的に作成および設定されます。

   ```
   vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
   <name> -volume <volume_name> -size <size> -autosize-mode
   <off|grow|grow_shrink>
   ```

   - `vserver`パラメータは、SVMの名前です。
   - `persistent-store`パラメータは、永続ストアの名前です。
   - `volume`パラメータは、永続的ストアボリュームの名前です。

     既存の空のボリュームを使用する場合は、コマンドを使用してボリューム `volume show`を検索し、volumeパラメータで指定します。

   - この `size`パラメータは、外部サーバ（パートナーアプリケーション）に配信されないイベントを保持する期間に基づいています。

     たとえば、1秒あたり30Kの通知があるクラスタで30分間のイベントを維持する場合は、次のコマンドを実行します。

     必要なボリュームサイズ= 30000 x 30 x 60 x 0.6KB（通知レコードの平均サイズ）= 32400000 KB =~32GB

     おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに問い合わせるか、FPolicyカウンタを使用します `requests_dispatched_rate`。

     既存のボリュームを使用する場合、sizeパラメータはオプションです。sizeパラメータに値を指定すると、指定したサイズに一致するボリュームが変更されます。

   - パラメータは `autosize-mode`、ボリュームのオートサイズモードを指定します。サポートされるオートサイズモードは次のとおりです。
     - off -使用済みスペースの量に応じてボリュームのサイズが拡張または縮小されません。
     - grow -ボリュームの使用済みスペースが拡張しきい値を超えると、ボリュームは自動的に拡張されます。

- grow_shrink -使用済みスペースの量に応じてボリュームのサイズが拡張または縮小されます。

2. FPolicyポリシーを作成し、そのポリシーに永続ストア名を追加します。詳細については、を参照してください "FPolicyポリシーを作成する"。

永続ストアの作成（**ONTAP 9 .14.1**）

ボリュームを作成し、そのボリュームを使用する永続的ストアを作成できます。作成したボリュームを外部ユーザプロトコルアクセス（CIFS / NFS）からブロックできます。

手順

1. 永続ストア用にプロビジョニング可能な空のボリュームをSVMに作成します。

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

十分なRBAC Privileges（ボリュームの作成）を持つ管理者ユーザは、必要なサイズのボリュームを（volume CLIコマンドまたはREST APIを使用して）作成し、永続的ストアのcreate CLIコマンドまたはREST APIでとしてボリュームの名前を指定する必要があります `-volume`。

- `vserver`パラメータは、SVMの名前です。
- `volume`パラメータは、永続的ストアボリュームの名前です。
- ボリュームを使用できるようにするには、 `state`パラメータをonlineに設定する必要があります。
- `policy`FPolicyサービスポリシーをすでに設定している場合、パラメータはに設定されます。そうでない場合は、あとでコマンドを使用してポリシーを追加できます `volume modify`。
- `unix-permissions`パラメータはオプションです。
- この `size`パラメータは、外部サーバ（パートナーアプリケーション）に配信されないイベントを保持する期間に基づいています。

  たとえば、1秒あたり30Kの通知があるクラスタで30分間のイベントを維持する場合は、次のコマンドを実行します。

  必要なボリュームサイズ= 30000 x 30 x 60 x 0.6KB（通知レコードの平均サイズ）= 32400000 KB =~32GB

おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに問い合わせるか、FPolicyカウンタを使用します `requests_dispatched_rate`。

- FlexVolボリュームの場合はaggregateパラメータが必要です。それ以外の場合は必須ではありません。
- `snapshot-policy`パラメータはnoneに設定する必要があります。これにより、スナップショットが誤ってリストアされて現在のイベントが失われることがなくなり、イベント処理の重複を防ぐことができます。

  既存の空のボリュームを使用する場合は、コマンドを使用してボリュームを検索し、コマンドを使用し `volume show`て必要な変更を行います。 `volume modify`永続ストアのポリシー、サイズ、およびパラメータが正しく設定されていることを確認します `snapshot-policy`。

2. 永続ストアを作成します。

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

   - `vserver`パラメータは、SVMの名前です。
   - `persistent-store`パラメータは、永続ストアの名前です。
   - `volume`パラメータは、永続的ストアボリュームの名前です。

3. FPolicyポリシーを作成し、そのポリシーに永続ストア名を追加します。詳細については、を参照してください "FPolicyポリシーを作成する"。

ONTAP FPolicyポリシーを作成する

FPolicyポリシーを作成するときは、外部エンジンと1つ以上のイベントをポリシーに関連付けます。また、このポリシーでは、必須のスクリーニングが必要かどうか、FPolicyサーバにStorage Virtual Machine（SVM）上のデータへの権限付きアクセスが許可されているかどうか、オフラインファイルのパススルーリードが有効かどうかを指定します。

開始する前に

- FPolicyポリシーワークシートを完成させる必要があります。
- FPolicyサーバを使用するようにポリシーを設定する場合は、外部エンジンが存在している必要があります。
- FPolicyポリシーに関連付けるFPolicyイベントが少なくとも1つ存在している必要があります。
- 権限付きデータアクセスを設定する場合は、SVM上にSMBサーバが存在している必要があります。
- ポリシーの永続ストアを設定するには、エンジンタイプを* async にし、ポリシーを non-mandatory *にする必要があります。

  詳細については、を参照してください "永続ストアの作成"。

手順

1. FPolicyポリシーを作成します。

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

   - FPolicy ポリシーには 1 つ以上のイベントを追加できます。
   - デフォルトでは、必須のスクリーニングが有効になっています。
   - パラメータをに `yes`設定して権限付きアクセスを許可する場合 `-allow-privileged-access`は、権限付きアクセスの権限付きユーザ名も設定する必要があります。
   - パラメータをに `true`設定してパススルーリードを設定する場合 `-is-passthrough-read-enabled`は、権限付きデータアクセスも設定する必要があります。

次のコマンドは、 "event1" というイベントと、 "engine1" という外部エンジンが関連付けられた "policy1 " という名前のポリシーを作成します。このポリシーでは、ポリシー設定にデフォルト値を使用します。
`vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

次のコマンドは、 "event2`" というイベントと、 "engine2`" という外部エンジンが関連付けられた "policy2`" というポリシーを作成します。このポリシーは、指定したユーザ名を使用して権限付きアクセスを使用するように設定されています。パススルーリードが有効になっている場合：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

次のコマンドは ' event3` というイベントが関連付けられた '' native1` という名前のポリシーを作成しますこのポリシーでは標準のエンジンを使用し、デフォルト値をポリシー設定に使用します。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. コマンドを使用してFPolicyポリシーの設定を確認します `vserver fpolicy policy show`。

   次のコマンドは、次の情報を含む、設定された3つのFPolicyポリシーに関する情報を表示します。

   - ポリシーに関連付けられている SVM
   - ポリシーに関連付けられている外部エンジン
   - ポリシーに関連付けられているイベント
   - スクリーニングを必須にするかどうか
   - 権限付きアクセスが必要かどうか
     `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

ONTAP FPolicyスコープを作成する

FPolicy ポリシーを作成したら、 FPolicy スコープを作成する必要があります。スコープを作成するときに、スコープを FPolicy ポリシーに関連付けます。スコープは、FPolicy ポリシーが適用される範囲を定義します。共有、エクスポートポリシー、ボリューム、およびファイル拡張子に基づいて、対象とするファイルまたは除外するファイルを指定できます。

開始する前に

FPolicy スコープワークシートを完成させる必要があります。FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があり（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、 FPolicy イベントを少なくとも 1 つは関連付ける必要があります。

手順

1. コマンドを使用してFPolicyスコープを作成し `vserver fpolicy policy scope create`ます。

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
policy1 -volumes-to-include datavol1,datavol2
```

2. コマンドを使用してFPolicyスコープの設定を確認します `vserver fpolicy policy scope show`。

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
 Export Policies to Include: -
 Export Policies to Exclude: -
 File Extensions to Include: -
 File Extensions to Exclude: -
```

ONTAP FPolicyポリシーを有効にする

FPolicy ポリシーの設定が完了したら、 FPolicy ポリシーを有効にします。ポリシーを有効にすると、優先度が設定され、ポリシーのファイルアクセスの監視が開始されます。

開始する前に

FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があり（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、 FPolicy イベントを少なくとも 1 つは関連付ける必要があります。FPolicy ポリシースコープが存在し、 FPolicy ポリシーに割り当てられている必要があります。

タスクの内容

Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。

管理 SVM ではポリシーを有効にできません。

手順

1. コマンドを使用して、FPolicyポリシーを有効にし `vserver fpolicy enable`ます。

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. コマンドを使用して、FPolicyポリシーが有効になっていることを確認します `vserver fpolicy show`。

```
vserver fpolicy show -vserver vs1.example.com
```

```
                                   Sequence
Vserver           Policy Name        Number  Status   Engine
---------------  ----------------- --------  -------- ---------
vs1.example.com  policy1                  1  on       engine1
```

FPolicy設定を管理します。

FPolicyの設定変更

ONTAP で FPolicy 設定を変更するコマンド

FPolicyの設定を変更するには、設定を構成する要素を変更します。外部エンジン、FPolicyイベント、FPolicyスコープ、FPolicy永続ストア、およびFPolicyポリシーを変更できます。FPolicyポリシーを有効または無効にすることもできます。FPolicyポリシーを無効にすると、そのポリシーのファイル監視が中止されます。

設定を変更する前に、FPolicyポリシーを無効にする必要があります。

変更する項目	使用するコマンド
外部エンジン	`vserver fpolicy policy external-engine modify`
イベント	`vserver fpolicy policy event modify`
スコープ	`vserver fpolicy policy scope modify`
永続的ストア	`vserver fpolicy persistent-store modify`
ポリシー	`vserver fpolicy policy modify`

の詳細については `vserver fpolicy policy`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP FPolicyポリシーを有効または無効にする

設定の完了後にFPolicyポリシーを有効にできます。ポリシーを有効にすると、優先度が設定され、ポリシーのファイルアクセスの監視が開始されます。ポリシーのファイルアクセスの監視を停止するには、FPolicyポリシーを無効にします。

開始する前に

FPolicyポリシーを有効にする前に、FPolicyの設定を完了しておく必要があります。

タスクの内容

- Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。
- 標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。
- FPolicyポリシーの優先度を変更する場合は、ポリシーを無効にしてから、新しいシーケンス番号を使用して再度有効にする必要があります。

ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
FPolicyポリシーを有効にする	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
FPolicyポリシーを無効にする	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

FPolicy設定に関する情報を表示する

ONTAP FPolicyのshowコマンドについて学ぶ

コマンドの仕組みを理解しておくと、FPolicyの設定に関する情報を表示するときに役立ち `show`ます。

パラメータを追加せずにコマンドを実行すると、 `show`情報が要約形式で表示されます。また `show`、各コマンドには、同じ2つのオプションパラメータ、およびが `-fields`あり `-instance`ます。

コマンドでパラメータを `show`使用する `-instance`と、コマンド出力には詳細情報がリスト形式で表示されます。場合によっては、詳細な出力に時間がかかり、必要以上の情報が含まれることがあります。パラメータを使用すると、指定したフィールドの情報のみが表示されるように出力をカスタマイズできます `-fields fieldname[,fieldname…]`。指定できるフィールドを特定するには、パラメータのあと `-fields`にと入力します `?`。

パラメータを指定したコマンドの `-fields`出力には `show`、要求したフィールドに関連する他の関連フィールドや必要なフィールドが表示される場合があります。

すべて `show`のコマンドには、その出力をフィルタリングして、コマンド出力に表示される情報の範囲を絞り込むことができる1つ以上のオプションパラメータがあります。コマンドで使用可能なオプションパラメータを確認するには、コマンドのあとに `show`と入力し `?`ます。

`show`コマンドでは、UNIX形式のパターンおよびワイルドカードがサポートされ、コマンドパラメータ引数の複数の値を照合できます。たとえば、ワイルドカード演算子（ * ）、 NOT 演算子（ ! ）、 OR 演算子（ | ）、範囲演算子（ integer...integer ）、 less-than 演算子（ < ）、 greater-than 演算子（ > ）、 less-than-or-equal-to 演算子（ \<= ）、 greater-than-or-equal-to 演算子（ >= ）を指定する場合に使用できます。

UNIX形式のパターンおよびワイルドカードの使用の詳細については、を参照してくださいONTAPコマンドラインインターフェイスの使用。

ONTAPのFPolicy設定に関する情報を表示するコマンド

FPolicy外部エンジン、イベント、スコープ、およびポリシーに関する情報など、FPolicyの設定に関する情報を表示するには、コマンドを使用し `fpolicy show`ます。

FPolicy に関する情報の表示	使用するコマンド
外部エンジン	`vserver fpolicy policy external-engine show`
イベント	`vserver fpolicy policy event show`
スコープ	`vserver fpolicy policy scope show`
ポリシー	`vserver fpolicy policy show`

の詳細については `vserver fpolicy policy`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP FPolicyポリシーのステータスに関する情報を表示する

FPolicyポリシーのステータスに関する情報を表示して、ポリシーが有効になっているかどうか、使用するように設定されている外部エンジン、ポリシーのシーケンス番号、およびFPolicyポリシーが関連付けられているStorage Virtual Machine（SVM）を確認できます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- ポリシー名
- ポリシーのシーケンス番号
- ポリシーのステータス

クラスタまたは特定のSVMで設定されているFPolicyポリシーのステータスに関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

パラメータを指定すると、リストされているポリシーに関する詳細情報を表示できます `-instance`。また、

パラメータを使用して、指定したフィールドのみをコマンド出力に表示したり、使用できるフィールドを確認したり `-fields ?`することもできます `-fields。

ステップ

1. 適切なコマンドを使用して、FPolicyポリシーのステータスに関する情報をフィルタリングして表示します。

ステータス情報を表示するポリシー	入力するコマンド
クラスタのポリシー	`vserver fpolicy show`
指定したステータスのポリシー	`vserver fpolicy show -status {on
off}`	指定したSVMのポリシー
`vserver fpolicy show -vserver vserver_name`	指定したポリシー名のポリシー
`vserver fpolicy show -policy-name policy_name`	指定した外部エンジンを使用するポリシー

例

次の例は、クラスタのFPolicyポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show
                                        Sequence
Vserver              Policy Name          Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy      -         off         eng1
vs1.example.com      v1p1                -         off         eng2
vs1.example.com      v1p2                -         off         native
vs1.example.com      v1p3                -         off         native
vs1.example.com      cserver_policy      -         off         eng1
vs2.example.com      v1p1                3         on          native
vs2.example.com      v1p2                1         on          eng3
vs2.example.com      cserver_policy      2         on          eng1
```

有効な **ONTAP FPolicy** ポリシーに関する情報を表示します

有効なFPolicyポリシーに関する情報を表示して、使用するように設定されている外部エンジン、ポリシーの優先度、およびFPolicyポリシーが関連付けられているStorage Virtual Machine（SVM）を確認できます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- ポリシー名
- ポリシーの優先度

コマンドパラメータを使用すると、指定した条件でコマンドの出力をフィルタリングできます。

ステップ

1. 適切なコマンドを使用して、有効なFPolicyポリシーに関する情報を表示します。

情報を表示する有効なポリシー	入力するコマンド
クラスタのポリシー	`vserver fpolicy show-enabled`
指定したSVMのポリシー	`vserver fpolicy show-enabled -vserver vserver_name`
指定したポリシー名のポリシー	`vserver fpolicy show-enabled -policy-name policy_name`
指定したシーケンス番号のファイル	`vserver fpolicy show-enabled -priority integer`

例

次の例は、クラスタの有効なFPolicyポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

FPolicyサーバの接続を管理します。

ONTAPでの外部FPolicyサーバへの接続

接続がすでに終了している場合は、ファイル処理を有効にするために、外部FPolicyサーバへの手動接続が必要になることがあります。サーバのタイムアウトに達した後、または何らかのエラーが原因で接続が終了します。または、管理者が接続を手動で終了することもできます。

タスクの内容

致命的なエラーが発生すると、FPolicyサーバへの接続が終了する可能性があります。致命的なエラーの原因となった問題を解決したら、FPolicyサーバに手動で再接続する必要があります。

手順

1. コマンドを使用して外部FPolicyサーバに接続します `vserver fpolicy engine-connect`。

   の詳細については `vserver fpolicy engine-connect`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用して、外部FPolicyサーバが接続されていることを確認します `vserver fpolicy show-engine`。

   の詳細については `vserver fpolicy show-engine`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPテノカイフFPolicyサアハカラノセツソク

外部FPolicyサーバからの手動での切断が必要になる場合があります。これは、FPolicyサーバで通知要求の処理に関する問題が発生した場合や、FPolicyサーバでメンテナンスを実施する必要がある場合に適しています。

手順

1. コマンドを使用して、外部FPolicyサーバから切断し `vserver fpolicy engine-disconnect`ます。

   の詳細については `vserver fpolicy engine-disconnect`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用して、外部FPolicyサーバが切断されたことを確認します `vserver fpolicy show-engine`。

   の詳細については `vserver fpolicy show-engine`、を"ONTAPコマンド リファレンス"参照してください。

外部の ONTAP FPolicy サーバへの接続に関する情報を表示します

クラスタまたは指定したStorage Virtual Machine（SVM）の外部FPolicyサーバ（FPolicyサーバ）への接続に関するステータス情報を表示できます。この情報は、接続されているFPolicyサーバを確認するのに役立ちます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- ノード名
- FPolicyポリシー名
- FPolicyサーバのIPアドレス
- FPolicyサーバノステータス
- FPolicyサーバのタイプ

クラスタまたは特定のSVMのFPolicy接続に関する情報の表示に加え、コマンドパラメータを使用して、他の

条件によってコマンドの出力をフィルタリングすることができます。

パラメータを指定すると、リストされているポリシーに関する詳細情報を表示できます `-instance`。また、パラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます `-fields`。パラメータのあとに `-fields`と入力すると、使用できるフィールドを確認できます `?`。

ステップ

1. 適切なコマンドを使用して、ノードとFPolicyサーバの間の接続ステータスに関する情報をフィルタリングして表示します。

接続ステータス情報を表示するFPolicy サーバ	入力するコマンド
指定したもの	`vserver fpolicy show-engine -server IP_address`
指定したSVMのもの	`vserver fpolicy show-engine -vserver vserver_name`
指定したポリシーに関連付けられているポリシー	`vserver fpolicy show-engine -policy-name policy_name`
指定したサーバステータスのファイル	`vserver fpolicy show-engine -server-status status` サーバのステータスは、次のいずれかになります。 • `connected` • `disconnected` • `connecting` • `disconnecting`
指定したタイプのファイル	`vserver fpolicy show-engine -server-type type` FPolicyサーバのタイプは次のいずれかになります。 • `primary` • `secondary`

指定した理由で切断されたもの	`vserver fpolicy show-engine -disconnect-reason text` 切断の理由はさまざまです。切断の一般的な理由は次のとおりです。 • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

例

次の例は、SVM vs1.example.com上のFPolicyサーバへの外部エンジン接続に関する情報を表示します。

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver          Policy    Node          Server      status        type
---------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

この例は、接続されているFPolicyサーバに関する情報のみを表示します。

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver          policy-name server
---------- ---------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

ONTAP FPolicyパススルー読み取り接続ステータスに関する情報を表示します

クラスタまたは指定したStorage Virtual Machine（SVM）の外部FPolicyサーバ（FPolicyサーバ）へのFPolicyパススルーリード接続のステータスに関する情報を表示できます。この情報は、パススルーリードデータ接続が確立されているFPolicyサーバや、パススル

ーリード接続が切断されているFPolicyサーバを確認するのに役立ちます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- FPolicyポリシー名
- ノード名
- FPolicyサーバのIPアドレス
- FPolicyパススルーリード接続のステータス

クラスタまたは特定のSVMのFPolicy接続に関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

パラメータを指定すると、リストされているポリシーに関する詳細情報を表示できます `-instance`。また、パラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます `-fields`。パラメータのあとに `-fields`と入力すると、使用できるフィールドを確認できます `?`。

ステップ

1. 適切なコマンドを使用して、ノードとFPolicyサーバの間の接続ステータスに関する情報をフィルタリングして表示します。

表示する接続ステータス情報	入力するコマンド
クラスタのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection`
指定したSVMのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
指定したポリシーのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
指定したポリシーの詳細なFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
指定したステータスのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status`サーバのステータスは、次のいずれかになります。 • `connected` • `disconnected`

例

次のコマンドは、クラスタ上のすべてのFPolicyサーバからのパススルーリード接続に関する情報を表示します。

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------ ----------- ----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

次のコマンドは、「 pol_cifs_1 」ポリシーに設定されている FPolicy サーバからのパススルーリード接続に関する詳細情報を表示します。

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                        Node: FPolicy-01
                                     Vserver: vs1.example.com
                                      Policy: pol_cifs_1
                                      Server: 1.1.1.1
                Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

セキュリティトレースを使用したアクセスの確認

ONTAP セキュリティ トレースの詳細

パーミッショントレーシングフィルタを追加すると、クライアントまたはユーザによるStorage Virtual Machine（SVM）上のSMBサーバおよびNFSサーバに対する処理要求が許可または拒否された理由がONTAPで記録されるようになります。これは、ファイルアクセスのセキュリティ方式が適切であることを確認する場合や、ファイルアクセスに関する問題のトラブルシューティングを行う場合に役立ちます。

セキュリティトレースを使用すると、SVM上でのSMBおよびNFS経由のクライアント処理を検出するフィルタを設定して、そのフィルタに一致するすべてのアクセスチェックをトレースできます。トレース結果には、アクセスが許可または拒否された理由がわかりやすくまとめられています。

SVMのファイルやフォルダに対するSMBアクセスやNFSアクセスのセキュリティ設定を確認する場合や、アクセスに関する問題がある場合は、パーミッショントレーシングを有効にするフィルタをすばやく追加できます。

次のリストに、セキュリティトレースの仕組みに関する重要な特性を示します。

- ONTAP は、セキュリティトレースを SVM レベルで適用します。
- 各受信要求がスクリーニングされ、有効になっているセキュリティトレースのフィルタ条件に一致するかどうかが確認されます。
- トレースは、ファイルとフォルダの両方のアクセス要求に対して実行されます。
- トレースでは、次の条件に基づいてフィルタリングできます。
  - クライアントIP
  - SMB または NFS パス
  - Windows 名
  - UNIX 名
- 要求は、 _allowed_or_Denied_access 応答結果でスクリーニングされます。
- 有効なトレースのフィルタ条件に一致する各要求が、トレース結果ログに記録されます。
- ストレージ管理者は、フィルタが自動的に無効になるようにタイムアウトを設定できます。
- 要求が複数のフィルタに一致する場合は、インデックス番号が最も大きいフィルタの結果が記録されます。
- ストレージ管理者は、トレース結果ログを出力し、アクセス要求が許可または拒否された理由を確認できます。

ONTAP SVMでセキュリティトレースが監視するアクセスチェックの種類

ファイルやフォルダに対するアクセスチェックは、複数の条件に基づいて行われます。これらすべての条件について、セキュリティトレースで処理が監視されます。

セキュリティトレースで監視されるアクセスチェックの種類は次のとおりです。

- ボリュームとqtreeのセキュリティ形式
- 処理が要求されるファイルやフォルダが格納されているファイルシステムの効果的なセキュリティ
- ユーザマッピング
- 共有レベルの権限
- エクスポートレベルの権限
- ファイルレベルの権限
- ストレージレベルのアクセス保護セキュリティ

ONTAP SVM でセキュリティ トレースを作成する際の考慮事項

Storage Virtual Machine（SVM）でセキュリティトレースを作成する場合は、いくつかの考慮事項に注意する必要があります。たとえば、トレースを作成できるプロトコル、サポートされるセキュリティ形式、アクティブなトレースの最大数を把握しておく必要があります。

- セキュリティトレースはSVM上でのみ作成できます。

- セキュリティトレースフィルタの各エントリはSVM固有です。

  トレースを実行するSVMを指定する必要があります。

- SMB要求とNFS要求に対してパーミッショントレーシングフィルタを追加できます。
- トレースフィルタを作成するSVM上にSMBサーバまたはNFSサーバをセットアップする必要があります。
- NTFS、UNIX、mixedセキュリティ形式のボリュームおよびqtree上に存在するファイルやフォルダに対してセキュリティトレースを作成できます。
- パーミッショントレーシングフィルタはSVMごとに10個まで追加できます。
- フィルタを作成または変更するときは、フィルタインデックス番号を指定する必要があります。

  フィルタはインデックス番号順に処理されます。インデックス番号が大きいフィルタの条件は、インデックス番号が小さいフィルタの条件よりも先に処理されます。トレースされる要求が複数の有効なフィルタの条件に一致する場合は、インデックス番号が最も大きいフィルタのみがトリガーされます。

- セキュリティトレースフィルタを作成して有効にしたら、トレースフィルタがキャプチャしてトレース結果ログに記録できるアクティビティを生成するために、クライアントシステムに対してファイル要求またはフォルダ要求を実行する必要があります。
- パーミッショントレーシングフィルタは、ファイルアクセスの検証またはトラブルシューティングの目的でのみ追加してください。

  パーミッショントレーシングフィルタを追加すると、コントローラのパフォーマンスが若干低下します。

  検証やトラブルシューティングが完了したら、すべてのパーミッショントレーシングフィルタを無効にするか削除する必要があります。さらに、ONTAPがログに大量のトレース結果を送信しないように、できるだけ具体的なフィルタ条件を選択する必要があります。

セキュリティトレースの実行

ONTAP セキュリティ トレースの実行方法を学ぶ

セキュリティトレースの実行では、セキュリティトレースフィルタの作成、フィルタ条件の確認、フィルタ条件に一致する SMB クライアントまたは NFS クライアントへのアクセス要求の生成、トレース結果の表示などを行います。

セキュリティフィルタを使用してトレース情報をキャプチャしたあと、フィルタを変更して再利用するか、不要になった場合は無効にすることができます。フィルタトレース結果を表示および分析したあと、その結果が不要になった場合は削除できます。

ONTAP SVMでセキュリティトレースフィルタを作成する

Storage Virtual Machine（SVM）でSMBとNFSのクライアント処理を検出し、フィルタに一致するすべてのアクセスチェックをトレースするセキュリティトレースフィルタを作成できます。セキュリティトレースの結果を使用して、設定の検証やアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

vserver security trace filter createコマンドには、次の2つの必須パラメータがあります。

必須パラメータ	説明
`-vserver vserver_name`	SVM 名 _ セキュリティトレースフィルタを適用するファイルやフォルダが格納されているSVMの名前。
`-index index_number`	フィルタインデックス番号 _ フィルタに適用するインデックス番号。トレースフィルタはSVMごとに10個まで使用できます。このパラメータに指定できる値は1~10です。

オプションのフィルタパラメータをいくつか使用すると、セキュリティトレースのフィルタをカスタマイズして、セキュリティトレースの結果を絞り込むことができます。

フィルタパラメータ	説明
`-client-ip IP_Address`	IPアドレスを指定します。このIPアドレスからSVMにアクセスしているユーザが対象です。
`-path path`	パーミッショントレースフィルタを適用するパスを指定します。の値 `-path`には、次のいずれかの形式を使用できます。 • 共有またはエクスポートのルートから始まる完全パス • 共有のルートに対する相対パス パス値には、NFS形式のディレクトリUNIX形式のディレクトリ区切り文字を使用する必要があります。
`-windows-name win_user_name`` または `-unix-name``unix_user_name`	アクセス要求をトレースするWindowsユーザ名またはUNIXユーザ名を指定できます。ユーザ名変数では大文字と小文字は区別されません。同じフィルタにWindowsユーザ名とUNIXユーザ名の両方を指定することはできません。 トレースできるのはSMBおよびNFSのアクセスイベントですが、mixedセキュリティ形式またはUNIXセキュリティ形式のデータに対してアクセスチェックを実行するときに、マッピングされたUNIXユーザおよびUNIXグループが使用されることがあります。
`-trace-allow{yes`	`no}`

セキュリティトレースフィルタでは、拒否イベントのトレースが常に有効になります。必要に応じて、許可イベントをトレースすることもできます。許可イベントをトレースするには、このパラメータをに設定し`yes`ます。	`-enabled{enabled`
`disabled}`	セキュリティトレースフィルタを有効または無効にすることができます。デフォルトでは、セキュリティトレースフィルタは有効になっています。
`-time-enabled integer`	フィルタのタイムアウトを指定できます。指定した時間が経過すると、フィルタは無効になります。

手順

1. セキュリティトレースフィルタを作成します。

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   `filter_parameters`は、オプションのフィルタパラメータのリストです。

   の詳細については `vserver security trace filter create`、を"ONTAPコマンド リファレンス"参照してください。

2. セキュリティトレースフィルタエントリを確認します。

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

例

次のコマンドは、IPアドレス10.10.10.7から共有パスのファイルにアクセスするすべてのユーザを対象としたセキュリティトレースフィルタを作成し `\\server\share1\dir1\dir2\file.txt`ます。フィルタでは、オプションに完全なパスが使用され `-path`ます。データへのアクセスに使用されるクライアントのIPアドレスは10.10.10.7です。フィルタは30分後にタイムアウトします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

次のコマンドは、オプションの相対パスを使用してセキュリティトレースフィルタを作成し `-path`ます。このフィルタは、「 `joe` 」という名前の `Windows` ユーザのアクセスをトレースします。`Joe`は共有パスの

ファイルにアクセスしています `\\server\share1\dir1\dir2\file.txt`。許可イベントと拒否イベントをトレースします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

ONTAP SVMのセキュリティトレースフィルタに関する情報を表示する

Storage Virtual Machine（SVM）で設定されているセキュリティトレースフィルタに関する情報を表示できます。これにより、各フィルタがトレースするアクセスイベントのタイプを確認できます。

ステップ

1. コマンドを使用して、セキュリティトレースフィルタエントリに関する情報を表示します `vserver security trace filter show`。

   の詳細については `vserver security trace filter show`、を"ONTAPコマンド リファレンス"参照してください。

例

次のコマンドを実行すると、 SVM vs1 のすべてのセキュリティトレースフィルタに関する情報が表示されます。

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

ONTAP SVM でセキュリティ トレース結果を表示する

セキュリティトレースフィルタに一致するファイル操作に対して生成されたセキュリティトレースの結果を表示できます。この結果を使用して、ファイルアクセスセキュリティ設定の検証や、SMBおよびNFSのファイルアクセスに関する問題のトラブルシューティングを行うことができます。

開始する前に

有効なセキュリティトレースフィルタが存在している必要があり、セキュリティトレースの結果が生成されるように、セキュリティトレースフィルタに一致するSMBクライアントまたはNFSクライアントから処理が実行されている必要があります。

タスクの内容

すべてのセキュリティトレース結果の概要を表示することも、オプションのパラメータを指定して、出力に表示する情報をカスタマイズすることもできます。これは、セキュリティトレースの結果に多数のレコードが含まれている場合に役立ちます。

オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- Storage Virtual Machine（SVM）名
- ノード名
- セキュリティトレースのインデックス番号
- セキュリティ形式
- パス
- 理由
- ユーザ名

  トレースフィルタの設定に応じて、ユーザ名が表示されます。

フィルタの設定方法	そしたら…。
UNIXユーザ名を使用	UNIXユーザ名が表示されます。
Windowsユーザ名を使用	Windowsユーザ名が表示されます。
ユーザ名を使用しない	Windowsユーザ名が表示されます。

オプションのパラメータを使用して、出力をカスタマイズできます。コマンド出力で返される結果を絞り込むために使用できるオプションのパラメータには、次のようなものがあります。

オプションのパラメータ	説明
`-fields` `field_name`はい。	選択したフィールドの出力を表示します。このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

-instance	セキュリティトレースイベントに関する詳細情報を表示します。このパラメータを他のオプションのパラメータとともに使用して、特定のフィルタ結果に関する詳細情報を表示します。
-node node_name	指定したノード上のイベントに関する情報のみを表示します。
-vserver vserver_name	指定したSVM上のイベントに関する情報のみを表示します。
-index integer	指定したインデックス番号に対応するフィルタの結果として発生したイベントに関する情報を表示します。
-client-ip IP_address	指定したクライアントIPアドレスからのファイルアクセスの結果として発生したイベントに関する情報を表示します。
-path path	指定したパスへのファイルアクセスの結果として発生したイベントに関する情報を表示します。
-user-name user_name	指定したWindowsユーザまたはUNIXユーザによるファイルアクセスの結果として発生したイベントに関する情報を表示します。
-security-style security_style	指定したセキュリティ形式のファイルシステムで発生したイベントに関する情報を表示します。

その他のオプションパラメータの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. コマンドを使用して、セキュリティトレースフィルタの結果を表示します `vserver security trace trace-result show`。

   ```
   vserver security trace trace-result show -user-name domain\user
   ```

   ```
   Vserver: vs1

   Node     Index   Filter Details          Reason
   -------- ------- ---------------------  ------------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

ONTAP SVMのセキュリティトレースフィルタを変更する

トレースされたアクセスイベントを特定する際に使用するオプションのフィルタパラメータを変更するには、既存のセキュリティトレースフィルタを変更します。

タスクの内容

変更するセキュリティトレースフィルタを特定するには、フィルタを適用したStorage Virtual Machine（SVM）の名前とフィルタのインデックス番号を指定します。オプションのフィルタパラメータはすべて変更できます。

手順

1. セキュリティトレースフィルタを変更します。

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name`は、セキュリティトレースフィルタを適用するSVMの名前です。
   - `index_number`は、フィルタに適用するインデックス番号です。このパラメータに指定できる値は1~10です。
   - `filter_parameters`は、オプションのフィルタパラメータのリストです。

2. セキュリティトレースフィルタエントリを確認します。

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

例

次の例は、インデックス番号 1 のセキュリティトレースフィルタを変更します。このフィルタは、任意のIPアドレスから共有パスを持つファイルにアクセスしているすべてのユーザのイベントをトレースし`\\server\share1\dir1\dir2\file.txt`ます。フィルタでは、オプションに完全なパスが使用され `-path`ます。許可イベントと拒否イベントをトレースします。

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                              Vserver: vs1
                         Filter Index: 1
            Client IP Address to Match: -
                                  Path: /dir1/dir2/file.txt
                  Windows User Name: -
                     UNIX User Name: -
                Trace Allow Events: yes
                    Filter Enabled: enabled
             Minutes Filter is Enabled: 60
```

ONTAP SVM のセキュリティ トレース フィルタを削除する

セキュリティトレースフィルタエントリが不要になった場合は削除できます。セキュリティトレースフィルタはStorage Virtual Machine（SVM）ごとに10個までしか使用できないため、上限に達した場合は、不要なフィルタを削除すると新しいフィルタを作成できます。

タスクの内容

削除するセキュリティトレースフィルタを一意に識別するには、次の項目を指定する必要があります。

- トレースフィルタが適用されている SVM の名前
- トレースフィルタのフィルタインデックス番号

手順

1. 削除するセキュリティトレースフィルタエントリのフィルタインデックス番号を確認します。

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. 前の手順で確認したフィルタインデックス番号を使用して、フィルタエントリを削除します。

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

   ```
   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. セキュリティトレースフィルタエントリが削除されたことを確認します。

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

ONTAP SVM のセキュリティ トレース レコードを削除する

セキュリティトレースレコードを使用したファイルアクセスセキュリティの検証や、SMB または NFS のクライアントアクセスに関する問題のトラブルシューティングが完了したら、セキュリティトレースのログからセキュリティトレースレコードを削除できます。

タスクの内容

セキュリティトレースレコードを削除する前に、レコードのシーケンス番号を確認しておく必要があります。

> 各Storage Virtual Machine（SVM）には、最大128件のトレースレコードを格納できます。SVM でこの上限に達した場合、最も古いトレースレコードが自動的に削除されて、新しいレコードが追加されます。したがって、 SVM のトレースレコードを手動で削除しなくても、上限に達したときに、 ONTAP によって自動的に最も古いトレース結果を削除して新しい結果用のスペースを確保することができます。

手順

1. 削除するレコードのシーケンス番号を指定します。

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. セキュリティトレースレコードを削除します。

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer
   ```

   ```
   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node` `node_name`は、削除するパーミッショントレーシングイベントが発生したクラスタノードの名前です。

     これは必須パラメータです。

   - `-vserver` `vserver_name`は、削除対象のパーミッショントレーシングイベントが発生したSVMの名前です。

     これは必須パラメータです。

   - `-seqnum` `integer`は、削除するログイベントのシーケンス番号です。

     これは必須パラメータです。

ONTAP SVM上のすべてのセキュリティトレースレコードを削除します

既存のセキュリティトレースレコードが不要である場合は、 1 つのコマンドで特定のノード上のレコードをすべて削除できます。

ステップ

1. すべてのセキュリティトレースレコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

   - `-node` `node_name`は、削除するパーミッショントレーシングイベントが発生したクラスタノードの名前です。
   - `-vserver` `vserver_name`は、削除するパーミッショントレーシングイベントが発生したStorage Virtual Machine（SVM）の名前です。

ONTAP セキュリティ トレースの結果を解釈する

セキュリティトレースの結果には、要求が許可または拒否された理由が示されます。出力には、アクセスを許可または拒否する理由と、アクセスが許可または拒否されるアクセスチェックパス内の場所を組み合わせた結果が表示されます。結果を使用して、アクションが許可されている理由と許可されていない理由を特定できます。

結果タイプとフィルタの詳細のリストに関する情報の検索

セキュリティトレースの結果に含めることができる結果タイプとフィルタの詳細のリストは、コマンドで確認`vserver security trace trace-result show`できます。の詳細については `vserver security trace trace-result show`、を"ONTAPコマンド リファレンス"参照してください。

結果タイプのフィールドの `Allow`出力例 `Reason`

次に、結果タイプのトレース結果ログに表示されるフィールドの `Allow`出力例を示し `Reason`ます。

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

結果タイプのフィールドの `Allow`出力例 `Reason`

次に、結果タイプのトレース結果ログに表示されるフィールドの `Deny`出力例を示し `Reason`ます。

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

フィールドの出力例 `Filter details`

次に、トレース結果ログのフィールドの出力例を示します。この出力 `Filter details`には、フィルタ条件に一致するファイルとフォルダが格納されているファイルシステムの有効なセキュリティ形式が表示されます。

```
Security Style: MIXED and ACL
```

ONTAP SVMに関する追加情報の入手先

SMBクライアントアクセスをテストしたあと、SMBの高度な設定を行ったり、SANアクセスを追加したりできます。NFSクライアントアクセスをテストしたあと、NFSの高度な設定を行ったり、SANアクセスを追加したりできます。プロトコルアクセスが完了したら、SVMのルートボリュームを保護する必要があります。

SMBの設定

SMBアクセスについてさらに詳しく設定するには、次のコマンドを使用します。

- "SMBの管理"

  SMBプロトコルを使用したファイルアクセスを設定および管理する方法について説明します。

- "NetAppテクニカルレポート4191：『Best Practices Guide for Clustered Data ONTAP 8 .2 Windows File Services』"

  SMBの導入やその他のWindowsファイルサービスの機能の概要と、ONTAPに関する推奨事項や基本的なトラブルシューティング情報を紹介します。

- "NetAppテクニカルレポート3740：『SMB 2 Next-Generation CIFS Protocol in Data ONTAP』"

  SMB 2の機能、設定の詳細、およびONTAPでの実装について説明します。

NFSの設定

NFSアクセスについてさらに詳しく設定するには、次のコマンドを使用します。

- "NFSの管理"

  NFSプロトコルを使用したファイルアクセスを設定および管理する方法について説明します。

- "NetAppテクニカルレポート4067：『NFS Best Practice and Implementation Guide』"

  NFSv3およびNFSv4の運用ガイドであり、NFSv4を中心にONTAPオペレーティングシステムの概要を説明しています。

- "NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

  LDAP、NIS、DNS、およびローカルユーザファイルとローカルグループファイルを認証用に設定する際のベストプラクティス、制限、推奨事項、および考慮事項を包括的に示します。

- "ネットアップテクニカルレポート 4616 ：『 NFS Kerberos in ONTAP with Microsoft Active Directory 』"
- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"
- "NetAppテクニカルレポート3580：『NFSv4の拡張機能とベストプラクティスガイド：Data ONTAPでの

実装』"

ONTAPを実行するシステムに接続されたAIX、Linux、またはSolarisクライアントにNFSv4のコンポーネントを実装する際のベストプラクティスを紹介しています。

ルートボリュームの保護

SVMでプロトコルを設定したら、ルートボリュームを保護してください。

- "データ保護"

  負荷共有ミラーを作成してSVMルートボリュームを保護する方法について説明しています。これは、NAS対応のSVMに対するNetAppのベストプラクティスです。また、SVMルートボリュームを負荷共有ミラーから昇格させてボリュームの障害や損失からリカバリする簡単な方法についても説明しています。

System Managerによる暗号化の管理

ソフトウェアベースの暗号化を使用して、 **ONTAP**クラスタに保存されたデータを暗号化します。

ボリューム暗号化を使用して、デバイスの転用、返却、置き忘れ、盗難に際してボリュームのデータが読み取られることがないようにします。ボリューム暗号化には特別なディスクは必要なく、すべてのHDDおよびSSDで使用できます。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"ソフトウェア レベルの暗号化を有効にします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ボリューム暗号化にはキー管理ツールが必要です。System Managerを使用してオンボードキーマネージャを設定できます。外部キー管理ツールも使用できますが、その場合はONTAP CLIを使用して事前にセットアップする必要があります。

キー管理ツールを設定すると、新しいボリュームはデフォルトで暗号化されます。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [暗号化]*で、をクリックし てオンボードキーマネージャを初めて設定します。
3. 既存のボリュームを暗号化するには、*[ストレージ]>[ボリューム]*をクリックします。
4. 目的のボリュームでをクリックし 、*[編集]*をクリックします。
5. *暗号化を有効にする*を選択します。

自己暗号化ドライブを使用して**ONTAP**クラスタに保存されたデータを暗号化します

ディスク暗号化を使用して、デバイスの転用、返却、置き忘れ、盗難に際してローカル

階層内のすべてのデータが読み取られることがないようにします。ディスク暗号化には、特殊な自己暗号化HDDまたはSSDが必要です。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、"以下の手順を実行します"ハードウェア レベルの暗号化を有効にします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ディスク暗号化にはキー管理ツールが必要です。System Managerを使用してオンボードキーマネージャを設定できます。外部キー管理ツールも使用できますが、その場合はONTAP CLIを使用して事前にセットアップする必要があります。

ONTAPで自己暗号化ディスクが検出された場合、ローカル階層の作成時にオンボードキーマネージャを設定するように求められます。

手順

1. [暗号化]*で、をクリックし てオンボードキーマネージャを設定します。
2. ディスクのキー変更が必要であることを示すメッセージが表示されたら、をクリックし 、*[ディスクのキー変更]*をクリックします。

CLIを使用した暗号化の管理

ONTAPの保存データの暗号化について学ぶ

NetAppは、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないように、ソフトウェアベースとハードウェアベースの暗号化テクノロジを提供します。

- NetApp Volume Encryption（NVE）を使用したソフトウェアベースの暗号化で、一度に1つのボリュームのデータ暗号化をサポート
- NetAppストレージ暗号化（NSE）を使用したハードウェアベースの暗号化では、データの書き込み時のフルディスク暗号化（FDE）がサポートされます。

NetAppボリュームとアグリゲートの暗号化を構成する

ONTAP NetAppボリュームとアグリゲートの暗号化について学ぶ

NetApp Volume Encryption（NVE）は、一度に1つのボリュームの保存データを暗号化するためのソフトウェアベースのテクノロジです。暗号化キーにはストレージシステムからしかアクセスできないため、デバイスの転用、返却、置き忘れ、盗難に際してボリュームのデータが読み取られることはありません。

NVEの概要

NVEでは、メタデータとデータ（Snapshotを含む）の両方が暗号化されます。データへのアクセスには、ボリュームごとに1つの一意のXTS-AES-256キーが使用されます。外部キー管理サーバまたはオンボードキーマネージャ（OKM）がノードにキーを提供します。

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

ONTAP 9 .7以降では、Volume Encryption（VE）ライセンスがあり、オンボードまたは外部のキー管理ツールを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。VEライセンスはに含まれてい"ONTAP One"ます。外部キーマネージャまたはオンボードキーマネージャが設定されている場合は、新しいアグリゲートおよび新しいボリュームに対する保存データの暗号化の設定方法が変更されます。新しいアグリゲートでは、NetAppアグリゲート暗号化（NAE）がデフォルトで有効になります。NAEアグリゲートに含まれていない新しいボリュームでは、デフォルトでNetApp Volume Encryption（NVE）が有効になります。マルチテナントキー管理を使用してデータStorage Virtual Machine（SVM）に独自のキー管理機能が設定されている場合、そのSVM用に作成されたボリュームには自動的にNVEが設定されます。

新規または既存のボリュームで暗号化を有効にできます。NVEは、重複排除や圧縮など、さまざまなStorage Efficiency機能をサポートしています。ONTAP 9 .14.1以降では、この機能を既存のSVMルートボリュームでNVEを有効にする使用できます。

> SnapLockを使用している場合は、新しい空のSnapLockでのみ暗号化を有効にできます。既存のSnapLockボリュームで暗号化を有効にすることはできません。

NVEは、アグリゲートのタイプ（HDD、SSD、ハイブリッド、アレイLUN）やRAIDタイプを問わず、サポートされているONTAP環境（ONTAP Selectを含む）で使用できます。NVE をハードウェアベースの暗号化と併用すれば、自己暗号化ドライブ上のデータを「暗号化」することもできます。

NVEを有効にすると、コアダンプも暗号化されます。

アグリゲートレベルの暗号化

通常、暗号化されたすべてのボリュームには一意のキーが割り当てられます。このキーは、ボリュームを削除すると一緒に削除されます。

ONTAP 9.6 以降では、 _NetApp Aggregate Encryption （ NAE ） _ を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。暗号化されたボリュームを削除しても、アグリゲートのキーは削除されません。このキーは、アグリゲート全体を削除すると削除されます。

アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。そうしないと、NVEでアグリゲートレベルの重複排除がサポートされません。

ONTAP 9.7以降では、Volume Encryption（VE）ライセンスがあり、オンボード / 外部キー マネージャを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。

NVEボリュームとNAEボリュームは同一アグリゲート内で共存できます。アグリゲートレベルの暗号化で暗号化されたボリュームは、デフォルトでNAEボリュームになります。このデフォルトの設定は、ボリュームを暗号化するときに無効にすることができます。

コマンドを使用して、NVEボリュームをNAEボリュームに（またはその逆に）変換できます `volume move` 。NAEボリュームはNVEボリュームにレプリケートできます。

NAEボリュームではコマンドを使用できません `secure purge`。

外部キー管理サーバを使用する状況

オンボード キー マネージャを使用した方がコストもかからず一般的には便利ですが、次のいずれかに当てはまる場合はKMIPサーバを用意する必要があります。

- 暗号化キー管理ソリューションが、Federal Information Processing Standards（FIPS；連邦情報処理標準）140-2またはOASIS KMIP標準に準拠している必要があります。
- 暗号化キーを一元管理できるマルチクラスタソリューションが必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

外部キー管理の範囲

外部キー管理の範囲によって、キー管理サーバがクラスタ内のすべてのSVMを保護するか、選択したSVMのみを保護するかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、 *cluster scop* を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。
- ONTAP 9.6 以降では、 *svm scop* を使用して、クラスタ内の指定した SVM に外部キー管理を設定できます。これは、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者のみが、そのテナントのキーにアクセスできます。
  - ONTAP 9.17.1以降では、 バービカンKMSデータ SVM のみの NVE キーを保護します。
  - ONTAP 9 .10.1以降では、を使用してNVEキーを保護できるのAzure Key Vault と Google Cloud KMS はデータSVMのみです。これは、9.12.0以降のAWS KMSで利用できるようになりました。

同じクラスタで両方のスコープを使用できます。1つのSVMに対してキー管理サーバが設定されている場合は、それらのサーバのみを使用してキーが保護されます。そうでない場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

検証済みの外部キー管理ツールのリストはにあり"NetApp Interoperability Matrix Tool（IMT）"ます。この一覧は、 IMT の検索機能に「キー管理ツール」という用語を入力すると表示されます。

Azure Key VaultやAWS KMSなどのクラウドKMSプロバイダはKMIPをサポートしていません。そのため、IMTには表示されません。

サポートの詳細

次の表に、NVEのサポートの詳細を示します。

リソースまたは機能	サポートの詳細
プラットフォーム	AES-NIオフロード機能が必要です。ご使用のプラットフォームでNVEとNAEがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

暗号化	ONTAP 9 .7以降では、Volume Encryption（VE）ライセンスを追加し、オンボードまたは外部のキー管理ツールを設定している場合、新しく作成したアグリゲートとボリュームはデフォルトで暗号化されます。暗号化されていないアグリゲートを作成する必要がある場合は、次のコマンドを使用します。
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	プレーンテキストボリュームを作成する必要がある場合は、次のコマンドを使用します。
	
	`volume create -encrypt false`
	
	次の場合、暗号化はデフォルトでは有効になりません。
	
	• VEライセンスがインストールされていません。
	• キー管理ツールが設定されていません。
	• プラットフォームまたはソフトウェアが暗号化をサポートしていません。
	• ハードウェア暗号化が有効になっています。

ONTAP	すべてのONTAP実装。Cloud Volumes ONTAPのサポートは、 ONTAP 9.5 以降で利用できます。
デバイス	HDD、SSD、ハイブリッド、アレイLUN。
RAID	RAID0、RAID4、RAID-DP、RAID-TEC。
ボリューム	データボリュームと既存のSVMルートボリューム。MetroClusterメタデータボリュームのデータは暗号化できません。9.14.1より前のバージョンのONTAPでは、NVEを使用してSVMルートボリュームのデータを暗号化できません。ONTAP 9 .14.1以降では、ONTAPはをサポートしていSVMルートボリュームのNVEます。
アグリゲートレベルの暗号化	ONTAP 9 .6以降では、NVEでアグリゲートレベルの暗号化（NAE）がサポートされます。 • アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。 • アグリゲートレベルで暗号化されたボリュームのキーは変更できません。 • アグリゲートレベルで暗号化されたボリュームでは、セキュア パージがサポートされません。 • NAEでは、データ ボリュームに加えて、SVMルート ボリュームとMetroClusterメタデータ ボリュームの暗号化がサポートされます。ただし、ルート ボリュームの暗号化はサポートされません。

SVMスコープ	MetroClusterはONTAP 9.8以降でサポートされます。 ONTAP 9.6以降では、NVEで外部キー管理のみを対象にSVMスコープがサポートされます。オンボード キー マネージャに対してはサポートされません。
Storage Efficiency	重複排除、圧縮、コンパクション、FlexClone。 クローンでは、親からスプリットしたあとも親と同じキーを使用します。スプリットクローンでを実行する必要があり `volume move`ます。この場合、スプリットクローンには別のキーが割り当てられます。
レプリケーション	• ボリュームレプリケーションでは、ソースボリュームとデスティネーションボリュームで異なる暗号化設定を使用できます。暗号化は、ソースに対して設定することも、デスティネーションに対して設定解除することもできます。逆も同様です。ソースで設定された暗号化はデスティネーションにレプリケートされません。暗号化は、ソースとデスティネーションで手動で設定する必要があります。NVEの設定およびを参照してくださいNVEによるボリュームデータの暗号化。 • SVMレプリケーションの場合、デスティネーション ボリュームは自動的に暗号化されます。ただし、ボリューム暗号化をサポートするノードがデスティネーションに含まれていない場合、レプリケーションは成功しますが、デスティネーション ボリュームは暗号化されません。 • MetroCluster構成では、各クラスタが設定されたキー サーバから外部キー管理のキーを取得します。OKM（オンボード キー マネージャ）のキーは、設定レプリケーション サービスによってパートナー サイトにレプリケートされます。
コンプライアンス	SnapLockは、コンプライアンス モードとエンタープライズ モードの両方で、新しいボリュームに対してのみサポートされます。既存のSnapLockボリュームで暗号化を有効にすることはできません。
FlexGroupホリユウム	FlexGroupボリュームがサポートされています。宛先アグリゲートは、ボリュームレベルまたはアグリゲートレベルのいずれかで、ソースアグリゲートと同じタイプである必要があります。ONTAP 9.5以降では、FlexGroupボリュームのキーをインプレースで変更できます。
7-Modeからの移行	7-Mode Transition Tool 3.3以降では、7-Mode Transition Tool CLIを使用して、クラスタ システムのNVE対応デスティネーション ボリュームへのコピーベースの移行を実行できます。

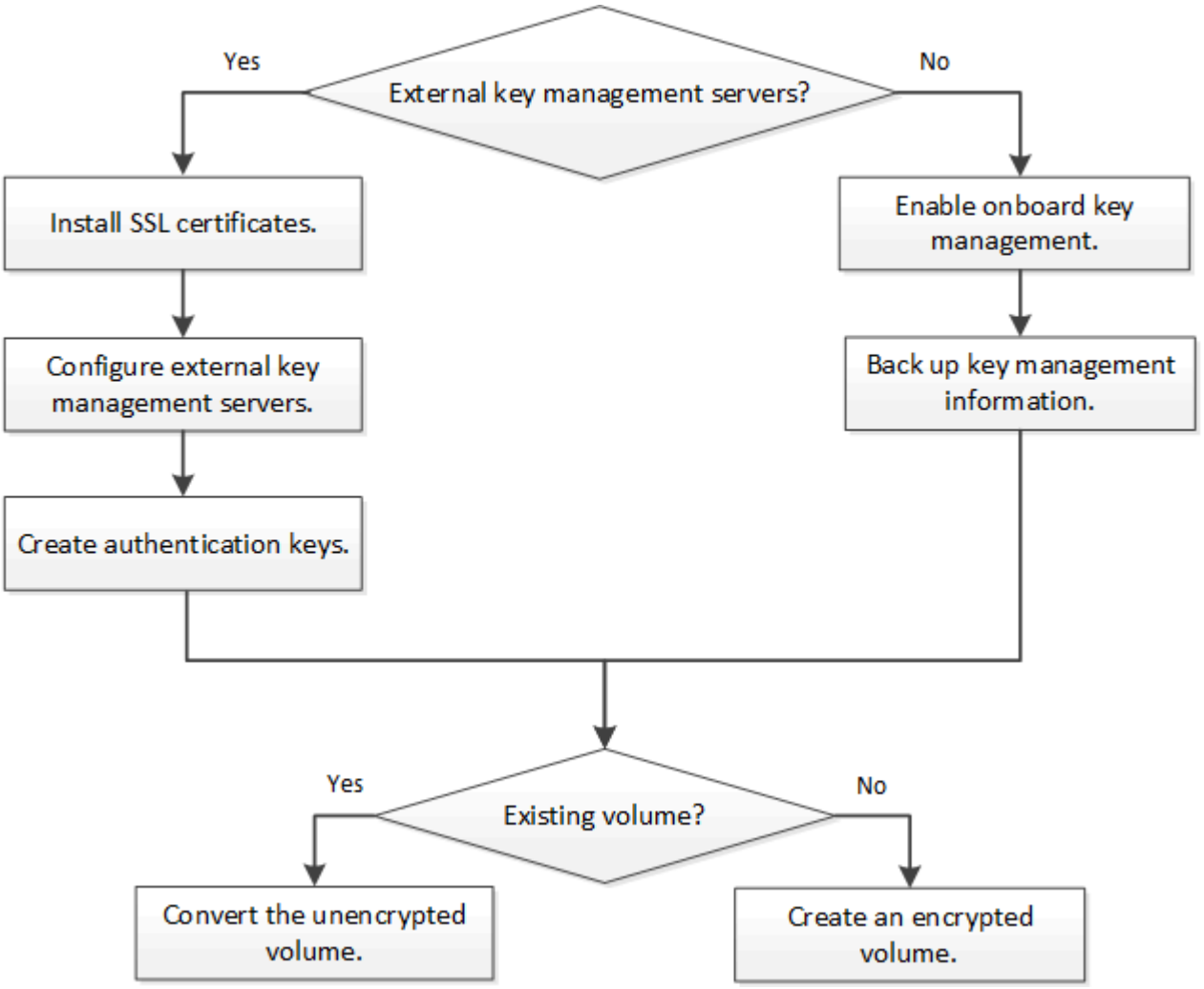
関連情報

- "FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"
- "storage aggregate create"

ONTAP NetAppボリューム暗号化ワークフロー

ボリューム暗号化を有効にする前に、キー管理サービスを設定する必要があります。新

しいボリュームと既存のボリュームのいずれでも暗号化を有効にできます。



"VEライセンスをインストールする必要があります。"NVEでデータを暗号化する前に、キー管理サービスを設定しておく必要があります。ライセンスをインストールする前に、を実行する必要があり"ONTAP のバージョンが NVE をサポートしているかどうかを確認します"ます。

NVEの設定

ONTAPクラスタバージョンがNVEをサポートしているかどうかを確認する

ライセンスをインストールする前に、クラスタのバージョンがNVEをサポートしているかどうかを確認する必要があります。クラスタのバージョンは、コマンドを使用して確認できます `version`。

タスクの内容

クラスタのバージョンは、クラスタ内のいずれかのノードで実行されているONTAPの最下位のバージョンです。

手順

1. クラスタのバージョンがNVEをサポートしているかどうかを確認します。

```
version -v
```

コマンドの出力に「no Data At Rest Encryption」というテキストが表示されている場合、または使用しているプラットフォームがに記載されていない場合は、NVEがサポートされません `1Ono-DARE`"サポートの詳細"。

ONTAPクラスタにボリューム暗号化ライセンスをインストールする

VEライセンスでは、クラスタ内のすべてのノードでこの機能を使用できます。このライセンスは、NVEでデータを暗号化する前に必要です。に含まれてい"ONTAP One"ます。

ONTAP Oneより前のバージョンでは、VEライセンスは暗号化バンドルに含まれていました。Encryptionバンドルは提供されなくなりましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は選択できます"ONTAP Oneへのアップグレード"。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 営業担当者からVEライセンスキーを入手するか、ONTAP Oneをインストールしておく必要があります。

手順

1. "VEライセンスがインストールされていることを確認します。"です。

   VEライセンスパッケージ名はです `VE`。

2. ライセンスがインストールされていない場合は、"System ManagerまたはONTAP CLIを使用してインストール"を参照してください。

外部キー管理の設定

ONTAP NetAppボリューム暗号化を使用した外部キー管理の構成について学習します

1つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードにキーを提供します。オンボード キー マネージャに加えて、 ONTAP は複数の外部キー管理サーバをサポートしています。

```
Beginning with ONTAP 9.10.1, you can use xref:{relative_path}manage-keys-
azure-google-task.html[Azure Key Vault or Google Cloud Key Manager
Service] to protect your NVE keys for data SVMs. Beginning with ONTAP
9.11.1, you can configure multiple external key managers in a cluster. See
xref:{relative_path}configure-cluster-key-server-task.html[Configure
clustered key servers]. Beginning with ONTAP 9.12.0, you can use
link:https://docs.aws.amazon.com/kms/latest/developerguide/overview.html[A
WS' KMS^] to protect your NVE keys for data SVMs. Beginning with ONTAP
9.17.1, you can use OpenStack's xref:{relative_path}manage-keys-barbican-
task.html[Barbican KMS] to protect your NVE keys for data SVMs.
```

ONTAP System Managerで外部キーマネージャを管理する

ONTAP 9 7以降では、オンボードキーマネージャを使用して認証キーと暗号化キーを格納および管理できます。ONTAP 9 .13.1以降では、外部キー管理ツールを使用してこれらのキーを格納および管理することもできます。

オンボードキーマネージャは、クラスタ内のセキュアなデータベースにキーを格納および管理します。スコープはクラスタです。外部キー管理ツールは、クラスタの外部にキーを格納および管理します。スコープには、クラスタまたはStorage VMを指定できます。1つ以上の外部キー管理ツールを使用できます。次の条件が適用されます。

- オンボードキーマネージャが有効になっている場合、外部キー管理ツールをクラスタレベルで有効にすることはできませんが、Storage VMレベルで有効にすることはできます。
- 外部キー管理ツールがクラスタレベルで有効になっている場合、オンボードキーマネージャを有効にすることはできません。

外部キー管理ツールを使用する場合は、Storage VMおよびクラスタごとに最大4つのプライマリキーサーバを登録できます。各プライマリキーサーバは、最大3台のセカンダリキーサーバでクラスタ化できます。

外部キー管理ツールを設定する

Storage VMに外部キー管理ツールを追加するには、Storage VMのネットワークインターフェイスの設定時にオプションのゲートウェイを追加する必要があります。Storage VMをネットワークルートなしで作成した場合は、外部キー管理ツール用のルートを明示的に作成する必要があります。を参照して "LIFを作成する（ネットワークインターフェイス）"

手順

外部キー管理ツールは、System Managerの別の場所から設定できます。

1. 外部キー管理ツールを設定するには、次のいずれかの開始手順を実行します。

ワークフロー	ナビゲーション	開始ステップ
キーマネージャを設定します	**[クラスタ]>*[設定]***	[セキュリティ]*セクションまでスクロールします。[暗号化]*で、を選択します。[外部キーマネージャ]*を選択します。
ローカル階層を追加してください	ストレージ>*階層*	[+ローカル階層の追加]*を選択します。[Configure Key Manager]チェックボックスをオンにします。[外部キーマネージャ]*を選択します。
ストレージを準備	ダッシュボード	セクションで、[ストレージの準備]*を選択します。次に、[Configure Key Manager]を選択します。[外部キーマネージャ]*を選択します。
暗号化を設定（キー管理ツールをStorage VMスコープでのみ使用）	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。の[暗号化]*セクションで、を選択します。

2. プライマリキーサーバを追加するには、を選択し Add 、**[IP**アドレス**]**または**[**ホスト名**]***および[ポート]*フィールドに入力します。
3. インストールされている既存の証明書は、**[KMIP Server CA Certificates]***フィールドと[KMIP Client Certificate]*フィールドに表示されます。次のいずれかの操作を実行できます。
   - を選択し て、キー管理ツールにマッピングするインストール済み証明書を選択します。（複数のサービスCA証明書を選択できますが、選択できるクライアント証明書は1つだけです）。
   - まだインストールされていない証明書を追加して外部キー管理ツールにマッピングする場合は、*[新しい証明書の追加]*を選択します。
   - 外部キー管理ツールにマッピングしないインストール済みの証明書を削除するには、証明書名の横にあるを選択し ます。
4. セカンダリキーサーバを追加するには、**[**セカンダリキーサーバ**]***列で[追加]*を選択し、詳細を指定します。
5. [保存]*を選択して設定を完了します。

既存の外部キー管理ツールを編集する

すでに外部キー管理ツールを設定している場合は、その設定を変更できます。

手順

1. 外部キー管理ツールの設定を編集するには、次のいずれかの開始手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	**[**クラスタ**]**>*[設定]*	セクションまでスクロールします。**[**暗号化**]***でを選択し、[外部キーマネージャの編集]*を選択します。
Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し、[外部キーマネージャの編集]*を選択します。

2. 既存のキーサーバは*[キーサーバ]*の表に表示されます。次の処理を実行できます。
   - を選択して新しいキーサーバを追加し Add ます。
   - キーサーバを削除するには、テーブルセルの末尾にあるキーサーバの名前を選択します 。そのプライマリキーサーバに関連付けられているセカンダリキーサーバも設定から削除されます。

外部キー管理ツールを削除する

ボリュームが暗号化されていない場合は、外部キー管理ツールを削除できます。

手順

1. 外部キー管理ツールを削除するには、次のいずれかの手順を実行します。

適用範囲	ナビゲーション	開始ステップ

クラスタスコープの外部キー管理ツール	**[クラスタ]>*[設定]***	セクションまでスクロールします。**[暗号化]***で、を選択し⋮、[外部キーマネージャの削除]*を選択します。
Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し⋮、[外部キーマネージャの削除]*を選択します。

キー管理ツール間でのキーの移行

クラスタで複数のキー管理ツールを有効にしている場合は、キー管理ツール間でキーを移行する必要があります。このプロセスはSystem Managerで自動的に完了します。

- クラスタレベルでオンボードキーマネージャまたは外部キー管理ツールが有効になっていて、一部のボリュームが暗号化されている場合は、Storage VMレベルで外部キー管理ツールを設定するときに、それらのキーをクラスタレベルのオンボードキーマネージャまたは外部キー管理ツールからStorage VMレベルの外部キー管理ツールに移行する必要があります。このプロセスは、System Managerによって自動的に実行されます。
- Storage VMで暗号化なしでボリュームを作成した場合は、キーを移行する必要はありません。

ONTAPクラスタに**SSL**証明書をインストールする

クラスタとKMIPサーバは、KMIP SSL証明書を使用して相互のIDを検証し、SSL接続を確立します。KMIPサーバとのSSL接続を設定する前に、クラスタのKMIPクライアントSSL証明書、およびKMIPサーバのルート認証局（CA）のSSLパブリック証明書をインストールする必要があります。

タスクの内容

HAペアでは、両方のノードで同じSSL KMIPパブリック証明書とプライベート証明書を使用する必要があります。複数のHAペアを同じKMIPサーバに接続する場合は、HAペアのすべてのノードで同じSSL KMIPパブリック証明書とプライベート証明書を使用する必要があります。

開始する前に

- 証明書を作成するサーバ、KMIPサーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリックSSL KMIPクライアント証明書を入手しておく必要があります。
- クラスタのSSL KMIPクライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIPクライアント証明書はパスワードで保護しないでください。
- KMIPサーバのルート認証局（CA）のSSLパブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

ⓘ KMIPサーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前後どちらでも実行できます。

手順

1. クラスタのSSL KMIPクライアント証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type client
```

SSL KMIPのパブリック証明書とプライベート証明書を入力するように求められます。

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. KMIPサーバのルート認証局（CA）のSSLパブリック証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

関連情報

- "セキュリティ証明書のインストール"

ONTAP 9.6以降で**NVE**の外部キー管理を有効にする

KMIP サーバーを使用して、クラスターが暗号化されたデータにアクセスするために使用するキーを保護します。ONTAP 9.6以降では、必要に応じて別の外部キー管理ツールを設定して、データSVMが暗号化されたデータにアクセスする際に使用するキーを保護することもできます。

ONTAP 9 .11.1以降では、プライマリキーサーバごとに最大3つのセカンダリキーサーバを追加してクラスタ化されたキーサーバを作成できます。詳細については、を参照してください クラスタ化された外部キーサーバの設定。

タスクの内容

1つのクラスタまたはSVMに最大4つのKMIPサーバを接続できます。冗長性と災害復旧のために少なくとも 2 台のサーバーを使用します。

外部キー管理の範囲によって、キー管理サーバがクラスタ内のすべてのSVMを保護するか、選択したSVMのみを保護するかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、 *cluster scop* を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。
- ONTAP 9.6 以降では、 *svm scop* を使用して、クラスタ内のデータ SVM に外部キー管理を設定できます。これは、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者のみが、そのテナントのキーにアクセスできます。
- マルチテナント環境の場合は、次のコマンドを使用して、 *MT_EK_MGMT* のライセンスをインストールします。

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  の詳細については `system license add`、を"ONTAPコマンド リファレンス"参照してください。

同じクラスタで両方のスコープを使用できます。1つのSVMに対してキー管理サーバが設定されている場合は、それらのサーバのみを使用してキーが保護されます。そうでない場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

オンボードキー管理はクラスタスコープで設定し、外部キー管理はSVMスコープで設定できます。コマンドを使用すると、クラスタスコープのオンボードキー管理からSVMスコープの外部キー管理ツールにキーを移行できます `security key-manager key migrate`。

の詳細については `security key-manager key migrate`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- MetroCluster環境の場合:
  - 外部キー管理を有効にする前に、 MetroCluster を完全に構成する必要があります。
  - 両方のクラスターに同じ KMIP SSL 証明書をインストールする必要があります。
  - 両方のクラスターで外部キー マネージャーを構成する必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > その `security key-manager external enable`コマンドは `security key-manager setup`指示。クラスタログインプロンプトでコマンドを実行すると、 `*admin_SVM*`デフォルトは現在のクラスタの管理 SVM になります。実行することができます `security key-manager external modify`外部キー管理構成を変更するコマンド。

   次のコマンドは、3台の外部キーサーバでの外部キー管理を有効にします `cluster1`。1つ目のキーサーバはホスト名とポートを使用して指定し、2つ目のキーサーバはIPアドレスとデフォルトポートを使用して指定し、3つ目のキーサーバはIPv6アドレスとポートを使用して指定します。

   ```
   cluster1::> security key-manager external enable -vserver cluster1 -key
   -servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. SVMでキー管理ツールを設定します。

   ```
   security key-manager external enable -vserver SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

- SVMログインプロンプトでコマンドを実行すると、 `SVM`デフォルトは現在の SVM になります。実行することができます `security key-manager external modify`外部キー管理構成を変更するコマンド。
- MetroCluster環境でデータSVMの外部キー管理を設定する場合、パートナークラスタでこのコマンドを繰り返す必要はありません `security key-manager external enable`。

次のコマンドは、デフォルトポート5696をリスンする単一のキーサーバでの外部キー管理を有効にします `svm1`。

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. SVMを追加する場合は、最後の手順を繰り返します。

コマンドを使用して追加のSVMを設定することもできます `security key-manager external add-servers`。 `security key-manager external add-servers`コマンドは、コマンドに置き換わるもの `security key-manager add`です。の詳細については `security key-manager external add-servers`、を"ONTAPコマンド リファレンス"参照してください。

4. 設定したすべてのKMIPサーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name
```

`security key-manager external show-status`コマンドは、コマンドに置き換わるもの `security key-manager show -status`です。の詳細については `security key-manager external show-status`、をlink:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAPコマンド リファレンス"^]参照してください。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  -----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   `volume encryption conversion start`

   ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。

関連情報

- クラスタ化された外部キーサーバの設定
- "システムライセンスの追加"
- "セキュリティキーマネージャーキー移行"
- "セキュリティキーマネージャー外部アドサーバー"
- "security key-manager external show-status"

ONTAP 9.5以前で**NVE**の外部キー管理を有効にする

1つ以上のKMIPサーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1つのノードに最大4つのKMIPサーバを接続できます。冗長性とディザスタリカバリのために、少なくとも2台のサーバが推奨されます。

タスクの内容

ONTAPでは、クラスタ内のすべてのノードに対してKMIPサーバの接続が設定されます。

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster環境を設定する必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタノードのキー管理ツールの接続を設定します。

   ```
   security key-manager setup
   ```

   キー管理ツールのセットアップが開始されます。

   MetroCluster環境では、このコマンドを両方のクラスタで実行する必要があります。詳細はこちら `security key-manager setup`の中で"ONTAPコマンド リファレンス"。

2. 各プロンプトで適切な応答を入力します。
3. KMIPサーバを追加します。

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   MetroCluster環境の場合は、両方のクラスタでこのコマンドを実行する必要があります。

4. 冗長性を確保するためにKMIPサーバを追加します。

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   MetroCluster環境の場合は、両方のクラスタでこのコマンドを実行する必要があります。

5. 設定したすべてのKMIPサーバが接続されていることを確認します。

   ```
   security key-manager show -status
   ```

   この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス" 。

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   ```
   volume encryption conversion start
   ```

   ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

クラウドプロバイダーを使用して**ONTAP**データ **SVM** の **NVE** キーを管理する

ONTAP 9.10.1以降では、と"Google Cloud Platform のキー管理サービス（ Cloud KMS ）"を使用して、クラウドホスト型アプリケーションでONTAP暗号化キーを保護できます"Azure キーボールト（ AKV ）"。NVEキーは、ONTAP 9 .12.0以降で保護することもできます"AWS KMS"。

AWS KMS、AKV、およびCloud KMSを使用して保護"NetApp Volume Encryption （ NVE ）キー"できるのは、データSVMの場合のみです。

タスクの内容

クラウドプロバイダを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

クラウドプロバイダを使用してキーを保護する場合は、デフォルトではデータSVM LIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス（Azureの場合はlogin.microsoftonline.com、Cloud KMSの場合はoauth2.googleapis.com）との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に使用されません。

クラウドプロバイダのキー管理サービスを利用する場合は、次の制限事項に注意してください。

- クラウドプロバイダのキー管理は、NetApp Storage Encryption（NSE）およびNetApp Aggregate Encryption（NAE）では使用できません。"外部 KMIP"代わりに使用できます。
- クラウドプロバイダのキー管理はMetroCluster構成では使用できません。
- クラウドプロバイダのキー管理は、データSVMでのみ設定できます。

開始する前に

- 適切なクラウドプロバイダでKMSを設定しておく必要があります。
- ONTAPクラスタのノードでNVEがサポートされている必要があります。
- "Volume Encryption（VE）ライセンスとマルチテナントEncryption Key Management（MTEKM）ライセ

ンスをインストールしておく必要があります。"です。これらのライセンスはに含まれてい"ONTAP One"ます。

- クラスタ管理者またはSVM管理者である必要があります。
- データSVMに暗号化されたボリュームが含まれていないことと、キー管理ツールを使用していないことを確認してください。データSVMに暗号化されたボリュームが含まれている場合は、KMSを設定する前にそれらのボリュームを移行する必要があります。

外部キー管理の有効化

外部キー管理を有効にする方法は、使用するキー管理ツールによって異なります。適切なキー管理ツールと環境のタブを選択します。

AWS

開始する前に

- 暗号化を管理するIAMロールで使用されるAWS KMSキーの付与を作成する必要があります。IAMロールには、次の処理を許可するポリシーが含まれている必要があります。
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`+詳細については、AWSのドキュメントを参照してください"助成金"。

ONTAP SVMでAWS KMVを有効にする

1. 作業を開始する前に、AWS KMSからアクセスキーIDとシークレットキーの両方を取得します。
2. 権限レベルをadvancedに設定します。
   `set -priv advanced`
3. AWS KMSを有効にします。
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. プロンプトが表示されたら、シークレットキーを入力します。
5. AWS KMSが正しく設定されたことを確認します。
   `security key-manager external aws show -vserver` *`svm_name`*

   の詳細については `security key-manager external aws`、を"ONTAPコマンド リファレンス"参照してください。

Azure

ONTAP SVMでAzure Key Vaultを有効にする

1. 開始する前に、適切な認証クレデンシャル（クライアントシークレットまたは証明書）をAzureアカウントから取得する必要があります。また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用し `cluster show`ます。の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。
2. 特権レベルをadvancedに設定
   `set -priv advanced`
3. SVMでAKVを有効にする
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`プロンプトが表示されたら、クライアント証明書またはAzureアカウントのクライアントシークレットのいずれかを入力します。
4. AKVが正しく有効になっていることを確認します。
   `security key-manager external azure show vserver` *`svm_name`*`サービスの到達可能性がOKでない場合は、データSVM LIFを介してAKVキー管理サービスへの接続を確立します。

   の詳細については `security key-manager external azure`、を"ONTAPコマンド リファレンス"参照してください。

Google Cloud

ONTAP SVMでCloud KMSを有効にする

1. 作業を開始する前に、Google Cloud KMSアカウント キー ファイルの秘密鍵をJSON形式で取得しておきます。これはGCPアカウントから入手できます。また、クラスタ内のすべてのノードが健全であることを確認する必要があります。これを確認するには、コマンドを使用し `cluster show`ます。の詳細については `cluster show`、を"ONTAPコマンド リファレンス"参照してください。
2. 特権レベルをadvancedに設定します。
   `set -priv advanced`
3. SVMでCloud KMSを有効にする
   `security key-manager external gcp enable -vserver *svm_name* -project-id *project_id*-key-ring-name *key_ring_name* -key-ring-location *key_ring_location* -key-name *key_name*`プロンプトが表示されたら、JSONファイルの内容とサービスアカウントの秘密鍵を入力します。
4. Cloud KMS が正しいパラメータで構成されていることを確認します。
   `security key-manager external gcp show vserver *svm_name*`の状態 `kms_wrapped_key_status`なるだろう `"UNKNOWN"`暗号化されたボリュームが作成されていない場合。サービスの到達可能性が「OK」でない場合は、データSVM LIFを使用してGCPキー管理サービスへの接続を確立します。

   の詳細については `security key-manager external gcp`、を"ONTAPコマンド リファレンス"参照してください。

データSVMに対して暗号化されたボリュームがすでに設定されていて、対応するNVEキーが管理SVMのオンボードキーマネージャで管理されている場合は、それらのキーを外部のキー管理サービスに移行する必要があります。これにはCLIを使用して次のコマンドを実行します。
`security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*`データSVMのすべてのNVEキーが正常に移行されるまで、テナントのデータSVM用に暗号化された新しいボリュームを作成できません。

関連情報

- "ネットアップのCloud Volumes ONTAP向け暗号化ソリューションを使用したボリュームの暗号化"
- "セキュリティキーマネージャー外部"

Barbican KMSで**ONTAP**キーを管理する

ONTAP 9.17.1以降では、OpenStackの"バービカンKMS" ONTAPの暗号化キーを保護するためにBarbican KMSが提供されています。Barbicanは、キーを安全に保存し、アクセスするためのサービスです。BarbicanKMSは、データSVMのNetAppボリューム暗号化（NVE）キーを保護するために使用できます。Barbicanは"オープンスタックKeystone"認証用の OpenStack の ID サービス。

タスクの内容

Barbican KMSによる鍵管理は、CLIまたはONTAP REST APIを使用して設定できます。9.17.1リリースでは、Barbican KMSのサポートに以下の制限があります。

- Barbican KMSはNetApp Storage Encryption（NSE）およびNetApp Aggregate Encryption（NAE）ではサポートされていません。代わりに、 "外部KMIP"または"オンボード キー マネージャー (OKM)" NSE および NVE キーの場合。
- Barbican KMS はMetroCluster構成ではサポートされていません。
- Barbican KMSはデータSVMに対してのみ設定できます。管理SVMでは使用できません。

特に記載がない限り、 `admin`特権レベルでは次の手順を実行できます。

開始する前に

- Barbican KMSとOpenStack Keystoneを設定する必要があります。Barbicanで使用するSVMは、BarbicanサーバーとOpenStack Keystoneサーバーへのネットワークアクセスが必要です。
- BarbicanおよびOpenStack Keystoneサーバーにカスタム認証局（CA）を使用している場合は、CA証明書を次のようにインストールする必要があります。 `security certificate install -type server-ca -vserver <admin_svm>` 。

Barbican KMS構成を作成してアクティブ化する

SVM に新しい Barbican KMS 構成を作成し、アクティブ化することができます。SVMには複数の非アクティブな Barbican KMS 構成を含めることができますが、一度にアクティブ化できるのは 1 つだけです。

手順

1. SVM の新しい非アクティブな Barbican KMS 構成を作成します。

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id`は、Barbican鍵暗号化鍵（KEK）の鍵識別子です。以下のURLを含む完全なURLを入力してください。 `https://` 。

> 一部のURLには疑問符（？）が含まれています。疑問符はONTAPコマンドラインのアクティブヘルプを起動します。クエスチョンマーク付きのURLを入力するには、まず、以下のコマンドでアクティブ・ヘルプを無効にする必要がある `set -active-help false`。アクティブ・ヘルプは、後でコマンド `set -active-help true`。"ONTAP コマンド リファレンス" 。

   - `-keystone-url` OpenStack Keystone認証ホストのURLです。 `https://` 。
   - `-application-cred-id`アプリケーション資格情報 ID です。

     このコマンドを入力すると、アプリケーション認証情報の秘密キーの入力を求められます。このコマンドは、非アクティブなBarbican KMS構成を作成します。

     次の例では、新しい非アクティブなBarbican KMS構成を作成します。 `config1` SVMの場合 `svm1` ：

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. 新しい Barbican KMS 構成をアクティブ化します。

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

このコマンドを使用すると、Barbican KMS構成を切り替えることができます。SVM上に既にアクティブなBarbican KMS構成がある場合は、その構成は非アクティブになり、新しい構成がアクティブになります。

3. 新しい Barbican KMS 構成がアクティブであることを確認します。

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

このコマンドは、SVMまたはノード上のアクティブなBarbican KMS構成のステータスを表示します。例えば、SVMが `svm1`ノード上 `node1`アクティブな Barbican KMS 構成がある場合、次のコマンドはその構成のステータスを返します。

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Barbican KMS構成の資格情報と設定を更新する

アクティブまたは非アクティブな Barbican KMS 構成の現在の設定を表示および更新できます。

手順

1. SVM の現在の Barbican KMS 構成を表示します。

```
security key-manager external barbican show -vserver <svm_name>
```

SVM 上の各 Barbican KMS 構成のキー ID、OpenStack Keystone URL、アプリケーション資格情報 ID が表示されます。

2. Barbican KMS 構成の設定を更新します。

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

このコマンドは、指定された Barbican KMS 構成のタイムアウトと検証設定を更新します。 `timeout` ONTAPがBarbicanからの応答を待つ時間を秒単位で指定します。この時間が過ぎると接続は失敗します。デフォルトは `timeout` 10秒です。 `verify`そして `verify-host`接続前にBarbicanホストのIDとホスト名を検証するかどうかを決定します。デフォルトでは、これらのパラメータは次のように設定されています。 `true` 。その `vserver`そして `config-name`パラメータは必須です。その他のパラメータはオプションです。

3. 必要に応じて、アクティブまたは非アクティブな Barbican KMS 構成の資格情報を更新します。

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

このコマンドを入力すると、新しいアプリケーション資格情報の秘密キーの入力を求められます。

4. 必要に応じて、アクティブな Barbican KMS 構成の不足している SVM キー暗号化キー (KEK) を復元します。
   a. 失われたSVM KEKを復元するには `security key-manager external barbican restore` ：

```
security key-manager external barbican restore -vserver <svm_name>
```

このコマンドは、Barbican サーバーと通信して、アクティブな Barbican KMS 構成の SVM KEK を復元します。

5. 必要に応じて、Barbican KMS 構成の SVM KEK のキーを再設定します。
   a. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

   b. SVM KEKを次のように再鍵化する。 `security key-manager external barbican rekey-internal` ：

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

このコマンドは、指定されたSVMの新しいSVM KEKを生成し、ボリューム暗号化キーを新しいSVM KEKで再ラップします。新しいSVM KEKは、アクティブなBarbican KMS構成によって保護されます。

Barbican KMSとオンボードキーマネージャー間でキーを移行する

Barbican KMSからOnboard Key Manager（OKM）へ、またその逆の方法で鍵を移行できます。OKMの詳細については、以下を参照してください。 "ONTAP 9 .6以降でオンボードキー管理を有効にする" 。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 必要に応じて、Barbican KMS から OKM にキーを移行します。

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` Barbican KMS 構成の SVM の名前です。

3. 必要に応じて、OKM から Barbican KMS にキーを移行します。

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Barbican KMS 構成を無効化して削除する

暗号化されたボリュームのないアクティブな Barbican KMS 構成を無効にしたり、非アクティブな Barbican KMS 構成を削除したりできます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. アクティブな Barbican KMS 構成を無効にします。

```
security key-manager keystore disable -vserver <svm_name>
```

SVMにNVE暗号化ボリュームが存在する場合は、それらを復号化するか、 キーを移行する Barbican KMS 構成を無効にする前に、次の手順に従ってください。新しい Barbican KMS 構成を有効にする場合、NVE ボリュームの復号化やキーの移行は不要であり、現在アクティブな Barbican KMS 構成は無効になります。

3. 非アクティブな Barbican KMS 構成を削除します。

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

ONTAP 9.6以降で**NVE**のオンボードキー管理を有効にする

オンボードキーマネージャを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager onboard sync`ます。

MetroCluster構成の場合は、同じパスフレーズを使用して最初にローカルクラスタでコマンドを実行してから、リモートクラスタでコマンドを実行する `security key-manager onboard sync`必要があります `security key-manager onboard enable`。ローカルクラスタからコマンドを実行したあとにリモートクラスタで同期する場合、 `security key-manager onboard enable`リモートクラスタからコマンドを再度実行する必要はありません `enable`。

詳細はこちら `security key-manager onboard enable`そして `security key-manager onboard sync`の中で"ONTAPコマンド リファレンス"。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。オプションを使用すると、リブート後にユーザにパスフレーズの入力を求めることができます `cc-mode-enabled=yes`。

NVEでは、を設定する `cc-mode-enabled=yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。で `volume create`は、を指定する必要はありません `-encrypt true`。で `volume move start`は、を指定する必要はありません `-encrypt-destination true`。

保存データの暗号化を設定する場合は、Commercial Solutions for Classified（CSfC）の要件を満たすために、NVEとNSEを使用し、オンボード キー マネージャがCommon Criteriaモードで有効にする必要があります。見る"CSfC 解決策 Brief （ CSfC の概要"。

オンボードキーマネージャがCCモードで有効になっ(`cc-mode-enabled=yes`ている場合）、システムの動作が次のように変更されます。

- システムは、情報セキュリティ国際評価基準モードで動作しているときに、クラスタパスフレーズの連続した失敗を監視します。

  クラスター パスフレーズの入力に 5 回失敗した場合は、24 時間待つか、ノードを再起動して制限をリセットします。

- システムイメージの更新では、通常のNetApp RSA-2048コード署名証明書とSHA-256コード署名ダイジェストの代わりに、NetApp RSA-3072コード署名証明書とSHA-384コード署名ダイジェストを使用してイメージの整合性をチェックします。

  アップグレード コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、または破損していないかを確認します。検証が成功した場合、システムはイメージ更新プロセスの次のステップに進みます。それ以外の場合、イメージの更新は失敗します。詳細はこちら `cluster image`の中で"ONTAPコマンド リファレンス"。

オンボード キー マネージャは揮発性メモリにキーを格納します。揮発性メモリの内容はシステムのリブート時または停止時にクリアされます。システムは停止すると 30 秒以内に揮発性メモリをクリアします。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster環境を設定する必要があります。

手順

1. キー管理ツールのセットアップを開始します。

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるように設定し `cc-mode-enabled=yes`ます。NVEでは、を設定する `cc-mode-enabled=yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。この `- cc-mode-enabled`オプションはMetroCluster構成ではサポートされません。`security key-manager onboard enable`コマンドは、コマンドに置き換わるもの `security key-manager setup`です。

2. 32 ～ 256 文字のパスフレーズを入力します。「cc-mode」の場合は 64 ～ 256 文字のパスフレーズを入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

   ```
   security key-manager key query -key-type NSE-AK
   ```

`security key-manager key query`コマンドは、コマンドに置き換わるもの `security key-manager query key`です。

の詳細については `security key-manager key query`、を"ONTAPコマンド リファレンス"参照してください。

5. オプションで、プレーン テキスト ボリュームを暗号化されたボリュームに変換できます。

   `volume encryption conversion start`

   ボリュームを変換する前に、オンボードキーマネージャの設定が完了している必要があります。MetroCluster環境では、両方のサイトでオンボードキーマネージャを設定する必要があります。

終了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーします。

オンボード キー マネージャーのパスフレーズを設定した後、その情報をストレージ システム外部の安全な場所に手動でバックアップします。見る"オンボードキー管理情報の手動でのバックアップ"。

関連情報

- "クラスターイメージコマンド"
- "セキュリティキーマネージャー外部有効化"
- "セキュリティキーマネージャーキークエリ"
- "セキュリティキーマネージャーオンボード有効化"

ONTAP 9.5以前で**NVE**のオンボードキー管理を有効にする

オンボードキーマネージャを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager setup`ます。

MetroCluster構成の場合は、次のガイドラインを確認してください。

- ONTAP 9 .5では、同じパスフレーズを使用してローカルクラスタと `security key-manager setup -sync-metrocluster-config yes`リモートクラスタでを実行する必要があります `security key-manager setup`。
- ONTAP 9を実行する前に、同じパスフレーズを使用してローカルクラスタでを実行し、20秒ほど待ってからリモートクラスタでを実行する `security key-manager setup`必要があります `security key-manager setup`。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができ `-enable-cc-mode yes`ます。

NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。で `volume create`は、を指定する必要はありません `-encrypt true`。で `volume move start`は、を指定する必要はありません `-encrypt-destination true`。

パスフレーズの入力に失敗した場合は、ノードを再起動する必要があります。

開始する前に

- NSE または NVE を外部キー管理 (KMIP) サーバーと共に使用している場合は、外部キー マネージャー データベースを削除します。

  "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボード キー マネージャを構成する前に、 MetroCluster環境を構成します。

手順

1. キー管理ツールのセットアップを開始します。

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにキー管理ツールのパスフレーズの入力を求めることができます `-enable-cc-mode yes`。NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。

   次の例では、リブートのたびにパスフレーズの入力を要求せずに、cluster1でキー管理ツールのセットアップを開始します。

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. オンボードキー管理を設定するかどうかを確認するプロンプトでと入力し `yes`ます。
3. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパ

スフレーズを「 cc-mode] 」に入力します。

> 指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

4. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
5. すべてのノードにキーが設定されていることを確認します。

   `security key-manager show-key-store`

   ```
   cluster1::> security key-manager show-key-store

   Node: node1
   Key Store: onboard
   Key ID                                                                   Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK

   Node: node2
   Key Store: onboard
   Key ID                                                                   Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK
   ```

   詳細はこちら `security key-manager show-key-store`の中で"ONTAPコマンド リファレンス"。

6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   `volume encryption conversion start`

   ボリュームを変換する前に、オンボード キー マネージャーを構成します。 MetroCluster環境では、両方のサイトで構成します。

終了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーします。

オンボード キー マネージャーのパスフレーズを構成するときは、災害に備えて、ストレージ システム外部の安全な場所に情報をバックアップしてください。見る"オンボードキー管理情報の手動でのバックアップ"。

関連情報

- "オンボードキー管理情報の手動でのバックアップ"
- "外部キー管理からオンボードキー管理への移行"

- "セキュリティ キー マネージャーのキー ストアの表示"

新しく追加された**ONTAP**ノードでオンボード キー管理を有効にする

オンボードキーマネージャを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

ONTAP 9 .6以降では、クラスタにノードを追加するたびにコマンドを実行する必要があります `security key-manager sync`。

ONTAP 9 .5以前の場合は、クラスタにノードを追加するたびにコマンドを実行する必要があります `security key-manager setup`。

オンボード キー管理を使用してクラスターにノードを追加する場合は、このコマンドを実行して、不足しているキーを更新します。

MetroCluster構成の場合は、次のガイドラインを確認してください。

- ONTAP 9 .6以降では、同じパスフレーズを使用してまずローカルクラスタでを実行し、次にリモートクラスタでを実行する `security key-manager onboard sync`必要があります `security key-manager onboard enable`。

  および `security key-manager onboard sync`の詳細については `security key-manager onboard enable`、を"ONTAPコマンド リファレンス"参照してください。

- ONTAP 9 .5では、同じパスフレーズを使用してローカルクラスタと `security key-manager setup -sync-metrocluster-config yes`リモートクラスタでを実行する必要があります `security key-manager setup`。
- ONTAP 9を実行する前に、同じパスフレーズを使用してローカルクラスタでを実行し、20秒ほど待ってからリモートクラスタでを実行する `security key-manager setup`必要があります `security key-manager setup`。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができ`-enable-cc-mode yes`ます。

NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。で `volume create`は、を指定する必要はありません `-encrypt true`。で `volume move start`は、を指定する必要はありません `-encrypt-destination true`。

パスフレーズの入力に失敗した場合は、ノードを再起動する必要があります。

関連情報

- "クラスターイメージコマンド"
- "セキュリティキーマネージャー外部有効化"

- "セキュリティキーマネージャーオンボード有効化"

NVE または NAE を使用してボリューム データを暗号化する

NVEを使用したONTAPボリュームデータの暗号化について学ぶ

ONTAP 9 .7以降では、VEライセンスがあり、オンボードまたは外部のキー管理を使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。ONTAP 9 .6以前では、新しいボリュームまたは既存のボリュームで暗号化を有効にできます。ボリューム暗号化を有効にする前に、VEライセンスをインストールし、キー管理を有効にしておく必要があります。NVEはFIPS-140-2レベル1に準拠しています。

ONTAPでVEライセンスを使用してアグリゲートレベルの暗号化を有効にする

ONTAP 9 .7以降では"VEライセンス"、およびオンボードまたは外部のキー管理を使用している場合、新しく作成したアグリゲートとボリュームはデフォルトで暗号化されます。ONTAP 9 6以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。

タスクの内容

アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。そうしないと、NVEでアグリゲートレベルの重複排除がサポートされません。

アグリゲートレベルの暗号化が有効になっているアグリゲートは、 _NAE アグリゲートと呼ばれます（ NetApp Aggregate Encryption の場合）。NAEアグリゲート内のすべてのボリュームは、NAEまたはNVE暗号化で暗号化する必要があります。アグリゲートレベルの暗号化では、アグリゲート内に作成するボリュームはデフォルトでNAE暗号化で暗号化されます。デフォルトを上書きしてNVE暗号化を使用することもできます。

NAEアグリゲートではプレーンテキストボリュームはサポートされません。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. アグリゲートレベルの暗号化を有効または無効にします。

目的	使用するコマンド
ONTAP 9 .7以降でNAEアグリゲートを作成する	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
ONTAP 9 .6を使用してNAEアグリゲートを作成します。	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

NAE以外のアグリゲートをNAEアグリゲートに変換する	`storage aggregate modify -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key true`
NAEアグリゲートをNAE以外のアグリゲートに変換する	`storage aggregate modify -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key false`

詳細はこちら `storage aggregate modify`の中で"ONTAPコマンド リファレンス" 。

次のコマンドは、でアグリゲートレベルの暗号化を有効にし `aggr1`ます。

- ONTAP 9 .7以降：

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9 .6以前：

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

の詳細については `storage aggregate create`、を"ONTAPコマンド リファレンス"参照してください。

2. アグリゲートで暗号化が有効になっていることを確認します。

`storage aggregate show -fields encrypt-with-aggr-key`

次のコマンドは、暗号化が有効になっていることを確認し `aggr1`ます。

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

の詳細については `storage aggregate show`、を"ONTAPコマンド リファレンス"参照してください。

終了後

コマンドを実行し `volume create`て暗号化されたボリュームを作成します。

ノードの暗号化キーを保存するために KMIP サーバを使用している場合、ボリュームを暗号化すると、ONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

コマンドを使用すると、新しいボリュームで暗号化を有効にできます `volume create`。

タスクの内容

ボリュームは、NetApp Volume Encryption（NVE）およびONTAP 9 .6以降のNetApp Aggregate Encryption（NAE）を使用して暗号化できます。NAEおよびNVEの詳細については、を参照してボリューム暗号化の概要ください。

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

ONTAPの新しいボリュームで暗号化を有効にする手順は、使用しているONTAPのバージョンと特定の構成によって異なります。

- ONTAP 9 4以降では、オンボードキーマネージャのセットアップ時にを有効にした場合、 `cc-mode`コマンドで作成するボリュームは `volume create`、指定したかどうかに関係なく自動的に暗号化され`-encrypt true`ます。
- ONTAP 9 .6以前のリリースでは、コマンドを指定して `volume create`暗号化を有効にする必要があります `-encrypt true`（有効にしていない場合 `cc-mode`）。
- ONTAP 9でNAEボリュームを作成する場合は、アグリゲートレベルでNAEを有効にする必要があります。6このタスクの詳細については、を参照してくださいVEライセンスでアグリゲートレベルの暗号化を有効にします。
- ONTAP 9 .7以降では"VEライセンス"、およびオンボードまたは外部キー管理を使用している場合、新しく作成したボリュームはデフォルトで暗号化されます。NAEアグリゲート内に作成される新しいボリュームのタイプは、デフォルトではNVEではなくNAEになります。
  - ONTAP 9 .7以降のリリースでは、コマンドに `volume create`を追加してNAEアグリゲートにボリュームを作成すると、 `-encrypt true`そのボリュームではNAEではなくNVE暗号化が使用されます。NAEアグリゲート内のすべてのボリュームは、NVEまたはNAEで暗号化する必要があります。

NAEアグリゲートではプレーンテキストボリュームはサポートされません。

手順

1. 新しいボリュームを作成し、そのボリュームで暗号化を有効にするかどうかを指定します。新しいボリュームがNAEアグリゲートに配置する場合、デフォルトでNAEで暗号化されます。

作成対象	使用するコマンド
NAEボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

NVEボリューム	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true+` NAEがサポートされないONTAP 9 .6以前では、 `-encrypt true` ボリュームをNVEで暗号化するように指定します。NAEアグリゲートにボリュームが作成されるONTAP 9 .7以降では、 `-encrypt true`デフォルトの暗号化タイプであるNAEよりも優先されてNVEボリュームが作成されます。
プレーンテキストボリューム	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false`

の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

2. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

結果

ノードの暗号化キーの格納にKMIPサーバを使用している場合は、ボリュームを暗号化するときにONTAPからサーバに暗号化キーが自動的に「プッシュ」されます。

既存の**ONTAP**ボリュームで **NAE** または **NVE** を有効にする

既存のボリュームで暗号化を有効にするには、コマンドまたは `volume encryption conversion start`コマンドを使用し `volume move start`ます。

タスクの内容

使用することができます `volume encryption conversion start`既存のボリュームを別の場所に移動することなく、その場で暗号化を有効にするコマンドです。あるいは、 `volume move start`指示。

volume encryption conversion startコマンドを使用して、既存のボリュームで暗号化を有効にする

使用することができます `volume encryption conversion start`ボリュームを別の場所に移動しなくても、既存のボリュームの暗号化を「その場で」有効にするコマンドです。

変換処理を開始したら、完了する必要があります。処理中にパフォーマンスの問題が発生した場合は、コマンドを実行して処理を一時停止し、 `volume encryption conversion resume`コマンドを実行して処理を再開できます `volume encryption conversion pause`。

SnapLockボリュームの変換にはを使用できません `volume encryption conversion start`。

手順

1. 既存のボリュームで暗号化を有効にします。

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

の詳細については `volume encryption conversion start`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、既存のボリュームで暗号化を有効にし `vol1`ます。

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

ボリュームの暗号化キーが作成されます。ボリュームのデータが暗号化されます。

2. 変換処理のステータスを確認します。

```
volume encryption conversion show
```

の詳細については `volume encryption conversion show`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、変換処理のステータスを表示します。

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ----------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. 変換処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State   Type  Size  Available  Used
-------  ------  ---------  -----   ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

結果

ノードの暗号化キーを保存するために KMIP サーバを使用している場合、ボリュームを暗号化すると、ONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

volume move startコマンドを使用して既存のボリュームで暗号化を有効にする

コマンドを使用すると、既存のボリュームを移動して暗号化を有効にできます `volume move start`。使用するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

- ONTAP 9 .8以降では、を使用してSnapLockまたはFlexGroupのボリュームで暗号化を有効にでき `volume move start`ます。
- ONTAP 9 .4以降では、オンボードキーマネージャのセットアップ時に「cc-mode」を有効にすると、コマンドで作成するボリュームが自動的に暗号化されます `volume move start`。指定する必要はありません `-encrypt-destination true`。
- ONTAP 9 6以降では、アグリゲートレベルの暗号化を使用して、移動するボリュームの包含アグリゲートにキーを割り当てることができます。一意のキーで暗号化されたボリュームは、_NVEボリューム_と呼ばれます（NetAppボリューム暗号化を使用することを意味します）。アグリゲートレベルのキーで暗号化されたボリュームは、 _NAE ボリューム（ NetApp Aggregate Encryption の場合）と呼ばれます。NAEアグリゲートではプレーンテキストボリュームはサポートされません。
- ONTAP 9 14.1以降では、NVEを使用してSVMルートボリュームを暗号化できます。詳細については、を参照してください SVMルートボリュームでのNetAppボリューム暗号化の設定。

開始する前に

このタスクを実行するには、クラスタ管理者であるか、クラスタ管理者から権限を委譲されたSVM管理者である必要があります。

"volume moveコマンドの実行権限の委譲"

手順

1. 既存のボリュームを移動し、そのボリュームで暗号化を有効にするかどうかを指定します。

変換対象	使用するコマンド
プレーンテキストボリュームからNVEボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
NVEボリュームまたはプレーンテキストボリュームからNAEボリューム（デスティネーションでアグリゲートレベルの暗号化が有効になっている場合）	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
NAEボリュームからNVEボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
NAEボリュームからプレーンテキスト ボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`

NVEボリュームからプレーンテキストボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

の詳細については `volume move start`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、という名前のプレーンテキストボリュームをNVEボリュームに変換し `vol1`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

次のコマンドは、デスティネーションでアグリゲートレベルの暗号化が有効になっている場合に、という名前のNVEボリュームまたはプレーンテキストボリュームをNAEボリュームに変換し `vol1`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

次のコマンドは、という名前のNAEボリュームをNVEボリュームに変換し `vol2`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

次のコマンドは、という名前のNAEボリュームをプレーンテキストボリュームに変換し `vol2`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

次のコマンドは、という名前のNVEボリュームをプレーンテキストボリュームに変換し `vol2`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. クラスタボリュームの暗号化タイプを表示します。

   `volume show -fields encryption-type none|volume|aggregate`

   この `encryption-type`フィールドは、ONTAP 9 .6以降で使用できます。

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、のボリュームの暗号化タイプを表示します `cluster2`。

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster2`ます。

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

結果

ノードの暗号化キーの格納にKMIPサーバを使用している場合、ボリュームの暗号化時にONTAPからサーバに暗号化キーが自動的にプッシュされます。

ONTAP SVMルートボリュームにNVEを設定する

ONTAP 9 14.1以降では、Storage VM（SVM）のルートボリュームでNetApp Volume Encryption（NVE）を有効にすることができます。NVEでは、ルートボリュームが一意のキーで暗号化されるため、SVMのセキュリティが向上します。

タスクの内容

SVMルートボリューム上のNVEは、SVMの作成後にのみ有効にできます。

開始する前に

- NetAppアグリゲート暗号化（NAE）で暗号化されたアグリゲートにSVMルートボリュームを配置しないでください。
- オンボードキーマネージャまたは外部キーマネージャを使用した暗号化を有効にしておく必要があります。
- ONTAP 9.14.1以降が実行されている必要があります。
- NVEで暗号化されたルート ボリュームが含まれるSVMを移行するには、移行の完了後にSVMルート ボリュームをプレーンテキスト ボリュームに変換したうえで、再度SVMルート ボリュームを暗号化する必要があります。

- SVM移行のデスティネーション アグリゲートでNAEを使用する場合、ルート ボリュームはデフォルトでNAEを継承します。

- SVMがSVMディザスタ リカバリ関係に含まれる場合、次のことに注意してください。
  - ミラーされたSVMの暗号化設定は、デスティネーションにコピーされません。ソースまたはデスティネーションでNVEを有効にする場合は、ミラーされたSVMルート ボリュームで個別にNVEを有効にする必要があります。
  - デスティネーション クラスタ内のすべてのアグリゲートでNAEが使用される場合、SVMルート ボリュームでもNAEが使用されます。

手順

ONTAP CLIまたはSystem Managerを使用して、SVMルートボリュームでNVEを有効にできます。

CLI

NVEは、SVMルートボリュームでインプレースで有効にすることも、アグリゲート間でボリュームを移動することによって有効にすることもできます。

ルートボリュームをインプレースで暗号化

1. ルートボリュームを暗号化されたボリュームに変換します。

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 暗号化が成功したことを確認しますには `volume show -encryption-type volume`、NVEを使用しているすべてのボリュームのリストが表示されます。

SVMルートボリュームの移動による暗号化

1. ボリュームの移動を開始します。

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   の詳細については `volume move`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用して、処理が成功した `volume move show`ことを確認します `volume move`。には `volume show -encryption-type volume`、NVEを使用しているすべてのボリュームのリストが表示されます。

System Manager

1. ストレージ>ボリュームに移動します。
2. 暗号化するSVMルートボリュームの名前の横にある[Edit]**を選択します ⋮ 。
3. [**Storage and Optimization*]**見出しで、**[** Enable encryption*]を選択します。
4. 保存を選択します。

ONTAPノードのルートボリュームに**NVE**を構成する

ONTAP 9 8以降では、NetAppボリューム暗号化を使用してノードのルートボリュームを保護できます。

タスクの内容

この手順はノードのルートボリュームに適用されます。SVMルートボリュームには適用されません。SVMルートボリュームは、アグリゲートレベルの暗号化およびで保護できますONTAP 9.14.1以降、NVE。

ルートボリュームの暗号化は、開始後に完了する必要があります。処理を一時停止することはできません。暗号化が完了すると、ルート ボリュームに新しいキーを割り当てられなくなるほか、セキュア パージ処理を実行できなくなります。

開始する前に

- システムでHA構成を使用している必要があります。
- ノードのルートボリュームを作成しておく必要があります。
- オンボードキーマネージャまたはKey Management Interoperability Protocol（KMIP）を使用する外部キー管理サーバがシステムに搭載されている必要があります。

手順

1. ルートボリュームを暗号化します。

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 変換処理のステータスを確認します。

   ```
   volume encryption conversion show
   ```

3. 変換処理が完了したら、ボリュームが暗号化されていることを確認します。

   ```
   volume show -fields
   ```

   次に、暗号化されたボリュームの出力例を示します。

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

NetAppハードウェアベースの暗号化の設定

ONTAPハードウェアベースの暗号化について学ぶ

NetAppのハードウェアベースの暗号化では、データの書き込み時のフルディスク暗号化（FDE）がサポートされます。ファームウェアに保存されている暗号化キーがないとデータを読み取ることはできません。暗号化キーには、認証されたノードだけがアクセスできます。

NetAppハードウェアベースの暗号化の概要

ノードは、外部キー管理サーバまたはオンボードキーマネージャから取得した認証キーを使用して自己暗号化ドライブへの認証を行います。

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

NetApp Volume Encryption をハードウェアベースの暗号化とともに使用すると、自己暗号化ドライブのデータを「暗号化」できます。

自己暗号化ドライブが有効な場合は、コアダンプも暗号化されます。

HAペアで暗号化SASドライブまたはNVMeドライブ（SED、NSE、FIPS）を使用している場合は、システムを初期化する前に、HAペア内のすべてのドライブに関連するトピックの手順に従う必要がありますFIPSドライブまたはSEDを非保護モードに戻す（ブートオプション4または9）。これを行わないと、ドライブを転用した場合にデータが失われる可能性があります。

サポートされている自己暗号化ドライブのタイプ

2種類の自己暗号化ドライブがサポートされています。

- すべてのFASシステムおよびAFFシステムで、自己暗号化機能を備えたFIPS認定のSASドライブまたはNVMeドライブがサポートされます。これらのドライブは _FIPS ドライブと呼ばれ、 Federal Information Processing Standard Publication 140-2 レベル 2 の要件に準拠しています。認定された機能により、ドライブに対するサービス拒否攻撃の防止など、暗号化に加えて保護も可能になります。FIPSドライブは、同じノードまたはHAペアで他のタイプのドライブと混在させることはできません。
- ONTAP 9 .6以降では、FIPSテストが完了していない自己暗号化NVMeドライブがAFF A800、A320、およびそれ以降のシステムでサポートされます。これらのドライブは_SED _と呼ばれ、FIPSドライブと同じ暗号化機能を提供しますが、同じノードまたはHAペアで非暗号化ドライブと混在させることもできます。
- FIPS検証済みドライブはすべて、FIPS検証済みのファームウェア暗号化モジュールを使用します。FIPSドライブ暗号化モジュールは、ドライブ外で生成されたキーを使用しません（ドライブに入力された認証パスフレーズは、ドライブのファームウェア暗号化モジュールがキー暗号化キーを取得するために使用されます）。

非暗号化ドライブは、SEDまたはFIPSドライブではないドライブです。

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

外部キー管理を使用する状況

オンボード キー マネージャを使用した方がコストもかからず一般的には便利ですが、次のいずれかに当てはまる場合は外部キー管理を使用する必要があります。

- 組織のポリシーで、FIPS 140-2レベル2（以上）の暗号化モジュールを使用するキー管理ソリューション

が求められる場合。

- 暗号化キーを一元管理できるマルチクラスタソリューションが必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

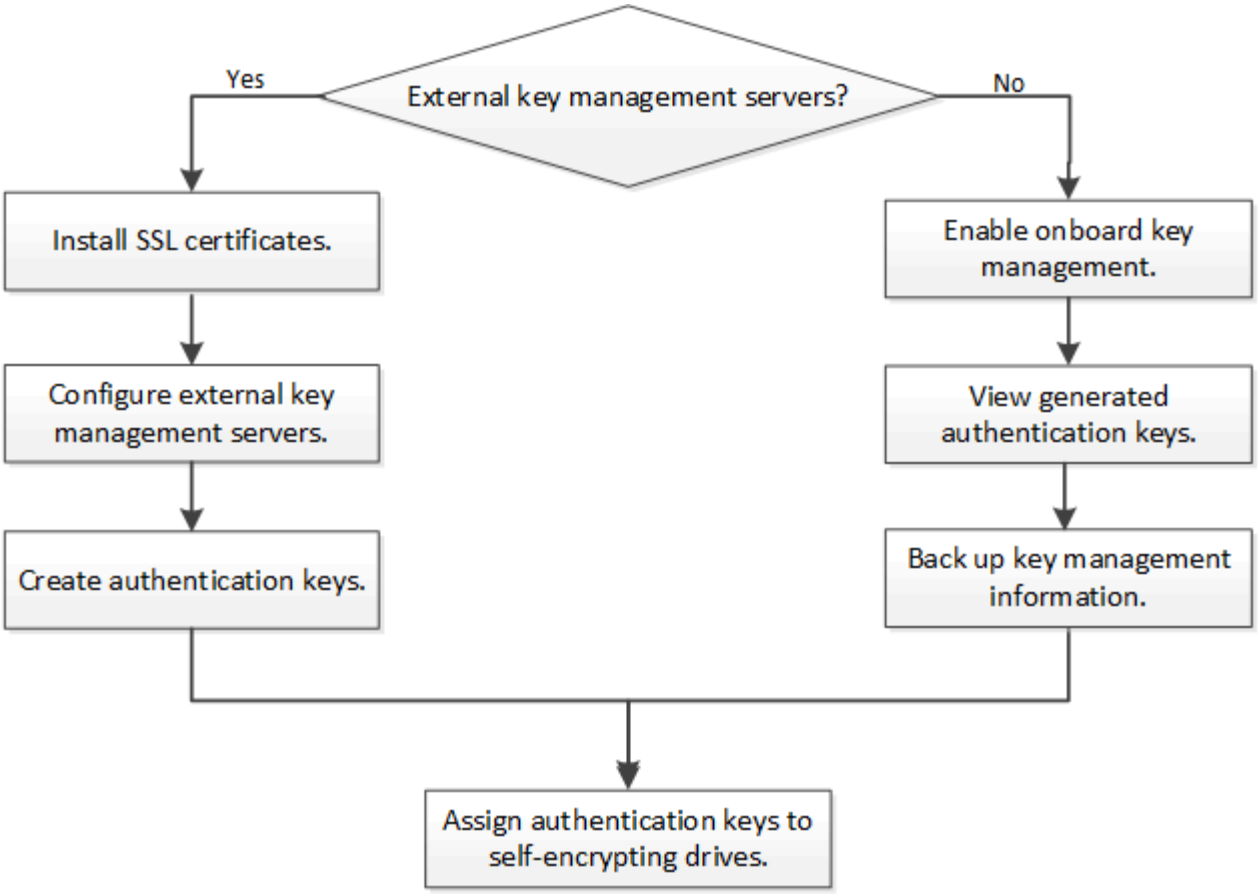
サポートの詳細

次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポート対象のKMIPサーバ、ストレージ システム、ディスク シェルフの最新情報については、Interoperability Matrixを参照してください。

リソースまたは機能	サポートの詳細
異なるタイプのディスクの混在	• FIPSドライブは、同じノードまたはHAペアで他のタイプのドライブと混在させることはできません。準拠したHAペアと準拠していないHAペアを同じクラスタに共存させることは可能です。 • SEDは、同じノードまたはHAペアで非暗号化ドライブと混在させることができます。
ドライブ タイプ	• FIPSドライブには、SASドライブまたはNVMeドライブを使用できます。 • SEDは、NVMeドライブである必要があります。
10Gbネットワーク インターフェイス	ONTAP 9.3以降では、KMIPを使用したキー管理の設定で外部キー管理サーバとの通信に10Gbネットワーク インターフェイスがサポートされます。
キー管理サーバとの通信用のポート	ONTAP 9.3以降では、任意のストレージ コントローラ ポートを使用してキー管理サーバと通信できます。それ以外の場合は、キー管理サーバとの通信にポートe0Mを使用する必要があります。ストレージ コントローラのモデルによっては、ブート プロセス時に一部のネットワーク インターフェイスをキー管理サーバとの通信に使用できない場合があります。
MetroCluster（MCC）	• NVMeドライブではMCCがサポートされます。 • SASドライブではMCCがサポートされません。

ハードウェアベースの暗号化のワークフロー

自己暗号化ドライブに対してクラスタを認証するには、キー管理サービスを設定する必要があります。外部キー管理サーバまたはオンボード キー マネージャを使用できます。



関連情報

- "NetApp Hardware Universe"
- "NetAppボリューム暗号化とNetAppアグリゲート暗号化"

外部キー管理の設定

ONTAP外部キー管理の設定について学ぶ

1つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを保護できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードにキーを提供します。

オンボードキーマネージャを使用してNetApp Volume Encryption（NVE）を実装できます。ONTAP 9.3以降では、NVEを外部キー管理（KMIP）とオンボードキーマネージャで実装できます。ONTAP 9.11.1以降では、クラスタに複数の外部キー管理ツールを設定できます。を参照し クラスタ化されたキーサーバを設定

ONTAPクラスタにSSL証明書をインストールする

クラスタとKMIPサーバは、KMIP SSL証明書を使用して相互のIDを検証し、SSL接続を確立します。KMIPサーバとのSSL接続を設定する前に、クラスタのKMIPクライアントSSL証明書、およびKMIPサーバのルート認証局（CA）のSSLパブリック証明書をインストールする必要があります。

タスクの内容

HAペアでは、両方のノードで同じSSL KMIPパブリック証明書とプライベート証明書を使用する必要があります。複数のHAペアを同じKMIPサーバに接続する場合は、HAペアのすべてのノードで同じSSL KMIPパブリック証明書とプライベート証明書を使用する必要があります。

開始する前に

- 証明書を作成するサーバ、KMIPサーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリックSSL KMIPクライアント証明書を入手しておく必要があります。
- クラスタのSSL KMIPクライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIPクライアント証明書はパスワードで保護しないでください。
- KMIPサーバのルート認証局（CA）のSSLパブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

KMIPサーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前後どちらでも実行できます。

手順

1. クラスタのSSL KMIPクライアント証明書をインストールします。

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   SSL KMIPのパブリック証明書とプライベート証明書を入力するように求められます。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. KMIPサーバのルート認証局（CA）のSSLパブリック証明書をインストールします。

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

関連情報

- "セキュリティ証明書のインストール"

ONTAP 9.6以降でハードウェアベースの暗号化の外部キー管理を有効にする

1つ以上のKMIPサーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1つのノードに最大4つのKMIPサーバを接続できます。冗長性とディザスタリカバリのために、少なくとも2台のサーバが推奨されます。

ONTAP 9 .11.1以降では、プライマリキーサーバごとに最大3つのセカンダリキーサーバを追加してクラスタ化されたキーサーバを作成できます。詳細については、を参照してください クラスタ化された外部キーサーバの設定。

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。

- このタスクを実行するには、クラスタ管理者である必要があります。
- MetroCluster環境の場合:
  - 外部キー管理ツールを設定する前に、MetroCluster環境を設定する必要があります。
  - 両方のクラスターに同じ KMIP SSL 証明書をインストールする必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

> ℹ
> - `security key-manager external enable`コマンドは、コマンドに置き換わるもの `security key-manager setup`です。外部キー管理の設定を変更するには、コマンドを実行し `security key-manager external modify`ます。の詳細については `security key-manager external enable`、を"ONTAPコマンドリファレンス"参照してください。
> - MetroCluster環境で管理SVMに外部キー管理を設定する場合は、パートナークラスタでこのコマンドを繰り返す必要があります `security key-manager external enable`。

次のコマンドは、3台の外部キーサーバでの外部キー管理を有効にします `cluster1`。1つ目のキーサーバはホスト名とポートを使用して指定し、2つ目のキーサーバはIPアドレスとデフォルトポートを使用して指定し、3つ目のキーサーバはIPv6アドレスとポートを使用して指定します。

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 設定したすべてのKMIPサーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

> ℹ
> `security key-manager external show-status`コマンドは、コマンドに置き換わるもの `security key-manager show -status`です。の詳細については `security key-manager external show-status`、をlink:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAPコマンド リファレンス"^]参照してください。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

関連情報

- クラスタ化された外部キーサーバの設定
- "セキュリティキーマネージャーの外部有効化"
- "セキュリティキーマネージャーの外部ステータス表示"

ONTAP 9.5以前でハードウェアベースの暗号化の外部キー管理を有効にする

1つ以上のKMIPサーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1つのノードに最大4つのKMIPサーバを接続できます。冗長性とディザスタリカバリのために、少なくとも2台のサーバが推奨されます。

タスクの内容

ONTAPでは、クラスタ内のすべてのノードに対してKMIPサーバの接続が設定されます。

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster環境を設定する必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタノードのキー管理ツールの接続を設定します。

   ```
   security key-manager setup
   ```

   キー管理ツールのセットアップが開始されます。

MetroCluster環境では、このコマンドを両方のクラスタで実行する必要があります。詳細はこちら `security key-manager setup`の中で"ONTAPコマンド リファレンス"。

2. 各プロンプトで適切な応答を入力します。
3. KMIPサーバを追加します。

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   MetroCluster環境の場合は、両方のクラスタでこのコマンドを実行する必要があります。

4. 冗長性を確保するためにKMIPサーバを追加します。

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   MetroCluster環境の場合は、両方のクラスタでこのコマンドを実行する必要があります。

5. 設定したすべてのKMIPサーバが接続されていることを確認します。

   `security key-manager show -status`

   この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス" 。

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   `volume encryption conversion start`

   ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

ONTAP 9.11.1以降では、SVMのクラスタ化された外部キー管理サーバへの接続を設定できます。クラスタ化されたキーサーバでは、SVMのプライマリキーサーバとセカンダリキーサーバを指定できます。キーを登録するとき、ONTAPは最初にプライマリキーサーバへのアクセスを試行してから、処理が正常に完了するまでセカンダリサーバへのアクセスを順次試行し、キーの重複を防止します。

外部キー サーバは、NSE、NVE、NAE、SEDの各キーに使用できます。1台のSVMに最大4台の外部プライマリKMIPサーバを指定できます。各プライマリ サーバには、最大3台のセカンダリ キー サーバを指定できます。

開始する前に

- "SVMでKMIPキー管理が有効になっている必要があります。"です。
- このプロセスでは、KMIPを使用するキーサーバのみがサポートされます。サポートされているキーサーバのリストについては、を参照してください"NetApp Interoperability Matrix Tool"。
- クラスタ内のすべてのノードでONTAP 9 .11.1以降が実行されている必要があります。
- パラメータ内のserversリストの引数の順序 `-secondary-key-servers`は、外部キー管理（KMIP）サーバのアクセス順序を反映しています。
- この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

クラスタ化されたキーサーバを作成する

設定手順は、プライマリキーサーバが設定されているかどうかによって異なります。

SVMにプライマリキーサーバとセカンダリキーサーバを追加する

1. クラスタでキー管理が有効になっていないことを確認します。
   `security key-manager external show -vserver *svm_name*`SVMですでに最大4つのプライマリキーサーバが有効になっている場合は、新しいプライマリキーサーバを追加する前に既存のいずれかを削除する必要があります。
2. プライマリキー管理ツールを有効にします。
   `security key-manager external enable -vserver *svm_name* -key-servers *server_ip* -client-cert *client_cert_name* -server-ca-certs *server_ca_cert_names*`
3. プライマリキーサーバを変更してセカンダリキーサーバを追加します。 `-secondary-key-servers`パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver *svm_name* -key-servers *primary_key_server* -secondary-key-servers *list_of_key_servers*`

既存のプライマリキーサーバにセカンダリキーサーバを追加する

1. プライマリキーサーバを変更してセカンダリキーサーバを追加します。 `-secondary-key-servers`パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver *svm_name* -key-servers *primary_key_server* -secondary-key-servers *list_of_key_servers*`セカンダリキーサーバの詳細については、を参照してください[mod-secondary]。

クラスタ化されたキーサーバの変更

外部キーサーバクラスタを変更するには、特定のキーサーバのステータス（プライマリまたはセカンダリ）を変更したり、セカンダリキーサーバを追加および削除したり、セカンダリキーサーバのアクセス順序を変更したりします。

プライマリキーサーバとセカンダリキーサーバの変換

プライマリキーサーバをセカンダリキーサーバに変換するには、まずコマンドを使用してそのサーバをSVMから削除する必要があります `security key-manager external remove-servers`。

セカンダリキーサーバをプライマリキーサーバに変換するには、まず既存のプライマリキーサーバからセカンダリキーサーバを削除する必要があります。を参照して [mod-secondary]既存のキーを削除するときにセカンダリキーサーバをプライマリサーバに変換すると、削除と変換を完了する前に新しいサーバを追加しようとすると、キーが重複することがあります。

セカンダリキーサーバを変更します。

セカンダリキーサーバの管理には、コマンドのパラメータを `security key-manager external modify-server`使用し `-secondary-key-servers`ます。 `-secondary-key-servers`パラメータには、カンマで区切ったリストを指定できます。リスト内のセカンダリキーサーバの指定した順序によって、セカンダリキーサーバのアクセス順序が決まります。アクセス順序を変更するには、セカンダリキーサーバを別の順序で入力してコマンドを実行し `security key-manager external modify-server`ます。

セカンダリキーサーバを削除するには、 `-secondary-key-servers`削除するキーサーバを省略して保持するキーサーバを引数に含める必要があります。すべてのセカンダリキーサーバを削除するには、引数（なし）を使用し `-`ます。

関連情報

- "セキュリティキーマネージャー外部"

ONTAP 9 .6以降で認証キーを作成する

コマンドを使用して、ノードの認証キーを作成し、設定したKMIPサーバに格納できます `security key-manager key create`。

タスクの内容

セキュリティの設定でデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれに別々 のキーを作成する必要があります。そうでない場合は、FIPSへの準拠にデータアクセスと同じ認証キーを使用できます。

ONTAPでは、クラスタ内のすべてのノードの認証キーが作成されます。

- このコマンドは、オンボードキーマネージャが有効になっている場合はサポートされません。ただし、オンボードキーマネージャを有効にすると、2つの認証キーが自動的に作成されます。キーを表示するには、次のコマンドを使用します。

```
security key-manager key query -key-type NSE-AK
```

- 設定済みのキー管理サーバにすでに128個を超える認証キーが格納されている場合は警告が表示されます。
- コマンドを使用すると、使用されていないキーを削除できます `security key-manager key delete`。 `security key-manager key delete`指定したキーがONTAPで現在使用されている場合、コマンドは失敗します。（このコマンドを使用するには、より大きいPrivilegesが必要です `admin`）。

> MetroCluster環境でキーを削除する前に、そのキーがパートナークラスタで使用されていないことを確認する必要があります。パートナークラスタで次のコマンドを使用して、キーが使用されていないことを確認できます。
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

を設定する `prompt-for-key=true`と、暗号化されたドライブを認証するときに、クラスタ管理者に使用するパスフレーズの入力を求めるプロンプトが表示されます。それ以外の場合は、32バイトのパスフレーズが自動的に生成されます。 `security key-manager key create`コマンドは、コマンドに置き換わるもの `security key-manager create-key`です。の詳細については `security key-manager key create`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、の認証キーを作成し `cluster1`、32バイトのパスフレーズを自動的に生成します。

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 認証キーが作成されたことを確認します。

```
security key-manager key query -node node
```

`security key-manager key query`コマンドは、コマンドに置き換わるもの `security key-manager query key`です。

出力に表示されるキーIDは、認証キーの参照に使用する識別子です。実際の認証キーまたはデータ暗号化キーではありません。

次の例では、の認証キーが作成されたことを確認し `cluster1`ます。

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

の詳細については `security key-manager key query`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "storage disk show | more"

ONTAP 9 .5以前で認証キーを作成する

コマンドを使用して、ノードの認証キーを作成し、設定したKMIPサーバに格納できます `security key-manager create-key`。

タスクの内容

セキュリティの設定でデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれに別々 のキーを作成する必要があります。そうでない場合は、FIPS準拠の認証キーをデータアクセスと同じにして使用できます。

ONTAPでは、クラスタ内のすべてのノードの認証キーが作成されます。

- このコマンドは、オンボードキー管理が有効になっている場合はサポートされません。
- 設定済みのキー管理サーバにすでに128個を超える認証キーが格納されている場合は警告が表示されます。

  キー管理サーバソフトウェアを使用して未使用のキーを削除してから、コマンドをもう一度実行します。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

   `security key-manager create-key`

   の詳細については `security key-manager create-key`、を"ONTAPコマンド リファレンス"参照してください。

   出力に表示されるキーIDは、認証キーの参照に使用する識別子です。実際の認証キーまたはデータ暗号化キーではありません。

   次の例は、の認証キーを作成し `cluster1`ます。

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 認証キーが作成されたことを確認します。

   `security key-manager query`

   の詳細については `security key-manager query`、を"ONTAPコマンド リファレンス"参照してください。

   次の例では、の認証キーが作成されたことを確認し `cluster1`ます。

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

ONTAP外部キー管理を使用して**FIPS**ドライブまたは**SED**にデータ認証キーを割り当てる

コマンドを使用して、FIPSドライブまたはSEDにデータ認証キーを割り当てることができます `storage encryption disk modify`。このキーは、クラスタノードでドライブ上の暗号化されたデータをロックまたはロック解除するときに使用します。

タスクの内容

自己暗号化ドライブは、認証キーIDがデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。SASドライブの標準のデフォルト値は、キーIDが0x0のManufacturer Secure ID（MSID；メーカーのセキュアID）です。NVMeドライブの場合、標準のデフォルト値はnullキーで、空のキーIDで表されます。このキーIDを自己暗号化ドライブに割り当てると、認証キーIDがデフォルト以外の値に変更されます。

この手順はシステムの停止を伴いません。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   の詳細については `storage encryption disk modify`、を"ONTAPコマンド リファレンス"参照して

ください。

> キーIDは、コマンドを使用して表示できます `security key-manager query -key -type NSE-AK`。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

関連情報

- "storage disk show | more"
- "ストレージ暗号化ディスクステータス表示"

オンボードキー管理の設定

ONTAP 9 .6以降でオンボードキー管理を有効にする

オンボードキーマネージャを使用して、クラスタノードをFIPSドライブまたはSEDに対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャはFIPS-140-2レベル1に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager onboard enable`ます。MetroCluster構成では、同じパスフレーズを使用してまずローカルクラスタでを実行し、次にリモートクラスタでを実行する `security key-manager onboard sync`必要があります `security key-manager onboard enable`。

詳細はこちら `security key-manager onboard enable`そして `security key-manager onboard sync`の中で"ONTAPコマンド リファレンス"。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。MetroClusterの場合を除き、オプションを使用すると、リブート後にユーザにパスフレーズの入力を求めることができます `cc-mode-enabled=yes`。

> オンボードキーマネージャがCCモードで有効になっ(`cc-mode-enabled=yes`ている場合）、システムの動作が次のように変更されます。
>
> - システムは、情報セキュリティ国際評価基準モードで動作しているときに、クラスタパスフレーズの連続した失敗を監視します。
>
> NetAppストレージ暗号化（NSE）が有効になっている場合にブート時に正しいクラスタパスフレーズを入力しないと、システムはドライブを認証できず、自動的にリブートします。これを修正するには、ブートプロンプトで正しいクラスタパスフレーズを入力する必要があります。ブート後、クラスタパスフレーズをパラメータとして必要とするコマンドについては、24時間以内に最大5回連続してクラスタパスフレーズを正しく入力できます。制限に達した場合（クラスタパスフレーズを5回連続で正しく入力しなかった場合など）は、24時間のタイムアウト時間が経過するまで待つか、ノードをリブートして制限をリセットする必要があります。
>
> - システムイメージの更新では、通常のNetApp RSA-2048コード署名証明書とSHA-256コード署名ダイジェストの代わりに、NetApp RSA-3072コード署名証明書とSHA-384コード署名ダイジェストを使用してイメージの整合性をチェックします。
>
> アップグレード コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、または破損していないかを確認します。検証が成功すると、イメージの更新は次のステップに進みます。検証が機能しない場合、イメージの更新は失敗します。詳細はこちら `cluster image`の中で"ONTAPコマンド リファレンス"。

> オンボードキーマネージャは、キーを揮発性メモリに格納します。揮発性メモリの内容は、システムを再起動または停止するとクリアされます。通常の動作状態では、システムが停止すると、揮発性メモリの内容は30秒以内に消去されます。

開始する前に

- NSEで外部キー管理（KMIP）サーバを使用する場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

  "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster環境を設定する必要があります。

手順

1. キー管理ツールのsetupコマンドを開始します。

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   > リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるように設定し `cc-mode-enabled=yes`ます。この `- cc-mode-enabled`オプションはMetroCluster構成ではサポートされません。 `security key-manager onboard enable`コマンドは、コマンドに置き換わるもの `security key-manager setup`です。

   次の例は、リブートのたびにパスフレーズの入力を要求せずに、cluster1でkey manager setupコマンドを開始します。

2. 32 ～ 256 文字のパスフレーズを入力します。「cc-mode」の場合は 64 ～ 256 文字のパスフレーズを入力します。

   > 指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. システムが認証キーを作成したことを確認します。

   ```
   security key-manager key query -node node
   ```

   > `security key-manager key query`コマンドは、コマンドに置き換わるもの `security key-manager query key`です。

   の詳細については `security key-manager key query`、を"ONTAPコマンド リファレンス"参照してください。

終了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーします。

システムは、キー管理情報をクラスターの複製データベース (RDB) に自動的にバックアップします。災害復旧のためにこの情報も手動でバックアップする必要があります。

関連情報

- "クラスターイメージコマンド"
- "セキュリティキーマネージャー外部有効化"
- "セキュリティキーマネージャーキークエリ"
- "セキュリティキーマネージャーオンボード有効化"
- "外部キー管理からオンボードキー管理への移行"

ONTAP 9 .5以前でオンボードキー管理を有効にする

オンボードキーマネージャを使用して、クラスタノードをFIPSドライブまたはSEDに対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャ

はFIPS-140-2レベル1に準拠しています。

オンボード キー マネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスターでオンボード キー マネージャーを有効にします。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager setup`ます。

MetroCluster構成の場合は、次のガイドラインを確認してください。

- ONTAP 9 .5では、同じパスフレーズを使用してローカルクラスタと `security key-manager setup -sync-metrocluster-config yes`リモートクラスタでを実行する必要があります `security key-manager setup`。
- ONTAP 9を実行する前に、同じパスフレーズを使用してローカルクラスタでを実行し、20秒ほど待ってからリモートクラスタでを実行する `security key-manager setup`必要があります `security key-manager setup`。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができ `-enable-cc-mode yes`ます。

NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。で `volume create`は、を指定する必要はありません `-encrypt true`。で `volume move start`は、を指定する必要はありません `-encrypt-destination true`。

パスフレーズの入力に失敗した場合は、ノードを再起動する必要があります。

開始する前に

- NSE を外部キー管理 (KMIP) サーバーで使用している場合は、外部キー マネージャー データベースを削除します。

  "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボード キー マネージャを構成する前に、 MetroCluster環境を構成します。

手順

1. キー管理ツールのセットアップを開始します。

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにキー管理ツールのパスフレーズの入力を求めることができます `-enable-cc-mode yes`。NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。

   次の例では、リブートのたびにパスフレーズの入力を要求せずに、cluster1でキー管理ツールのセットア

ップを開始します。

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. オンボードキー管理を設定するかどうかを確認するプロンプトでと入力し `yes`ます。
3. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

4. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
5. すべてのノードにキーが設定されていることを確認します。

   ```
   security key-manager show-key-store
   ```

   詳細はこちら `security key-manager show-key-store`の中で"ONTAPコマンド リファレンス"。

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

終了後

ONTAP は、キー管理情報をクラスタの複製データベース (RDB) に自動的にバックアップします。

オンボード キー マネージャーのパスフレーズを設定した後、その情報をストレージ システム外部の安全な場所に手動でバックアップします。見る"オンボードキー管理情報の手動でのバックアップ"。

関連情報

- "オンボードキー管理情報の手動でのバックアップ"
- "security key-manager setupの実行"
- "セキュリティ キー マネージャーのキー ストアの表示"
- "外部キー管理からオンボードキー管理への移行"

ONTAPオンボードキー管理を使用して**FIPS**ドライブまたは**SED**にデータ認証キーを割り当てます

コマンドを使用して、FIPSドライブまたはSEDにデータ認証キーを割り当てることができます `storage encryption disk modify`。このキーは、クラスタノードでドライブ上のデータにアクセスするときに使用します。

タスクの内容

自己暗号化ドライブは、認証キーIDがデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。SASドライブの標準のデフォルト値は、キーIDが0x0のManufacturer Secure ID（MSID；メーカーのセキュアID）です。NVMeドライブの場合、標準のデフォルト値はnullキーで、空のキーIDで表されます。このキーIDを自己暗号化ドライブに割り当てると、認証キーIDがデフォルト以外の値に変更されます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   の詳細については `storage encryption disk modify`、を"ONTAPコマンド リファレンス"参照してください。

   > キーIDは、コマンドを使用して表示できます `security key-manager key query -key-type NSE-AK`。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   の詳細については `security key-manager key query`、を"ONTAPコマンド リファレンス"参照してください。

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   [...]
   ```

関連情報

- "storage disk show | more"
- "ストレージ暗号化ディスクステータス表示"

ONTAP FIPSドライブに**FIPS 140-2**認証キーを割り当てる

コマンドでオプションを指定する `-fips-key-id`と、FIPSドライブにFIPS 140-2認証キーを割り当てることができます `storage encryption disk modify`。このキーは、クラスタノードでデータアクセス以外のドライブ処理（ドライブに対するDoS攻

撃の防止など）に使用されます。

タスクの内容

セキュリティの設定によっては、データ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合があります。そうでない場合は、FIPS準拠の認証キーをデータアクセスと同じにして使用できます。

この手順はシステムの停止を伴いません。

開始する前に

ドライブファームウェアがFIPS 140-2準拠をサポートしている必要があります。サポートされるドライブファームウェアのバージョンについては、を"NetApp Interoperability Matrix Tool"参照してください。

手順

1. 最初に、データ認証キーが割り当てられていることを確認する必要があります。これは、またはを使用して実行できます外部キー管理ツールオンボードキーマネージャ。コマンドを使用して、キーが割り当てられていることを確認します `storage encryption disk show`。
2. SEDにFIPS 140-2認証キーを割り当てます。

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   キーIDは、コマンドを使用して表示できます `security key-manager query`。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show -fips`

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

   ```
   cluster1::> storage encryption disk show -fips
   Disk    Mode FIPS-Compliance Key ID
   ------  ----
   ------------------------------------------------------------------------
   2.10.0  full <id_value>
   2.10.1  full <id_value>
   [...]
   ```

関連情報

- "ストレージ暗号化ディスクの変更"
- "storage disk show | more"
- "ストレージ暗号化ディスクステータス表示"

ONTAPの**KMIP**サーバ接続に対してクラスタ全体の**FIPS**準拠モードを有効にする

コマンドで`-is-fips-enabled`オプションを使用すると、転送中のデータに対してクラスタ全体の`FIPS`準拠モードを有効にできます `security config modify`。これにより、クラスタからKMIPサーバに接続するときにFIPSモードのOpenSSLが使用されるようになります。

タスクの内容

クラスタ全体のFIPS準拠モードを有効にすると、自動的にTLS1.2とFIPS検証済みの暗号スイートのみが使用されます。クラスタ全体のFIPS準拠モードは、デフォルトでは無効になっています。

クラスタ全体のセキュリティ設定を変更した場合は、クラスタノードを手動でリブートする必要があります。

開始する前に

- ストレージコントローラはFIPS準拠モードで設定する必要があります。
- すべてのKMIPサーバでTLSv1.2がサポートされている必要があります。クラスタ全体のFIPS準拠モードが有効になっている場合、KMIPサーバへの接続を完了するにはTLSv1.2が必要です。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. TLSv1.2がサポートされていることを確認します。

   ```
   security config show -supported-protocols
   ```

   の詳細については `security config show`、を"ONTAPコマンド リファレンス"参照してください。

   ```
   cluster1::> security config show
             Cluster                                                 Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:          yes
                                                !aNULL:!EXP:
                                                !eNULL
   ```

3. クラスタ全体のFIPS準拠モードを有効にします。

```
security config modify -is-fips-enabled true -interface SSL
```

の詳細については `security config modify`、を"ONTAPコマンド リファレンス"参照してください。

4. クラスタノードを手動でリブートします。
5. クラスタ全体のFIPS準拠モードが有効になっていることを確認します。

```
security config show
```

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                              !aNULL:!EXP:
                                              !eNULL:!RC4
```

NetApp暗号化の管理

ONTAPでボリュームデータの暗号化を解除

コマンドを使用して、ボリュームデータを移動したり暗号化を解除したりできます `volume move start`。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 既存の暗号化されたボリュームを移動し、ボリュームのデータの暗号化を解除します。

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate
aggregate_name -encrypt-destination false
```

の詳細については `volume move start`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに `aggr3`移動し `vol1`、ボリュームのデータの暗号化を解除します。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3 -encrypt-destination false
```

ボリュームの暗号化キーが削除されます。ボリュームのデータの暗号化が解除されます。

2. ボリュームで暗号化が無効になっていることを確認します。

   `volume show -encryption`

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、のボリュームが暗号化されているかどうかを表示します `cluster1`。

```
cluster1::> volume show -encryption

Vserver  Volume   Aggregate   State    Encryption State
-------  ------   ---------   -----    ----------------
vs1      vol1     aggr1       online   none
```

ONTAPで暗号化されたボリュームを移動する

コマンドを使用すると、暗号化されたボリュームを移動できます `volume move start`。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

デスティネーションノードまたはデスティネーションボリュームでボリューム暗号化がサポートされていない場合、移動は失敗します。

のオプション `volume move start`は `-encrypt-destination`、暗号化されたボリュームに対してはデフォルトでtrueになります。デスティネーションボリュームを暗号化しないように指定すると、ボリューム上のデータの暗号化が誤って解除されることがなくなります。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 既存の暗号化されたボリュームを移動し、ボリュームのデータを暗号化されたままにします。

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   の詳細については `volume move start`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに `aggr3`移動し`vol1`、ボリュームのデータを暗号化したままにします。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3
```

2. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

ONTAPで**volume encryption rekey start**コマンドを使用してボリュームの暗号化キーを変更する

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。ONTAP 9 .3以降では、コマンドを使用して暗号化キーを変更できます `volume encryption rekey start`。

タスクの内容

キー変更処理を開始したら、最後まで完了する必要があります。古いキーに戻ることはできません。処理中にパフォーマンスの問題が発生した場合は、コマンドを実行して処理を一時停止し、 `volume encryption rekey resume`コマンドを実行して処理を再開できます `volume encryption rekey pause`。

キー変更処理が完了するまで、ボリュームには 2 つのキーが存在することになります。新しい書き込みとそれに対応する読み取りでは、新しいキーが使用されます。それ以外の読み取りでは、古いキーが使用されます。

SnapLockボリュームのキー変更にはを使用できません `volume encryption rekey start`。

手順

1. 暗号化キーを変更します。

   ```
   volume encryption rekey start -vserver SVM_name -volume volume_name
   ```

   次のコマンドは、SVMののvs1暗号化キーを変更し `vol1`ます。

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. キー変更処理のステータスを確認します。

   ```
   volume encryption rekey show
   ```

   の詳細については `volume encryption rekey show`、を"ONTAPコマンド リファレンス"参照してください。

次のコマンドは、キー変更処理のステータスを表示します。

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ----------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. キー変更処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

ONTAPのvolume move startコマンドを使用してボリュームの暗号化キーを変更します

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。暗号化キーは、コマンドを使用して変更できます `volume move start`。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

SnapLockボリュームまたはFlexGroupボリュームのキーの変更にはを使用できません `volume move start`。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 既存のボリュームを移動し、暗号化キーを変更します。

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   の詳細については `volume move start`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに **`aggr2`**`移動し` **`vol1`**、暗号化キーを変更します。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

ボリュームの新しい暗号化キーが作成されます。ボリュームのデータは暗号化されたままです。

2. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

ONTAP NetAppストレージ暗号化の認証キーのローテーション

NetAppストレージ暗号化（NSE）を使用する場合、認証キーをローテーションできます。

タスクの内容

外部キーマネージャ（KMIP）を使用している場合は、NSE環境での認証キーのローテーションがサポートされます。

> オンボードキーマネージャ（OKM）では、NSE環境での認証キーのローテーションはサポートされていません。

手順

1. コマンドを使用し `security key-manager create-key`て、新しい認証キーを生成します。

   認証キーを変更する前に、新しい認証キーを生成する必要があります。

2. コマンドを使用し `storage encryption disk modify -disk * -data-key-id`て、認証キーを変更します。

関連情報

- "ストレージ暗号化ディスクの変更"

ONTAPで暗号化されたボリュームを削除する

コマンドを使用すると、暗号化されたボリュームを削除できます `volume delete`。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- ボリュームはオフラインである必要があります。

ステップ

1. 暗号化されたボリュームを削除します。

   `volume delete -vserver SVM_name -volume volume_name`

   の詳細については `volume delete`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、という名前の暗号化されたボリュームを削除し `vol1`ます。

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   削除の確認を求められたら、と入力し `yes`ます。

   ボリュームの暗号化キーは24時間後に削除されます。

   オプションとともに `-force true`使用して、 `volume delete`ボリュームを削除し、対応する暗号化キーをただちに破棄します。このコマンドには高度な`Privileges`が必要です。の詳細については `volume delete`、を"ONTAPコマンド リファレンス"参照してください。

終了後

コマンドの実行後、コマンドを使用して、削除したボリュームを保持期間内にリカバリ `volume delete`できます `volume recovery-queue`。

`volume recovery-queue SVM_name -volume volume_name`

"ボリュームリカバリ機能の使用方法"

暗号化されたボリューム上のデータのセキュアパージ

暗号化された**ONTAP**ボリュームからデータを安全に消去する方法について説明します。

ONTAP 9 4以降では、セキュアパージを使用して、NVE対応ボリュームのデータを無停止でスクラビングできます。暗号化されたボリュームのデータをスクラビングすることで、「柱」、「ブロックが上書きされたときにデータトレースが残されている」などの物理メディアからデータをリカバリすることができなくなります。また、解約するテナントのデータを安全に削除することもできます。

セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボードキーマネージャではなく、KMIPサーバを使用する必要があります。

セキュアパージを使用する場合の考慮事項

- NetApp Aggregate Encryption（NAE）が有効になっているアグリゲートで作成したボリュームでは、セキュアパージはサポートされません。

- セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボードキーマネージャではなく、KMIPサーバを使用する必要があります。

セキュアパージの動作は、ONTAPのバージョンによって異なります。

ONTAP 9.8以降

- セキュアパージはMetroClusterとFlexGroupでサポートされています。
- パージするボリュームがSnapMirror関係のソースである場合は、SnapMirror関係を解除してセキュアパージを実行する必要はありません。
- 再暗号化の方法は、SnapMirrorデータ保護を使用するボリュームとSnapMirrorデータ保護（DP）を使用しないボリューム、またはSnapMirror拡張データ保護を使用するボリュームで異なります。
  - SnapMirrorデータ保護（DP）モードを使用するボリュームでは、デフォルトでボリューム移動再暗号化方式を使用してデータが再暗号化されます。
  - SnapMirrorデータ保護を使用しないボリューム、またはSnapMirror XDP（拡張データ保護）モードを使用するボリュームでは、インプレース再暗号化方式がデフォルトで使用されます。
  - これらのデフォルト値は、コマンドを使用して変更でき `secure purge re-encryption-method [volume-move|in-place-rekey]`ます。
- デフォルトでは、FlexVolボリューム内のすべてのSnapshotはセキュアパージの実行時に自動的に削除されます。デフォルトでは、FlexGroupおよびSnapMirrorデータ保護を使用するボリューム内のSnapshotは、セキュアパージ処理で自動的に削除されません。これらのデフォルト値は、コマンドを使用して変更でき `secure purge delete-all-snapshots [true|false]`ます。

ONTAP 9 .7以前：

- セキュアパージでは、次の項目はサポートされません。
  - FlexClone
  - SnapVault
  - FabricPool
- パージするボリュームがSnapMirror関係のソースである場合は、ボリュームをパージする前にSnapMirror関係を解除する必要があります。

  ボリューム内に使用中のSnapshotがある場合は、ボリュームをパージする前にSnapshotを解放する必要があります。たとえば、FlexCloneボリュームを親からスプリットする必要がある場合があります。

- セキュアパージ機能を呼び出すと、ボリューム移動がトリガーされ、パージされていない残りのデータが新しいキーで再暗号化されます。

  移動されたボリュームは現在のアグリゲートに残ります。古いキーは自動的に破棄されるため、パージされたデータをストレージメディアからリカバリできません。

SnapMirror関係のない暗号化された**ONTAP**ボリュームからデータをスクラブする

ONTAP 9.4 以降では、 NVE 対応ボリューム上で、システムを停止することなく「 crub

」データにセキュアパージを使用できます。

タスクの内容

削除されたファイル内のデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、セキュアパージを実行できません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。

手順

1. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
2. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

3. セキュアパージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 削除したファイルのセキュアパージを実行します。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   次のコマンドは、SVM上`vs1`で削除したファイルのセキュアパージを実行し `vol1`ます。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. セキュアパージ処理のステータスを確認します。

   ```
   volume encryption secure-purge show
   ```

SnapMirror非同期関係を使用して暗号化された**ONTAP**ボリュームからデータをスクラブする

ONTAP 9 .8以降では、セキュアパージを使用して、SnapMirror非同期関係にあるNVE対応ボリュームで無停止でデータを「スクラビング」できます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

削除されたファイル内のデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、セキュアパージを実行できません。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
3. 非同期関係のデスティネーションボリュームをセキュアパージする準備をします。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

4. セキュアパージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. セキュアパージを実行するファイルがベースSnapshotに含まれている場合は、次の手順を実行します。
   a. SnapMirror非同期関係のデスティネーションボリュームにSnapshotを作成します。

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. SnapMirrorを更新してベースSnapshotを転送します。

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   a. 手順（a）と（b）を、ベースSnapshotの数に1を加えた値に繰り返します。

たとえば、ベースSnapshotが2つある場合は、手順（a）と（b）を3回繰り返します。

b. ベースSnapshotが存在することを確認します。+
`snapshot show -vserver SVM_name -volume volume_name`

c. ベースSnapshotを削除します。+
`snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 削除したファイルのセキュアパージを実行します。

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは、 SVM 「 vs1 」上の「 vol1 」にある削除済みファイルを安全にパージします。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. セキュアパージ処理のステータスを確認します。

   `volume encryption secure-purge show`

関連情報

- "snapmirror update"

SnapMirror同期関係を使用して暗号化された**ONTAP**ボリュームからデータをスクラブする

ONTAP 9 8以降では、セキュアパージを使用して、SnapMirror同期関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

タスクの内容

セキュアパージは、削除されたファイル内のデータ量によっては、完了までに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、セキュアパージを実行できません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
3. 非同期関係のデスティネーションボリュームをセキュアパージする準備をします。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   SnapMirror同期関係のもう一方のボリュームに対してこの手順を繰り返します。
4. セキュアパージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```
5. セキュアパージファイルがベースSnapshotまたは共通Snapshotに含まれている場合は、SnapMirrorを更新して共通Snapshotを転送します。

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   共通のSnapshotは2つあるため、このコマンドは2回実行する必要があります。
6. セキュアパージファイルがアプリケーションと整合性のあるSnapshotに含まれている場合は、SnapMirror同期関係の両方のボリュームでSnapshotを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   この手順は両方のボリュームで実行します。
7. 削除したファイルのセキュアパージを実行します。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   SnapMirror同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは 'SVM "vs1 `" 上の "vol1" 上の削除されたファイルを安全にパージします

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```
8. セキュアパージ処理のステータスを確認します。

   ```
   volume encryption secure-purge show
   ```

関連情報

- "snapmirror update"

ONTAPオンボードキー管理パスフレーズを変更する

オンボードキー管理パスフレーズを定期的に変更してください。新しいパスフレーズをストレージ システム外部の安全な場所に保存します。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。
- ONTAP MetroCluster環境を管理している場合は、両方のクラスタでパスフレーズを更新する必要があります。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. オンボードキー管理のパスフレーズを変更します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard update-passphrase`
ONTAP 9.5以前	`security key-manager update-passphrase`

3. 32 ～ 256 文字のパスフレーズを入力します。「`cc-mode`」の場合は 64 ～ 256 文字のパスフレーズを入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

4. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。

終了後

あとで使用できるように、ストレージシステムの外部の安全な場所にオンボードキー管理のパスフレーズをコピーしておく必要があります。

オンボードキー管理のパスフレーズを変更するときは、キー管理情報を手動でバックアップする必要があります。

関連情報

- "オンボードキー管理情報の手動バックアップ"
- "security key-manager onboard update-passphrase（セキュリティキー管理ツールオンボード更新パスフレーズ）"

ONTAPオンボードキー管理情報を手動でバックアップする

オンボードキーマネージャのパスフレーズを設定する場合、ストレージシステムの外部の安全な場所にオンボードキー管理の情報をコピーしておく必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

キー管理情報はすべて、クラスタのReplicated Database（RDB；複製データベース）に自動的にバックアップされます。災害時に備えて、キー管理情報を手動でもバックアップしておく必要があります。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスタのキー管理バックアップ情報を表示します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard show-backup`
ONTAP 9.5以前	`security key-manager backup show`

   次の9.6コマンドは、キー管理バックアップ情報を表示します。 `cluster1` ：

```
cluster1::> security key-manager onboard show-backup

      -------------------------BEGIN BACKUP-------------------------
      TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
      QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
      dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
      3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
      IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
      QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
      BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

開始する前に

- NSE を外部 KMIP サーバーと共に使用する場合は、外部キー マネージャー データベースを削除します。詳細については、"外部キー管理からONTAPオンボードキー管理への移行" 。
- このタスクを実行するには、クラスタ管理者である必要があります。

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

ONTAP 9.6以降

> ONTAP 9.8以降を実行していてルートボリュームが暗号化されている場合は、の手順を実行します [ontap-9-8]。

1. キーをリストアする必要があることを確認します。+
`security key-manager key query -node node`

   の詳細については `security key-manager key query`、を"ONTAPコマンド リファレンス"参照してください。

2. キーをリストアします。+
`security key-manager onboard sync`

   の詳細については `security key-manager onboard sync`、を"ONTAPコマンド リファレンス"参照してください。

3. パスフレーズのプロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。

ルートボリュームを暗号化した**ONTAP 9.8**以降

ONTAP 9 .8以降を実行しており、ルートボリュームが暗号化されている場合は、ブートメニューでオンボードキー管理のリカバリパスフレーズを設定する必要があります。このプロセスは、ブートメディアを交換する場合にも必要です。

1. ノードをブートメニューでブートし、オプションを選択します `(10) Set onboard key management recovery secrets`。
2. と入力して、 `y`このオプションを使用します。
3. プロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。
4. プロンプトで、バックアップキーのデータを入力します。

   バックアップ キー データを入力すると、ノードはブート メニューに戻ります。

5. ブートメニューからオプションを選択します `(1) Normal Boot`。

ONTAP 9.5以前

1. キーをリストアする必要があることを確認します。+
`security key-manager key show`
2. キーをリストアします。+

```
security key-manager setup -node node
```

詳細はこちら `security key-manager setup`の中で"ONTAPコマンド リファレンス"。

3. パスフレーズのプロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。

ONTAP外部キー管理暗号化キーを復元する

外部キー管理の暗号化キーを手動でリストアし、別のノードにプッシュすることができます。この処理は、クラスタのキーの作成時に一時的に停止していたノードを再起動する場合に実行します。

タスクの内容

ONTAP 9 .6以降では、コマンドを使用してキーのリストアが必要かどうかを確認できます `security key-manager key query -node node_name`。

ONTAP 9 .5以前では、コマンドを使用してキーのリストアが必要かどうかを確認できます `security key-manager key show`。

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

の詳細については `security key-manager key query`、を"ONTAPコマンド リファレンス"参照してください。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. ONTAP 9 .8以降を実行していて、ルートボリュームが暗号化されている場合は、次の手順を実行します。

   ONTAP 9 .7以前を実行している場合、またはONTAP 9 .8以降を実行していてルートボリュームが暗号化されていない場合は、この手順を省略します。

   a. bootargを設定します。
   ```
   setenv kmip.init.ipaddr <ip-address>
   setenv kmip.init.netmask <netmask>
   setenv kmip.init.gateway <gateway>
   setenv kmip.init.interface e0M++
   boot_ontap
   ```
   b. ノードをブートメニューでブートし、オプションを選択します `(11) Configure node for external key management`。
   c. プロンプトに従って管理証明書を入力します。

      管理証明書の情報をすべて入力すると、システムがブート メニューに戻ります。

   d. ブートメニューからオプションを選択します `(1) Normal Boot`。

2. キーをリストアします。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5以前

`node`デフォルトはすべてのノードです。

このコマンドは、オンボードキー管理が有効になっている場合はサポートされません。

次のONTAP 9 .6コマンドは、外部キー管理の認証キーをのすべてのノードにリストアします `cluster1`。

```
clusterl::> security key-manager external restore
```

関連情報

- "security key-manager external restoreのように指定します"

ONTAPクラスタ上の**KMIP SSL**証明書を置き換える

すべてのSSL証明書には有効期限があります。認証キーへのアクセスが失われないように、証明書の有効期限が切れる前に証明書を更新する必要があります。

開始する前に

- クラスタの交換用のパブリック証明書と秘密鍵（KMIPクライアント証明書）を入手しておく必要があります。
- KMIPサーバの交換用のパブリック証明書（KMIP server-ca証明書）を入手しておく必要があります。
- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- MetroCluster環境でKMIP SSL証明書を交換する場合は、同じ交換用KMIP SSL証明書を両方のクラスタにインストールする必要があります。

KMIPサーバへの交換用のクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでも実行できます。

手順

1. 新しいKMIPサーバCA証明書をインストールします。

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

2. 新しいKMIPクライアント証明書をインストールします。

   ```
   security certificate install -type client -vserver <>
   ```

3. 新しくインストールした証明書を使用するようにキー管理ツールの設定を更新します。

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
-certs <>
```

MetroCluster環境でONTAP 9 .6以降を実行していて、管理SVMのキー管理ツールの設定を変更する場合は、構成内の両方のクラスタでコマンドを実行する必要があります。

新しいクライアント証明書の公開鍵と秘密鍵が以前にインストールしたキーと異なる場合、新しくインストールした証明書を使用するようにキー管理ツールの設定を更新するとエラーが返されます。参照"NetAppナレッジベース: 新しいクライアント証明書の公開鍵または秘密鍵が既存のクライアント証明書と異なります"このエラーを回避する方法については、こちらをご覧ください。

関連情報

- "セキュリティ証明書のインストール"
- "security key-manager external modifyのような変更が可能です"

ONTAPでの**FIPS**ドライブまたは**SED**の交換

FIPSドライブまたはSEDは、通常のディスクと同じ方法で交換できます。交換用ドライブに新しいデータ認証キーを割り当ててください。FIPSドライブの場合は、新しいFIPS 140-2認証キーを割り当てることもできます。

HAペアでを使用している場合は"SAS ドライブまたは NVMe ドライブの暗号化（ SED 、 NSE 、 FIPS ）"、システムを初期化する前に、HAペア内のすべてのドライブに対応するトピックの手順に従う必要があります"FIPSドライブまたはSEDを非保護モードに戻す"（ブートオプション4または9）。これを行わないと、ドライブを転用した場合にデータが失われる可能性があります。

開始する前に

- ドライブで使用される認証キーのキーIDを確認しておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. ディスクが障害状態としてマークされていることを確認します。

   ```
   storage disk show -broken
   ```

   の詳細については `storage disk show`、を"ONTAPコマンド リファレンス"参照してください。

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. ディスクシェルフモデルのハードウェアガイドの手順に従って、障害ディスクを取り外し、新しいFIPSドライブまたはSEDに交換します。
3. 交換した新しいディスクの所有権を割り当てます。

   `storage disk assign -disk disk_name -owner node`

   の詳細については `storage disk assign`、を"ONTAPコマンド リファレンス"参照してください。

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 新しいディスクが割り当てられたことを確認します。

   `storage encryption disk show`

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

"FIPSドライブまたはSEDへのデータ認証キーの割り当て（外部キー管理）"

6. 必要に応じて、FIPS 140-2認証キーをFIPSドライブに割り当てます。

   "FIPSドライブへのFIPS 140-2認証キーの割り当て"

関連情報

- "storage disk assign"
- "storage disk show"
- "storage disk show | more"

FIPSドライブまたはSEDのデータにアクセスできないようにする

FIPSドライブまたはSED上のONTAPデータをアクセス不能にする方法について学習します

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブの未使用スペースを新しいデータに使用できるようにしておく場合は、ディスクを完全消去できます。データに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、ディスクを破棄できます。

- ディスク完全消去

  自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID 0x0（SASドライブ）またはnullキー（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去したディスクは、初期化されていないスペアディスクとして再利用できます。

- ディスクの破棄

  FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ディスクが完全にロックされます。これにより、ディスクが永続的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。

完全消去と破棄は、個々の自己暗号化ドライブまたはノードのすべての自己暗号化ドライブに対して実行できます。

ONTAPのFIPSドライブまたはSEDの完全消去

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、そのドライブを新しいデータに使用する場合は、コマンドを使用してドライブを完全消去できます `storage encryption disk sanitize`。

タスクの内容

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID 0x0（SASドライブ）またはnullキー（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去したディスクは、初期化されていないスペアディスクとして再利用できます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 完全消去するFIPSドライブまたはSEDのアグリゲートを削除します。

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   の詳細については `storage aggregate delete`、を"ONTAPコマンド リファレンス"参照してください。

3. 完全消去するFIPSドライブまたはSEDのディスクIDを確認します。

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   キーIDは、コマンドを使用して表示できます `security key-manager query`。

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. ドライブを完全消去します。

```
storage encryption disk sanitize -disk disk_id
```

このコマンドを使用して完全消去できるのは、ホットスペアディスクまたは破損ディスクのみです。タイプに関係なくすべてのディスクを完全消去するには、オプションを使用し `-force-all-state`ます。の詳細については `storage encryption disk sanitize`、を"ONTAPコマンド リファレンス"参照してください。

> ⓘ 続行する前に、確認フレーズの入力を求めるプロンプトがONTAPに表示されます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. 完全消去したディスクの障害状態を解除します。
`storage disk unfail -spare true -disk disk_id`
7. ディスクに所有者があるかどうかを確認します
`storage disk show -disk disk_id`。+ディスクに所有者がない場合は、所有者を割り当てます。
`storage disk assign -owner node -disk disk_id`
8. 完全消去するディスクを所有するノードのノードシェルに切り替えます。

   `system node run -node node_name`

   コマンドを実行します `disk sanitize release`。
9. ノードシェルを終了します。ディスクの障害状態を再度解除します。
`storage disk unfail -spare true -disk disk_id`
10. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
`storage disk show -disk disk_id`

関連情報

- "storage disk assign"
- "storage disk show"
- "ストレージディスクの故障なし"
- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスクサニタイズ"
- "ストレージ暗号化ディスクステータス表示"

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、コマンドを使用してディスクを破棄できます `storage encryption disk destroy`。

タスクの内容

FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ドライブが完全にロックされます。これにより、ディスクが実質的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。ただし、ディスクのラベルに印刷されているPhysical Secure ID（PSID；物理的なセキュアID）を使用して、ディスクを工場出荷時の設定にリセットすることができます。詳細については、を参照してください "認証キーが失われた場合にFIPSドライブまたはSEDを使用可能な状態に戻す"。

> 障害ディスク返却不要サービス（NRD Plus）を利用している場合を除き、FIPSドライブまたはSEDは破棄しないでください。ディスクを破棄すると保証が無効になります。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 破棄する FIPS ドライブまたは SED のアグリゲートを削除します。

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   の詳細については `storage aggregate delete`、を"ONTAPコマンド リファレンス"参照してください。

3. 破棄する FIPS ドライブまたは SED のディスク ID を確認します。

   `storage encryption disk show`

   の詳細については `storage encryption disk show`、を"ONTAPコマンド リファレンス"参照してください。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. ディスクを破棄します。

   `storage encryption disk destroy -disk disk_id`

   の詳細については `storage encryption disk destroy`、を"ONTAPコマンド リファレンス"参照してください。

   続行する前に確認のフレーズを入力するように求められます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

関連情報

- "ストレージ暗号化ディスク破壊"
- "storage disk show | more"
- "ストレージ暗号化ディスクステータス表示"

ONTAPの**FIPS**ドライブまたは**SED**の緊急時のシュレッディングデータ

セキュリティに関する緊急事態が発生した場合は、ストレージシステムまたはKMIPサーバへの給電が遮断されていても、FIPSドライブまたはSEDへのアクセスを即座に禁止できます。

開始する前に

- 使用可能な電力が供給されていないKMIPサーバを使用している場合は、破棄しやすい認証アイテム（スマートカードやUSBドライブなど）を使用してKMIPサーバを設定する必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. FIPSドライブまたはSEDのデータの緊急時のシュレッディングを実行します。

状況	そしたら…。

ストレージシステムに給電されており、ストレージシステムを正常にオフラインにする時間がある	a. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。
	b. すべてのアグリゲートをオフラインにしてから削除します。
	c. 権限レベルをadvancedに設定します。+
	`set -privilege advanced`
	d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。+
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. ストレージシステムを停止します。
	f. メンテナンスモードでブートします。
	g. ディスクを完全消去するか破棄します。
	◦ ディスクのデータにアクセスできない状態にしてディスクを再利用する場合は、ディスクを完全消去します。+
	`disk encrypt sanitize -all`
	◦ ディスクのデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄します。+
	`disk encrypt destroy disk_id1 disk_id2 …`
		ストレージシステムに給電されており、データをただちにシュレッディングする必要がある

a. * ディスク上のデータにアクセスできない状態にし、ディスクを再利用する場合は、ディスクを完全消去します。 *
b. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。
c. 権限レベルをadvancedに設定します。
`set -privilege advanced`
d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. ディスクを完全消去します。
`storage encryption disk sanitize -disk * -force-all-states true`
	a. * ディスク上のデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄してください： *
	b. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。
	c. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	d. ディスクを破棄します。
	`storage encryption disk destroy -disk * -force-all-states true`
		ストレージシステムがパニック状態になり、システムは永続的に無効な状態になり、すべてのデータが消去されます。システムを再度使用するには、再設定する必要があります。

KMIPサーバに給電されているが、ストレージシステムには給電されていない	a. KMIPサーバにログインします。 b. アクセスを禁止するデータを含むFIPSドライブまたはSEDに関連付けられているすべてのキーを破棄します。これにより、ストレージシステムからディスク暗号化キーにアクセスできなくなります。	KMIPサーバまたはストレージシステムに給電されていない

関連情報

- "ストレージ暗号化ディスク破壊"
- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスクサニタイズ"

ONTAPで認証キーが失われた場合、**FIPS**ドライブまたは**SED**をサービスに戻す

FIPSドライブまたはSEDの認証キーが永久に失われ、KMIPサーバから取得できない場

合、FIPSドライブまたはSEDは破損しているとみなされます。ディスク上のデータにアクセスしたりリカバリしたりすることはできませんが、SEDの未使用スペースをデータに再び使用できるようにすることができます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

タスクの内容

このプロセスは、FIPSドライブまたはSEDの認証キーが永久に失われてリカバリできないことが確実である場合にのみ使用してください。

ディスクがパーティショニングされている場合は、このプロセスを開始する前にパーティショニングを解除する必要があります。

ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用できます。NetAppサポートから指示があった場合にのみ実行してください。続行する前に**NetApp**サポートに連絡することを強くお勧めします。また、"NetAppナレッジベース: ONTAPでスペアドライブのパーティションを解除する方法" 。

手順

1. FIPSドライブまたはSEDを使用可能な状態に戻します。

SED の状況	実行する手順

FIPS準拠モードではない、またはFIPS準拠モードでFIPSキーを使用できる	a. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	b. FIPSキーをデフォルトのメーカーセキュアIDである0x0にリセットします。
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 処理が成功したことを確認します。
	`storage encryption disk show-status`処理に失敗した場合は、このトピックのPSIDプロセスを使用してください。
	d. 破損ディスクを完全消去します。次の手順に進む前に、コマンドを使用して処理が成功したことを確認します `storage encryption disk show-status`。
	`storage encryption disk sanitize -disk disk_id`
	e. 完全消去したディスクの障害状態を解除します。
	`storage disk unfail -spare true -disk disk_id`
	f. ディスクに所有者があるかどうかを確認します
	`storage disk show -disk disk_id`。+ディスクに所有者がない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk disk_id`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node node_name`
	コマンドを実行します `disk sanitize release`。
	g. ノードシェルを終了します。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk disk_id`
	h. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk disk_id`

FIPS準拠モードでFIPSキーを使用できず、SEDのPSIDがラベルに印刷されている	a. ディスクラベルからディスクのPSIDを確認します。
	b. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	c. ディスクを工場出荷時の設定にリセットします。次の手順に進む前に、コマンドを使用して処理が成功したことを確認し `storage encryption disk show-status`ます。
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`
	d. ONTAP 9.8P5以前を実行している場合は、次の手順に進みます。ONTAP 9 .8P6以降を実行している場合は、完全消去したディスクの障害状態を解除します。
	`storage disk unfail -disk disk_id`
	e. ディスクに所有者があるかどうかを確認します
	`storage disk show -disk disk_id`。+ディスクに所有者がない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk disk_id`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node node_name`
	コマンドを実行します `disk sanitize release`。
	f. ノードシェルを終了します。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk disk_id`
	g. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk disk_id`

関連情報

- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスクを元の状態に戻す"
- "ストレージ暗号化ディスクサニタイズ"
- "ストレージ暗号化ディスクステータス表示"

ONTAPで**FIPS**ドライブまたは**SED**を非保護モードに戻す

FIPSドライブまたはSEDは、ノードの認証キーIDがデフォルト以外の値に設定されている場合にのみ不正アクセスから保護されます。FIPSドライブまたはSEDを非保護モードに戻すには、コマンドを使用して `storage encryption disk modify`キーIDをデフォルトに設定します。非保護モードのFIPSドライブまたはSEDではデフォルトの暗号化キーが使用され、保護モードのFIPSドライブまたはSEDでは指定したシークレット暗号化キーが使用されます。ドライブに暗号化されたデータがあり、ドライブが非保護モードにリセ

ットされても、データは暗号化されたままになり、公開されません。

> FIPS ドライブまたは SED が非保護モードに戻った後、暗号化されたデータにアクセスできなくなるようにするには、次の手順に従ってください。FIPS とデータ キー ID がリセットされると、元のキーを復元しない限り、既存のデータは復号化できなくなり、アクセスできなくなります。

HAペアで暗号化SASドライブまたはNVMeドライブ（SED、NSE、FIPS）を使用している場合は、システムを初期化する前に、HAペア内のすべてのドライブでこのプロセスを実行する必要があります（ブートオプション4または9）。これを行わないと、ドライブを転用した場合にデータが失われる可能性があります。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   キーIDは、コマンドを使用して表示できます `security key-manager query`。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   コマンドを使用して、処理が成功したことを確認します。

   ```
   storage encryption disk show-status
   ```

   「Disks Begun」と「Disks Done」の数字が同じになるまで、show-status コマンドを繰り返します。

```
cluster1:: storage encryption disk show-status

            FIPS    Latest   Start               Execution   Disks
Disks Disks
Node        Support Request  Timestamp           Time (sec)  Begun
Done  Successful
-------     ------- -------- ------------------  ---------- ------
------  ----------
cluster1    true    modify   1/18/2022 15:29:38    3           14     5
5
1 entry was displayed.
```

3. ノードのデータ認証キーIDをデフォルトのMSIDである0x0に戻します。

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   SASドライブとNVMeドライブのどちらを非保護モードに戻すかに関係なく、の値は `-data-key-id`0x0に設定する必要があります。

   キーIDは、コマンドを使用して表示できます `security key-manager query`。

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

   コマンドを使用して、処理が成功したことを確認します。

   `storage encryption disk show-status`

   値が同じになるまでshow-statusコマンドを繰り返します。「disks began」と「disks done」の数字が同じであれば、操作は完了です。

メンテナンスモオト

ONTAP 9 .7以降では、保守モードからFIPSドライブのキーを変更できます。保守モードは、前述のONTAP CLIの手順を使用できない場合にのみ使用してください。

手順

1. ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   `disk encrypt rekey_fips 0x0 disklist`

2. ノードのデータ認証キーIDをデフォルトのMSIDである0x0に戻します。

```
disk encrypt rekey 0x0 disklist
```

3. FIPS認証キーのキーが正常に変更されたことを確認します。

```
disk encrypt show_fips
```

4. データ認証キーのキーが変更されたことを確認します。

```
disk encrypt show
```

出力には、デフォルトのMSID 0x0キーIDまたはキーサーバが保持する64文字の値が表示される可能性があります。 `Locked?`フィールドはデータロックを参照します。

```
Disk        FIPS Key ID                  Locked?
----------- ---------------------------- -------
0a.01.0     0x0                           Yes
```

関連情報

- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスクステータス表示"

ONTAPで外部キー管理ツールの接続を削除する

KMIPサーバが不要になったときはノードから切断できます。たとえば、ボリューム暗号化に移行するときにKMIPサーバを切断できます。

タスクの内容

HAペアの一方のノードからKMIPサーバを切断すると、すべてのクラスタノードから自動的にサーバが切断されます。

KMIPサーバを切断したあとも外部キー管理を引き続き使用する場合は、別のKMIPサーバで認証キーを提供できることを確認してください。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

ステップ

1. 現在のノードからKMIPサーバを切断します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external remove-servers -vserver SVM -key-servers host_name
IP_address:port,…`	ONTAP 9.5以前

MetroCluster環境の場合は、管理SVMの両方のクラスタでこれらのコマンドを繰り返す必要があります。

次のONTAP 9 .6コマンドは、2つの外部キー管理サーバへの接続を無効にします。1つ目はデフォルトポート5696をリスンするという名前のサーバ、 `ks1`もう1つはポート24482をリスンするIPアドレス10.0.0.20のサーバ `cluster1`です。

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

および `security key-manager delete`の詳細については `security key-manager external remove-servers`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP外部キー管理サーバのプロパティを変更する

ONTAP 9 .6以降では、コマンドを使用して外部キー管理サーバのI/Oタイムアウトとユーザ名を変更でき `security key-manager external modify-server`ます。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。
- MetroCluster環境の場合は、管理SVMの両方のクラスタで上記の手順を繰り返す必要があります。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスタの外部キー管理サーバのプロパティを変更します。

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。このコマンドをクラスタのログインプロンプトで実行すると、が `*admin_SVM*`デフォルトで現在のクラスタの管理SVMに設定されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者である必要があります。

   次のコマンドは、デフォルトポート5696をリスンしている外部キー管理サーバのタイムアウト値を45秒に変更します `cluster1`。

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. SVMの外部キー管理サーバのプロパティを変更します（NVEのみ）。

   ```
   security key-manager external modify-server -vserver SVM -key-server
   ```

```
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。このコマンドをSVMのログインプロンプトで実行すると、が `*SVM*`デフォルトで現在のSVMに設定されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者またはSVM管理者である必要があります。

次のコマンドは、デフォルトポート5696をリスンする外部キー管理サーバのユーザ名とパスワードを変更し `svm1`ます。

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. SVMを追加する場合は、最後の手順を繰り返します。

関連情報

- "security key-manager external modify -server"

ONTAPのオンボードキー管理から外部キー管理への移行

オンボードキー管理から外部キー管理に切り替える場合は、外部キー管理を有効にする前にオンボードキー管理の設定を削除する必要があります。

開始する前に

- ハードウェアベースの暗号化の場合は、すべてのFIPSドライブまたはSEDのデータキーをデフォルト値にリセットする必要があります。

  "FIPSドライブまたはSEDを非保護モードに戻す"

- ソフトウェアベースの暗号化では、すべてのボリュームの暗号化を解除する必要があります。

  "ボリューム データの暗号化の解除"

- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. クラスタのオンボードキー管理の設定を削除します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5以前	`security key-manager delete-key-database`

および `security key-manager delete-key-database`の詳細については `security key-

`manager onboard disable`、を"ONTAPコマンド リファレンス"参照してください。

外部キー管理から**ONTAP**オンボードキー管理に切り替える

オンボード キー管理に切り替えるには、オンボード キー管理を有効にする前に、外部キー管理構成を削除します。

開始する前に

- ハードウェアベースの暗号化の場合は、すべてのFIPSドライブまたはSEDのデータキーをデフォルト値にリセットする必要があります。

  "FIPSドライブまたはSEDを非保護モードに戻す"

- すべての外部キー管理ツールの接続を削除しておく必要があります。

  "外部キー管理ツールの接続の削除"

- このタスクを実行するには、クラスタ管理者である必要があります。

手順

キー管理の移行手順は、使用しているONTAPのバージョンによって異なります。

ONTAP 9.6以降

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを使用します。

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   MetroCluster環境の場合は、管理SVMに対して両方のクラスタでこのコマンドを繰り返す必要があります。

詳細はこちら `security key-manager external disable`の中で"ONTAPコマンド リファレンス"。

ONTAP 9.5以前

次のコマンドを使用します。

```
security key-manager delete-kmip-config
```

詳細はこちら `security key-manager delete-kmip-config`の中で"ONTAPコマンド リファレンス"。

関連情報

- "セキュリティキーマネージャー外部無効化"

ブートプロセス時に NSE 用に構成されたストレージシステムが指定されたどのキー管理サーバにもアクセスできない場合、 ONTAP ではストレージシステムの望ましくない動作を回避するために、特定の予防措置を取ります。

ストレージシステムが NSE 用に設定されている場合、 SED のキーが変更されてロックされ、 SED の電源がオンになっているときは、ストレージシステムは、キー管理サーバから必要な認証キーを取得して SED に対して自身を認証し、データにアクセスできるようにする必要があります。

ストレージシステムは、指定されたキー管理サーバへのアクセスを最大 3 時間試行します。その時間が経過してもストレージシステムがどのキー管理サーバにもアクセスできない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムは、指定されたいずれかのキー管理サーバに正常にアクセスできた場合、SSL接続の確立を最大15分間試行します。ストレージシステムが指定されたどのキー管理サーバとも SSL 接続を確立できない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムがキー管理サーバへのアクセスと接続を試行している間、失敗したアクセス試行に関する詳細情報がCLIに表示されます。アクセスの試行は、 Ctrl+C キーを押すことによっていつでも中断できます

セキュリティ対策として、SEDでは許可される不正アクセスの試行回数が制限され、試行回数が制限されたあとは既存データへのアクセスが無効になります。ストレージシステムが指定されたどのキー管理サーバにもアクセスできず、適切な認証キーを取得できない場合、デフォルトのキーでの認証しか試行できないため、試行が失敗してパニック状態になります。パニック状態が発生した場合に自動的にリブートするように設定されているストレージシステムはブートループに入り、SEDでの認証が連続して失敗します。

設計上、このような状況でストレージシステムを停止するのは、認証の連続失敗回数の上限を超えたためにSEDが永続的にロックされた場合に、ストレージシステムがブートループに入ったり、意図しないデータ損失が発生したりするのを防ぐためです。ロックアウト保護の制限とタイプは、SEDの製造仕様とタイプによって異なります。

SEDタイプ	ロックアウトされるまでの認証の連続失敗回数	安全制限に達したときのロックアウト保護タイプ
HDD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンがNA00またはNA01のX440_PHM2800MCTO 800GB NSE SSD	5	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンがNA00またはNA01のX577_PHM2800MCTO 800GB NSE SSD	5	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。

ファームウェアリビジョンが上位のX440_PHM2800MCTO 800GB NSE SSD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンが上位のX577_PHM2800MCTO 800GB NSE SSD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
その他すべての SSD モデル	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。

すべての SED タイプでは、認証が成功すると試行回数が 0 にリセットされます。

ストレージシステムが指定されたどのキー管理サーバにもアクセスできないために停止した場合は、引き続きストレージシステムのブートを試行する前に、通信エラーの原因を特定して修正しておく必要があります。

ONTAP暗号化をデフォルトで無効にする

ONTAP 9 .7以降では、Volume Encryption（VE）ライセンスがあり、オンボードまたは外部のキー管理ツールを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。必要に応じて、暗号化をデフォルトでクラスタ全体で無効にすることができます。

開始する前に

このタスクを実行するには、クラスタ管理者であるか、クラスタ管理者から権限を委譲されたSVM管理者である必要があります。

ステップ

1. ONTAP 9 .7以降でクラスタ全体の暗号化をデフォルトで無効にするには、次のコマンドを実行します。

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

データ保護とディザスタリカバリ

クラスタと**SVM**のピアリング

ONTAPクラスタと**SVM**のピアリングの詳細

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

ONTAP 9 .3では、クラスタとSVM間のピア関係の設定方法が簡易化されています。クラスタとSVMのピアリング手順は、ONTAP 9のすべてのバージョンで使用できます。使用しているONTAPのバージョンに応じた手順を使用してください。

手順の実行には、System Managerや自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用します。

クラスタと**SVM**のピアリングの準備

ONTAPピアリングの基本

SnapMirrorを使用してSnapshotをレプリケートする前に、ソースとデスティネーションのクラスタ間およびソースとデスティネーションのSVM間で_peer relationships_を作成しておく必要があります。ピア関係で定義されるネットワーク接続により、クラスタ間および SVM 間でデータをセキュアにやり取りすることができます。

ピア関係にあるクラスタおよび SVM は、 _intercluster 論理インターフェイス（ LIF ）を使用してクラスタ間ネットワーク経由で通信します。 _ クラスタ間 LIF は、「 intercluster-core 」ネットワークインターフェイスサービスをサポートする LIF で、通常は「 default-intercluster 」ネットワークインターフェイスサービスポリシーを使用して作成されます。ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成する必要があります。

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

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

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

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

の詳細については `network interface service-policy show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPピアリングの前提条件

クラスタピアリングを設定する前に、接続、ポート、IPアドレス、サブネット、ファイアウォール、およびクラスタの命名要件が満たされていることを確認する必要があります。

ONTAP 9 .6以降では、クラスタピアリングでデータレプリケーションに対してTLS 1.2 AES-256 GCM暗号化がデフォルトでサポートされます。暗号化が無効になっていてもクラスタピアリングが機能するには、デフォルトのセキュリティ暗号（「PSK-AES256-GCM-SHA384」）が必要です。

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

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

接続要件

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

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

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

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

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

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

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

ポートの要件

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

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

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

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

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

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

ファイアウォールの要件

ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

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

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

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

デフォルトのファイアウォールポリシーは、 `intercluster`HTTPSプロトコルによるアクセスとすべてのIPアドレス（0.0.0.0/0）からのアクセスを許可します。必要に応じて、ポリシーを変更または置き換えることができます。

クラスタの要件

クラスタは、次の要件を満たす必要があります。

- 1つのクラスタでピア関係を確立できるクラスタは最大255個です。

共有または専用の**ONTAP**ポートを使用する

クラスタ間通信には専用のポートを使用することも、データネットワークで使用されるポートを共有することもできます。ポートを共有するかどうかを判断する際は、ネット

ワーク帯域幅、レプリケーション間隔、およびポートの可用性を考慮する必要があります。

ピア関係にある一方のクラスタではポートを共有し、もう一方のクラスタでは専用ポートを使用することができます。

ネットワーク帯域幅

10GbEなどの高速ネットワークを使用している場合は、データアクセスに使用されるのと同じ10GbEポートを使用してレプリケーションを実行するのに十分なローカルLAN帯域幅がある可能性があります。

その場合も、 LAN 側と WAN 側の使用帯域幅を比較する必要があります。WAN 側で使用可能な帯域幅が 10GbE よりも大幅に狭い場合、専用ポートを使用しなければならないことがあります。

ただし、クラスタのすべてまたは多数のノードでデータをレプリケートする場合は例外で、この場合は一般に帯域幅がノード間で分散して使用されます。

専用ポートを使用しない場合、一般にレプリケーションネットワークの最大転送単位（ MTU ）サイズはデータネットワークの MTU サイズと同じにします。

レプリケーション間隔

ピーク時を避けてレプリケーションを実施する場合は、 10GbE LAN 接続がなくてもデータポートを使用できるはずです。

通常の業務時間にレプリケーションを実施する場合は、レプリケートされるデータの量と、原因がデータプロトコルと競合するために必要な帯域幅を考慮する必要があるかどうかを検討する必要があります。データプロトコル（ SMB 、 NFS 、 iSCSI ）によるネットワーク利用率が 50% を超える場合は、ノードのフェイルオーバーが発生してもパフォーマンスの低下を招かないよう、クラスタ間通信に専用のポートを使用します。

ポートの可用性

レプリケーショントラフィックがデータトラフィックの妨げになる場合は、同じノード上にある他の任意のクラスタ間対応共有ポートにクラスタ間 LIF を移行できます。

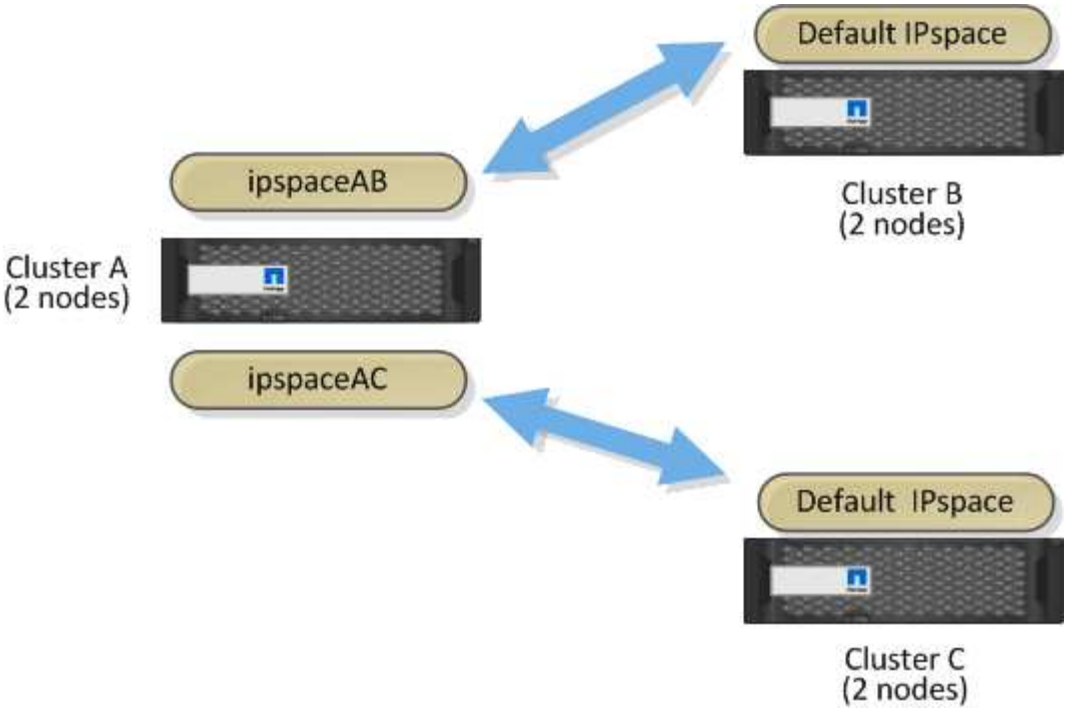
VLAN ポートをレプリケーション専用にすることもできます。ポートの帯域幅は、すべてのVLANとベースポートの間で共有されます。

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

カスタムIPspaceを使用すると、クラスタとピアのやり取りを分離できます。Called_Designated intercluster connectivity_ 。この設定により、サービスプロバイダはマルチテナント環境でレプリケーショントラフィックを分離できます。

たとえば、クラスタAとクラスタBの間のレプリケーション トラフィックをクラスタAとクラスタCの間のレプリケーション トラフィックから切り離すためには、クラスタAにIPspaceを2つ作成します。

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



関連情報

- "ONTAP IPspace設定の詳細"

クラスタ間LIFを設定

共有データポートでのONTAPクラスタ間LIFの設定

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

手順

1. クラスタ内のポートの一覧を表示します。

   ```
   network port show
   ```

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、のネットワークポートを示してい `cluster01`ます。

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

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

オプション	説明
• ONTAP 9.6 以降： *	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
• ONTAP 9.5 以前： *	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、クラスタ間LIFと `cluster01_icl02`を作成し `cluster01_icl01`ます。

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

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

3. クラスタ間LIFが作成されたことを確認します。

オプション	説明
• ONTAP 9.6 以降：* 	`network interface show -service-policy default-intercluster`
• ONTAP 9.5 以前：* 	`network interface show -role intercluster`

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. クラスタ間LIFが冗長構成になっていることを確認します。

オプション	説明
• ONTAP 9.6 以降： *	`network interface show -service-policy default-intercluster -failover`
• ONTAP 9.5 以前： *	`network interface show -role intercluster -failover`

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、インタークラスタLIFおよび `cluster01_icl02`ポート上の `e0c`ポートがそのポートにフェイルオーバーする `e0d`ことを示しています `cluster01_icl01`。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

専用ポートでのONTAPクラスタ間LIFの設定

クラスタ間LIFは専用ポートに設定できます。これにより、通常、レプリケーショントラフィックに使用できる帯域幅が増加します。

手順

1. クラスタ内のポートの一覧を表示します。

   `network port show`

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、のネットワークポートを示してい `cluster01`ます。

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

2. クラスタ間通信専用に使用できるポートを特定します。

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

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

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

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

3. 専用ポートのフェイルオーバーグループを作成します。

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

次の例は、システムSVM上の `cluster01`フェイルオーバーグループに `intercluster01`ポートと `e0f`を割り当て `e0e`ます。

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

4. フェイルオーバーグループが作成されたことを確認します。

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

の詳細については `network interface failover-groups show`、を"ONTAPコマンド リファレンス"参照してください。

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

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

オプション	説明
• ONTAP 9.6 以降： *	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`
• ONTAP 9.5 以前： *	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group`

の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、クラスタ間LIFとを `cluster01_icl02`フェイルオーバーグループに `intercluster01`作成し `cluster01_icl01`ます。

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

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

6. クラスタ間LIFが作成されたことを確認します。

オプション	説明
• ONTAP 9.6 以降： *	`network interface show -service-policy default-intercluster`
• ONTAP 9.5 以前： *	`network interface show -role intercluster`

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

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

7. クラスタ間LIFが冗長構成になっていることを確認します。

オプション	説明
• ONTAP 9.6 以降： *	`network interface show -service-policy default-intercluster -failover`
• ONTAP 9.5 以前： *	`network interface show -role intercluster -failover`

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、クラスタ間LIFと `cluster01_icl02`SVMポート上のe0eポートがそのポートにフェイルオーバー `e0f`することを示しています `cluster01_icl01`。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

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

カスタム IPspace を作成すると、その IPspace 内のシステムオブジェクトのコンテナとして機能するシステム Storage Virtual Machine （ SVM ）が作成されます。この SVM は、作成した IPspace 内のすべてのクラスタ間 LIF のコンテナとして使用できます。新しい SVM の名前がカスタム IPspace と同じです。

手順

1. クラスタ内のポートの一覧を表示します。

   `network port show`

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、のネットワークポートを示してい `cluster01`ます。

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

2. クラスタにカスタム IPspace を作成します。

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

   次の例は、カスタムIPspaceを作成し `ipspace-IC1`ます。

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

の詳細については `network ipspace create`、を"ONTAPコマンド リファレンス"参照してください。

3. クラスタ間通信専用に使用できるポートを特定します。

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

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

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

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

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

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

   一度に複数のブロードキャストドメインにポートを配置することはできません。の詳細については `network port broadcast-domain remove-ports`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、デフォルトのブロードキャストドメインからポートとを `e0f`削除し `e0e`ます。

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

5. デフォルトのブロードキャストドメインからポートが削除されたことを確認します。

   `network port show`

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

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

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

6. カスタム IPspace にブロードキャストドメインを作成します。

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

   次の例は、IPspaceに `ipspace-IC1`ブロードキャストドメインを作成し `ipspace-IC1-bd`ます。

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

7. ブロードキャストドメインが作成されたことを確認します。

   `network port broadcast-domain show`

   の詳細については `network port broadcast-domain show`、を"ONTAPコマンド リファレンス"参照してください。

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

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

オプション	説明
• ONTAP 9.6 以降： *	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask`
• ONTAP 9.5 以前： *	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask`

LIF は、ホームポートが割り当てられているブロードキャストドメインに作成されます。ブロードキャストドメインには、そのドメインと同じ名前のデフォルトのフェイルオーバーグループがあります。の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、ブロードキャストドメインに `ipspace-IC1-bd`クラスタ間LIFと `cluster01_icl02`を作成し `cluster01_icl01`ます。

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

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

9. クラスタ間LIFが作成されたことを確認します。

オプション	説明
• ONTAP 9.6 以降：*	`network interface show -service-policy default-intercluster`
• ONTAP 9.5 以前：*	`network interface show -role intercluster`

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

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

10. クラスタ間LIFが冗長構成になっていることを確認します。

オプション	説明
• ONTAP 9.6 以降： *	`network interface show -service-policy default-intercluster -failover`
• ONTAP 9.5 以前： *	`network interface show -role intercluster -failover`

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、クラスタ間LIFと `cluster01_icl02`SVMポート上の `e0e`ポートが「e0f」ポートにフェイルオーバーすることを示しています `cluster01_icl01`。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

ピア関係の設定

ONTAPクラスタピア関係を作成します。

データバックアップやディザスタリカバリを目的としてリモートクラスタにデータをレプリケートしてデータを保護するには、ローカルクラスタとリモートクラスタの間にクラスタピア関係を作成する必要があります。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"スナップショット レプリケーションを作成してセットアップします。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

いくつかのデフォルトの保護ポリシーを使用できます。カスタムの保護ポリシーを使用する場合は、保護ポリシーを作成しておく必要があります。

開始する前に

ONTAP CLIを使用している場合は、次のいずれかの方法でピア関係にあるクラスタ内の各ノードにクラスタ間LIFを作成しておく必要があります。

- "共有データポートにクラスタ間LIFを設定"
- "専用データポートにクラスタ間LIFを設定"
- "カスタムIPspaceでのクラスタ間LIFの設定"

手順

このタスクは、ONTAPシステムマネージャまたはONTAP CLIを使用して実行します。

System Manager

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

   リモートクラスタでこの手順を繰り返します。
3. リモートクラスタで、*[クラスタ]>[設定]*をクリックします。
4. セクションをクリックし ⋮ 、[パスフレーズの生成]*を選択します。
5. リモートONTAPクラスタのバージョンを選択します。
6. 生成されたパスフレーズをコピーします。
7. ローカルクラスタで、**[クラスタピア]***で、[ピアクラスタ]をクリックし ⋮ て[ピアクラスタ]*を選択します。
8. ウィンドウで、パスフレーズを貼り付け、[クラスタピアリングの開始]*をクリックします。

CLI

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

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

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

   カスタムIPspaceを使用しない場合は、このオプションを無視してかまいません `-ipspace`。の詳細については `cluster peer create`、を"ONTAPコマンド リファレンス"参照してください。

   ONTAP 9 .6以降でピア関係を作成する場合に、クラスタ間ピアリング通信を暗号化しないようにするには、オプションを使用して暗号化を無効にする必要があります `-encryption-protocol -proposed none`。

   次の例は、リモートクラスタを指定せずにクラスタピア関係を作成し、SVMと `vs2`ローカルクラスタのピア関係を事前承認します `vs1`。

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

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

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

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

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

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

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

次の例は、リモートクラスタを指定せずにクラスタピア関係を作成し、SVMと `vs2`ローカルクラスタのピア関係を事前承認しますvs1。

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

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

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

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

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

の詳細については `cluster peer create`、を"ONTAPコマンド リファレンス"参照してください。

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

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

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタ ピア関係が作成されたことを確認します。

```
cluster peer show -instance
```

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

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

4. ピア関係にあるノードの接続状態とステータスを確認します。

```
cluster peer health show
```

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

ONTAPで実行するその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic（ONTAP 9 .7以前で使用可能）	"ボリュームのディザスタリカバリの準備の概要"

ONTAPクラスタ間**SVM**ピア関係を作成する

コマンドを使用すると、ローカルクラスタとリモートクラスタのSVM間にピア関係を作成できます `vserver peer create`。

開始する前に

- ソースクラスタとデスティネーションクラスタのピア関係が確立されている必要があります。
- リモートクラスタのSVMについて、「事前承認された」ピア関係が必要です。

  詳細については、を参照してください "クラスタピア関係の作成"。

タスクの内容

複数のSVMのピア関係を「事前承認」するには、SVMをリストします。 `-initial-allowed-vserver`クラスターピア関係を作成するときに選択します。詳細については、を参照してください "クラスタピア関係の作成"。

手順

1. データ保護のデスティネーションクラスタで、ピアリング用に事前承認されたSVMを表示します。

   `vserver peer permission show`

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

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

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

   の詳細については `vserver peer create`、を"ONTAPコマンド リファレンス"参照してください。

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

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

3. SVMピア関係を確認します。

   `vserver peer show`

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

ONTAPクラスタ間**SVM**ピア関係を追加

クラスタピア関係を設定したあとにSVMを作成する場合は、SVMのピア関係を手動で追加する必要があります。コマンドを使用すると、SVM間のピア関係を作成できます `vserver peer create`。ピア関係が作成されたら、をリモートクラスタで実行してピア関係を承認できます `vserver peer accept`。

開始する前に

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

タスクの内容

ローカルデータバックアップ用に、同じクラスタ内のSVM間にピア関係を作成できます。の詳細については `vserver peer create`、を"ONTAPコマンド リファレンス"参照してください。

管理者がコマンドを使用して、提示されたSVMピア関係を拒否することがあります `vserver peer reject`。SVM間の関係が状態になっている場合 `rejected`は、新しい関係を作成する前に関係を削除する必要があります。の詳細については `vserver peer reject`、を"ONTAPコマンド リファレンス"参照してください。

手順

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

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

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

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

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

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

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

   `vserver peer show-all`

   の詳細については `vserver peer show-all`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、SVMとSVM`vs1`の間のピア関係が開始されたことを示しています`pvs1`。

   ```
   cluster01::> vserver peer show-all
               Peer        Peer                          Peering
   Vserver     Vserver     State      Peer Cluster       Applications
   --------    --------    ---------  -------------      ------------
   pvs1        vs1         initiated   Cluster02           snapmirror
   ```

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

   `vserver peer show`

   の詳細については `vserver peer show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、の保留中のピア関係を表示し `cluster02`ます。

```
cluster02::> vserver peer show

                    Peer                Peer
Vserver             Vserver             State
-----------         -----------         ------------
vs1                 pvs1                pending
```

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

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

   の詳細については `vserver peer accept`、を"ONTAPコマンド リファレンス"参照してください。

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

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

5. SVMピア関係を確認します。

   `vserver peer show`

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

ピア関係に対して**ONTAP**クラスタピアリング暗号化を有効にする

ONTAP 9 .6以降では、新しく作成されるすべてのクラスタピア関係で、クラスタピアリングの暗号化がデフォルトで有効になります。クラスタピアリングの暗号化では、事前共有キー（PSK）とTransport Security Layer（TLS）を使用して、クラスタ間ピアリン

グ通信が保護されます。これにより、ピアクラスタ間のセキュリティが強化されます。

タスクの内容

ピアクラスタをONTAP 9 .6以降にアップグレードする場合、ONTAP 9 .5以前でピア関係が作成されているときは、アップグレード後にクラスタピアリングの暗号化を手動で有効にする必要があります。クラスタピアリングの暗号化を有効にするには、ピア関係の両方のクラスタでONTAP 9 .6以降が実行されている必要があります。

手順

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

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

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

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

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

の詳細については `cluster peer modify`、を"ONTAPコマンド リファレンス"参照してください。

ピア関係からONTAPクラスタピアリング暗号化を削除する

デフォルトでは、ONTAP 9 .6以降で作成されたすべてのピア関係に対してクラスタピアリングの暗号化が有効になります。クラスタ間ピアリング通信に暗号化を使用しない場合は、暗号化を無効にできます。

手順

1. デスティネーションクラスタで、クラスタピアリングの暗号化を中止するようにソースクラスタとの通信を変更します。
   - 認証を維持したまま暗号化を解除するには、

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

   - 暗号化と認証を解除するには：
     i. 認証されていないアクセスを許可するようにクラスタピアリングポリシーを変更します。

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

ii. 暗号化および認証アクセスを変更します。

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

2. プロンプトが表示されたらパスフレーズを入力します。
3. パスフレーズを再入力して確認のためにもう一度入力します。
4. ソースクラスタで、デスティネーションクラスタとの通信の暗号化を無効にします。
   - 認証を維持したまま暗号化を解除するには、

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

   - 暗号化と認証を解除するには：
     i. 認証されていないアクセスを許可するようにクラスタピアリングポリシーを変更します。

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

     ii. 暗号化および認証アクセスを変更します。

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

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

ローカル**Snapshot**を管理します。

ローカル**ONTAP**スナップショットの管理について

a_snapshot_は、読み取り専用のポイントインタイムボリュームイメージです。イメージには前回のSnapshot以降のファイルへの変更のみが記録されるため、ストレージスペースは最小限しか消費されず、パフォーマンスのオーバーヘッドもわずかです。

スナップショットを使用して、ボリュームの内容全体をリストアしたり、個 々 のファイルまたはLUNをリカバリしたりできます。スナップショットはボリューム上のディレクトリに保存されます。 `.snapshot`

ONTAP 9.4 以降では、 FlexVol volumeに最大 1023 個のスナップショットを含めることができます。 ONTAP 9.3 以前では、ボリュームには最大 255 個のスナップショットを含めることができます。

ONTAP 9.8以降では、FlexGroupボリュームに1023個のSnapshotを格納できます。詳細については、を参照してください "Snapshotを使用したFlexGroupボリュームの保護"。

ONTAPの長期保存スナップショットについて学ぶ

ポリシー タイプが「vault」または「mirror-vault」であるSnapMirror関係では、SnapMirror関係のセカンダリ ボリューム上にスナップショットを直接作成できます。これらのスナップショットは、バックアップとして保存先に保存されます。これらのスナップショットは長期保存用に作成されることが多く、長期保存 (LTR) スナップショットと呼ばれます。

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

長期保存スナップショットは、 FlexVol SnapMirror構成でのみ使用できます。 FlexGroup SnapMirror構成ではLTR スナップショットを作成することはできません。

SnapMirrorカスケード関係では、長期保存スナップショットはカスケードの最後のボリュームにのみ作成できます。

関連情報

- "カスケード展開の仕組みについて学ぶ"
- "ONTAP SnapMirrorスケジュールを定義してデスティネーションにローカルコピーを作成する"

カスタムSnapshotポリシーの設定

カスタムのONTAP Snapshotポリシーの設定の詳細

a_snapshot policy_システムによるスナップショットの作成方法を定義しますこのポリシーは、Snapshotを作成するタイミング、保持するコピーの数、およびSnapshotに名前を付ける方法を指定します。たとえば、毎日午前12時10分にSnapshotを1つ作成し、最新の2つのコピーを保持して、それらのコピーに「毎日」という名前を付けることができます.*timestamp*。

ボリュームのデフォルトポリシーでは、次のスケジュールでSnapshotが自動的に作成され、新しいコピー用のスペースを確保するために最も古いSnapshotが削除されます。

- 最大6つの時間単位のスナップショットが毎時5分に作成されます。
- 最大2つの日次スナップショットが月曜日から土曜日の午前0時10分に作成されます。
- 最大2つの週単位Snapshotが毎週日曜日の午前0時15分に作成されます。

ボリュームの作成時にSnapshotポリシーを指定しなかった場合は、そのボリュームを含むStorage Virtual Machine（SVM）に関連付けられているSnapshotポリシーが継承されます。

カスタムの**ONTAP Snapshot**ポリシーを設定するタイミング

デフォルトのSnapshotポリシーがボリュームに適していない場合は、Snapshotの頻度、保持期間、および名前を変更するカスタムポリシーを設定できます。スケジュールは、主にアクティブファイルシステムの変更率によって決まります。

使用頻度の高いファイルシステムは 1 時間ごとにデータベースのようにバックアップし、ほとんど使用されないファイルは 1 日に 1 回バックアップします。データベースであっても、通常は 1 日に 1~2 回フルバックアップを実行しますが、トランザクションログのバックアップは 1 時間ごとに行います。

その他の要因としては、組織におけるファイルの重要性、サービスレベルアグリーメント（ SLA ）、目標復旧時点（ RPO ）、および目標復旧時間（ RTO ）があります。一般的に、Snapshotは必要な数だけ保持してください。

ONTAP Snapshotジョブスケジュールの作成

Snapshotポリシーには、Snapshotジョブスケジュールが少なくとも1つ必要です。System Managerまたはコマンドを使用して、ジョブスケジュールを作成できます `job schedule cron create`。の詳細については `job schedule cron create`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"スナップショット ジョブ スケジュールを作成します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

デフォルトでは、ONTAPは、ジョブスケジュール名にタイムスタンプを追加してSnapshotの名前を作成します。

日にちと曜日の両方に値を指定すると、それぞれ個別に判断されます。たとえば、dayを指定し、dayを指定`13`したcronスケジュール `Friday`は、13日の金曜日だけでなく、各月の毎週金曜日と13日に実行されます。

例 **30.** 手順

System Manager

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

CLI

1. ジョブスケジュールを作成します。

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

`-dayofweek`、および `-hour`では `-month`、ジョブを毎月、曜日、および時間ごとに実行するように指定できます `all`。

ONTAP 9 .10.1以降では、ジョブスケジュールにSVMを含めることができます。

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

次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `myweekly`。

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

次の例は、という名前のスケジュールを作成し、 `myweeklymulti`複数の日、時間、および分を指定します。

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

ONTAP Snapshotポリシーを作成します。

Snapshotポリシーは、Snapshotを作成するタイミング、保持するコピーの数、およ

びSnapshotに名前を付ける方法を指定します。たとえば、毎日午前12時10分にSnapshotを1つ作成し、最新の2つのコピーを保持して「daily」という名前を付けます。Snapshotポリシーには最大5つのジョブスケジュールを含めることができます `.timestamp`。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"スナップショット ポリシーを作成します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

デフォルトでは、ONTAPは、ジョブスケジュール名にタイムスタンプを追加してSnapshotの名前を作成します。

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

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

```
`snapmirror-label`オプションは
SnapMirrorレプリケーション用です。詳細については、を参照してください
xref:{relative_path}define-rule-policy-task.html["ポリシーのルールの定義"]。
```

手順

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

System Manager

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

CLI

1. Snapshotポリシーを作成します。

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

次の例は、スケジュールに基づいて実行する `daily`という`Snapshot`ポリシーを作成します `snap_policy_daily`。このポリシーには最大5つのSnapshotがあり、それぞれに名前とSnapMirrorラベルが `daily`付いてい `daily.`*timestamp*`ます。

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

Snapshotを手動で管理する

スナップショットを手動で作成および削除する

スケジュールされたSnapshotが作成されるのを待たずに手動でSnapshotを作成したり、不要になったSnapshotを削除したりできます。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"オンデマンド スナップショットを作成します。ASAr2 システムは、SAN のみのお客様向けに簡素化

された ONTAP エクスペリエンスを提供します。

スナップショットを手動で作成する

SnapshotはSystem ManagerまたはONTAP CLIを使用して手動で作成できます。

System Manager

手順

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

CLI

1. Snapshotを作成します。

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

Snapshotの手動削除

SnapshotはSystem ManagerまたはONTAP CLIを使用して手動で削除できます。

System Manager

手順

1. [ストレージ]>[ボリューム]に移動し、[Snapshotコピー]*タブを選択します。
2. 削除するSnapshotを探してをクリックし、*[削除]*を選択します。
3. ウィンドウで、[スナップショットの削除]*を選択します。
4. [削除（ Delete ）] をクリックします。

CLI

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

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

この例では、コマンドを実行すると、SVM vs3内のボリュームvol3上のSnapshotが表示されます。

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

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

2. Snapshotを削除します。

状況	入力するコマンド
単一のSnapshotを削除する	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

状況	入力するコマンド
複数のスナップショットの削除	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
すべてのSnapshotを削除	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

Snapshotを削除する前に再利用可能なスペースを計算

ONTAP 9.10.1以降では、System Managerを使用して、削除するSnapshotを選択し、削除前に再利用可能なスペースを計算できます。

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. Snapshotを削除するボリュームを選択します。
3. *スナップショット*をクリックします。
4. 1つ以上のSnapshotを選択します。
5. [再計算可能スペースを計算（ Calculate Reclaimable Space ）] をクリックします。

Snapshotリザーブの管理

ONTAPスナップショットリザーブの管理について

スナップショット予約_は'スナップショット用にディスク領域のパーセンテージ(デフォルトでは5%)を確保しますスナップショットリザーブを使い切ると、スナップショットはアクティブファイルシステムの領域を使用するため、必要に応じてスナップショットリザーブを増やすことができます。また、リザーブがいっぱいになったときにスナップショットを自動削除することもできます。

Snapshotリザーブを増やすタイミング

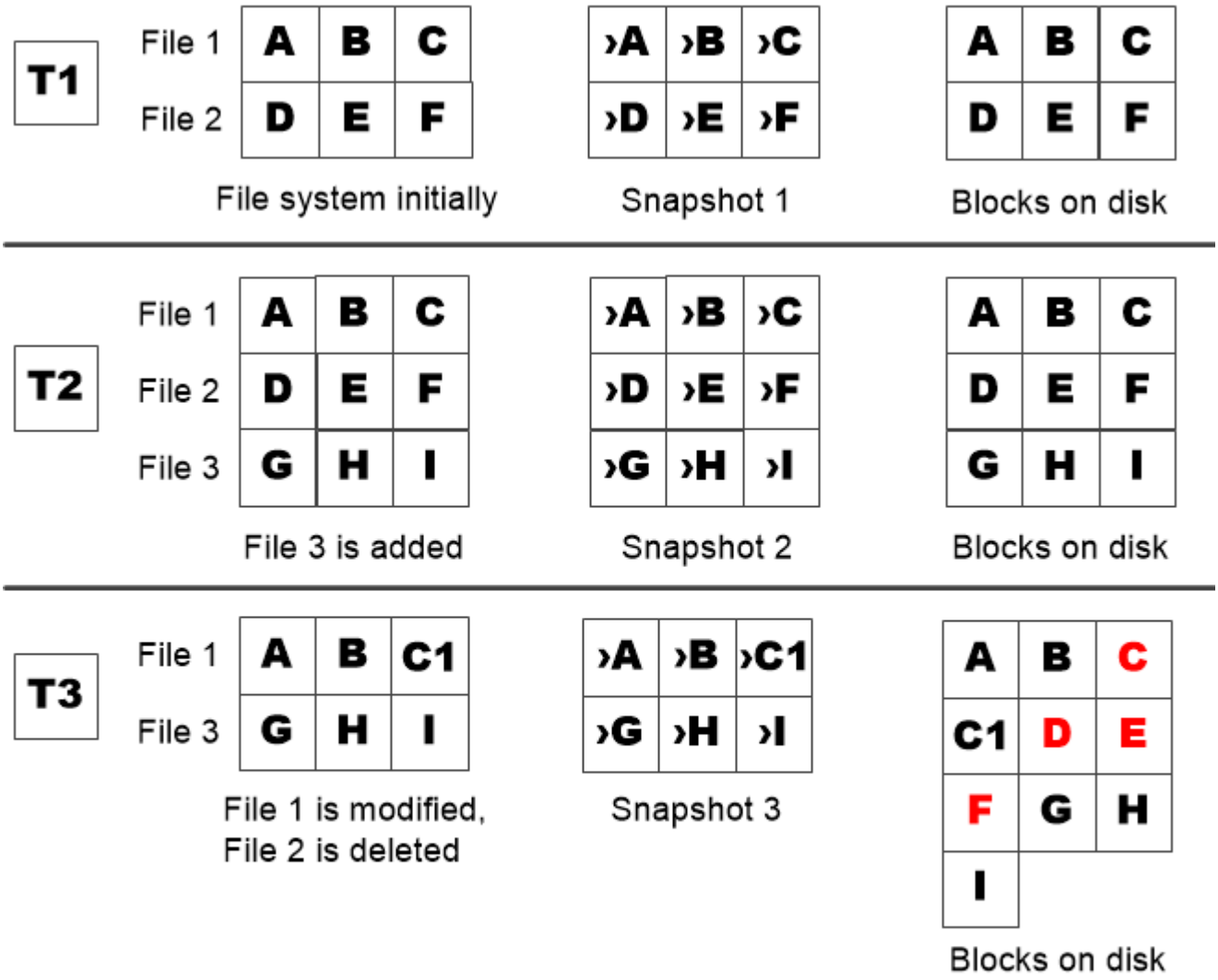
スナップショット予約を増やすかどうかを決定する際には、スナップショットが記録されるのは、最後のスナップショットが作成されてからのファイルへの変更のみであることを覚えておくことが重要です。ディスクスペースが消費されるのは、アクティブファイルシステム内のブロックが変更または削除された場合だけです。

つまり、スナップショットによって使用されるディスクスペースの量を決定する際には、ファイルシステムの

変更率が重要な要素となります。作成するSnapshotの数に関係なく、アクティブファイルシステムが変更されていない場合、Snapshotはディスクスペースを消費しません。

たとえば、データベーストランザクションログを含むFlexVol volumeでは、変更率の増加に対応するために20%のSnapshotリザーブを確保できます。データベースへの頻繁な更新をキャプチャするために、より多くのスナップショットを作成するだけでなく、スナップショットが消費する追加のディスク容量を処理するために、より大きなスナップショット予約も必要になります。

Snapshotは、ブロックのコピーではなくブロックへのポインタで構成されます。ポインタはブロック上の「要求」と考えることができます。ONTAPは、Snapshotが削除されるまでブロックを「保持」します。



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

ホコタイシヨウノファイルノサクシヨニヨルファイルスヘスカシヨウキヨウ

スナップショットは、そのブロックを使用していたファイルを削除したあとも、そのブロックを参照しています。これは、スナップショット予約を使い果たした場合、ファイルシステム全体を削除すると、ファイルシステムが占有しているよりも使用可能なスペースが少なくなるという直感に反する結果につながる可能性がある

理由を説明しています。

次の例を考えてみましょう。ファイルを削除する前の `df`コマンド出力は次のとおりです。

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

ファイルシステム全体を削除してボリュームのSnapshotを作成すると、 `df`次の出力が生成されます。

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

この出力に示されているように、削除前に使用されていた0.5GBに加えて、アクティブファイルシステムで使用されていた3GB全体がSnapshotで使用されています。

スナップショットによって使用されるディスク領域がスナップショットリザーブを超えているため、アクティブファイル用に予約された領域に2.5 GBの「錠剤」がオーバーフローし、3 GBを想定していたファイル用に0.5 GBの空き領域が残ります。

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

ONTAPスナップショットによるディスク使用状況の監視

Snapshotのディスク使用状況は、コマンドを使用して監視できます `df`。コマンドは、アクティブファイルシステムとSnapshotリザーブの空きスペースの量を表示します。

ステップ

1. スナップショットのディスク使用状況を表示します。 `df`

   次の例は、Snapshotによるディスク使用状況を示しています。

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

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

ボリューム上の使用可能な**ONTAP**スナップショット予約の確認

コマンドでパラメータを `volume show`使用すると、ボリュームで使用可能

なSnapshotリザーブの容量を確認できます `snapshot-reserve-available`。の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. ボリュームで使用可能なSnapshotリザーブを確認します。

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

   次の例は、の使用可能なSnapshotリザーブを表示し `vol1`ます。

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

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

ONTAPスナップショット予約の変更

アクティブファイルシステム用に予約されたスペースをスナップショットが使用しないように、より大きなスナップショット予約を構成することができます。スナップショット用の容量が不要になった場合は、スナップショット予約を減らすことができます。

ステップ

1. Snapshotリザーブを変更します。

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

   の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

   次の例では、のSnapshotリザーブを10%に設定し `vol1`ます。

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

ONTAP Snapshotの自動削除

コマンドを使用すると、Snapshotリザーブを超過したときにSnapshotの自動削除をトリガーできます `volume snapshot autodelete modify`。デフォルトでは、最も古いSnapshotから順に削除されます。の詳細については `volume snapshot autodelete modify`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

LUNクローンとファイルクローンは、削除するSnapshotがなくなると削除されます。

ステップ

1. Snapshotの自動削除：

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

   次の例では、Snapshotリザーブを使い切った場合にのSnapshotを自動削除し `vol1`ます。

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

スナップショットからファイルをリストア

NFSまたは**SMB**クライアント上の**ONTAP**スナップショットからファイルをリストアする

NFSまたはSMBクライアントのユーザは、ストレージシステム管理者の手を借りなくても、Snapshotから直接ファイルをリストアできます。

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

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

各サブディレクトリには、スナップショットによって参照されるファイルが含まれています。ユーザが誤ってファイルを削除または上書きした場合、snapshotサブディレクトリから読み書き可能ディレクトリにファイルをコピーすることで、読み書き可能な親ディレクトリにファイルをリストアできます。

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

ONTAPスナップショットディレクトリへのNFSおよびSMBクライアントアクセスの有効化と無効化

ディレクトリへのアクセスは、コマンドのONTAP CLIオプションを `volume modify` 使用して有効または無効にできます `-snapdir-access`。ONTAP 9.10.1以降では、System Managerを使用してクライアントシステムからボリュームのSnapshotディレクトリへのアクセスを有効または無効にできます。アクセスを有効にすると、クライアントからはSnapshotディレクトリが表示され、Windowsクライアントからは、Snapshotディレクトリにドライブをマッピングしてその内容を表示およびアクセスできるようになります。その後、NFSクライアントとSMBクライアントは、Snapshotからファイルまたは LUNをリストアできます。

ボリュームのSnapshotディレクトリへのアクセスを有効または無効にするには、ボリュームの設定を編集するか、ボリュームの共有設定を編集します。

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

手順

ONTAPシステムマネージャまたはONTAP CLIを使用して、クライアントのSnapshotディレクトリへのアクセスを有効または無効にできます。デフォルトでは、ボリューム上のsnapshotディレクトリにクライアントからアクセスできます。

System Manager

1. [ストレージ]>[ボリューム]*をクリックします。
2. 表示または非表示にするSnapshotディレクトリを含むボリュームを選択します。
3. をクリック ⋮ し、*[編集]*を選択します。
4. スナップショット (ローカル) 設定 セクションで、スナップショット ディレクトリをクライアントに表示する を選択または選択解除します。
5. [保存（ Save ）] をクリックします。

CLI

1. Snapshotディレクトリのアクセスステータスを確認します。

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

例：

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

の詳細については `volume show`、を"ONTAPコマンド リファレンス"参照してください。

2. Snapshotディレクトリへのアクセスを有効または無効にします。

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

次の例は、vol1でSnapshotディレクトリへのアクセスを有効にします。

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

の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

共有の編集による**Snapshot**ディレクトリへのクライアントアクセスの有効化または無効化

デフォルトでは、ボリューム上のsnapshotディレクトリにクライアントからアクセスできます。

手順

1. [* ストレージ] 、 [共有] の順にクリックします。
2. 表示または非表示にするSnapshotディレクトリを含むボリュームを選択します。
3. をクリック ⋮ し、*[編集]*を選択します。
4. [共有のプロパティ]*セクションで、[クライアントにスナップショットディレクトリへのアクセスを許可する]*を選択または選択解除します。
5. [保存（ Save ）] をクリックします。

ONTAPスナップショットから単一ファイルをリストアする

コマンドを使用すると、Snapshotから単一のファイルまたはLUNをリストアできます `volume snapshot restore-file`。既存のファイルを置き換えない場合は、読み書き可能な親ボリュームの別の場所にファイルをリストアできます。

タスクの内容

既存のLUNをリストアする場合は、LUNクローンが作成され、Snapshotの形式でバックアップされます。リストア処理中に、LUNに対する読み取りと書き込みを実行できます。

デフォルトでは、ストリームを含むファイルがリストアされます。

手順

1. ボリューム内のSnapshotを一覧表示します。

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

   の詳細については `volume snapshot show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、のSnapshotを示してい `vol1`ます。

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

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

7 entries were displayed.
```

2. スナップショットからファイルをリストアします。

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

   の詳細については `volume snapshot restore-file`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、ファイルをリストアし `myfile.txt`ます。

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

ONTAPスナップショットからファイルの一部をリストアする

コマンドを使用すると、SnapshotからLUN、またはNFS / SMBコンテナファイルに一定の範囲のデータをリストアできます `volume snapshot partial-restore-file`。ただし、データの開始バイトオフセットとバイト数がわかっている必要があります。このコマンドは、同じLUNに複数のデータベースが格納されているホスト上のいずれかのデータベースをリストアする場合に使用します。

ONTAP 9.12.1以降では、を使用するボリュームに対して部分リストアをSnapMirrorアクティブ同期実行できます。

手順

1. ボリューム内のSnapshotを一覧表示します。

   `volume snapshot show -vserver SVM -volume volume`

   の詳細については `volume snapshot show`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、のSnapshotを示してい `vol1`ます。

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

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

7 entries were displayed.
```

2. Snapshotからファイルの一部をリストアします。

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

   開始バイトオフセットとバイト数は 4 、 096 の倍数でなければなりません。

   次に、ファイルの最初の4、096バイトをリストアする例を示し `myfile.txt`ます。

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

ONTAP Snapshotからボリュームの内容をリストアする

Snapshotからリストアすることで、ボリュームを過去のある時点の状態にリカバリできます。System Managerまたはコマンドを使用して、Snapshotからボリュームの内容をリストアできます `volume snapshot restore`。の詳細については `volume snapshot restore`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

ボリュームにSnapMirror関係がある場合は、Snapshotからリストアしたあとすぐに、ボリュームのすべてのミラーコピーを手動でレプリケートします。ミラーコピーを使用しないと、ミラーコピーを使用できなくなり、削除および再作成が必要になる可能性があります。

手順

以前のSnapshotからリストアするには、System ManagerまたはONTAP CLIを使用します。

System Manager

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

CLI

1. ボリューム内のSnapshotを一覧表示します。

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

次の例は、のSnapshotを示してい `vol1`ます。

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

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

7 entries were displayed.
```

2. Snapshotからボリュームの内容をリストアします。

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

次の例は、の内容をリストアし `vol1`ます。

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

SnapMirrorボリュームのレプリケーション

SnapMirrorボリュームレプリケーションの詳細

ONTAP SnapMirror非同期ディザスタリカバリの詳細

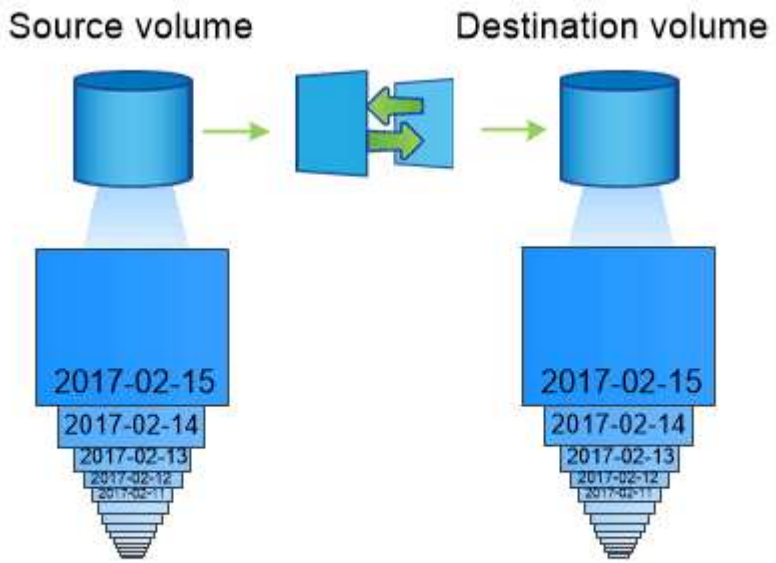
_ SnapMirror _は、地理的に離れたサイトのプライマリストレージからセカンダリストレージへのフェイルオーバー用に設計されたディザスタリカバリテクノロジです。名前が示すように、 SnapMirror はセカンダリストレージに作業データのレプリカ（ _mirror ）を作成します。このデータから、プライマリサイトで災害が発生した場合にもデータの提供を継続できます。

プライマリサイトから引き続きデータを提供できる場合は、必要なデータをプライマリサイトに戻すだけで、ミラーからクライアントを提供することはできません。フェイルオーバーのユースケースが示すように、ミラーリングされたストレージからデータを効率的に提供するには、セカンダリシステムのコントローラがプライマリシステムのコントローラと同等またはほぼ同等である必要があります。

データ保護関係

データはボリュームレベルでミラーリングされます。プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、_データ保護関係と呼ばれます。_ボリュームが配置されているクラスタと、ボリュームからデータを提供するSVMは、である必要があります。"ピアリング完了"ピア関係にあることで、クラスタとSVM間でデータをセキュアにやり取りできます。

次の図は、SnapMirrorデータ保護関係を示しています。



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

データ保護関係の範囲

データ保護関係は、ボリューム間で直接作成することも、ボリュームを所有するSVM間で作成することもできます。SVM のデータ保護関係では、 SVM のすべてまたは一部の設定が NFS エクスポートおよび SMB 共有から RBAC にレプリケートされます。また、 SVM が所有するボリューム内のデータもレプリケートされます。

SnapMirrorは、次の特殊なデータ保護アプリケーションにも使用できます。

- SVM ルートボリュームの負荷共有ミラーコピーを作成すると、ノードに障害やフェイルオーバーが発生したときに引き続きデータにアクセスできます。
- SnapLock ボリューム間のデータ保護関係： WORM ファイルをセカンダリストレージにレプリケートできます。

  "SnapLockテクノロジを使用したアーカイブとコンプライアンス"

- ONTAP 9 .13.1以降では、SnapMirror非同期を使用して保護できます整合グループ。ONTAP 9.14.1以降では、SnapMirror非同期を使用して、整合性グループ関係を使用してボリューム単位のSnapshotをデスティネーションクラスタにレプリケートできます。詳細については、を参照してください SnapMirror非同期保護の設定。

SnapMirrorデータ保護関係を初期化する方法

SnapMirror を初めて起動すると、ソース・ボリュームからデスティネーション・ボリュームへの _ ベースライン転送 _ が実行されます。関係の _SnapMirror ポリシー _ は、ベースラインおよび更新の内容を定義します。

デフォルトのSnapMirrorポリシーに基づくベースライン転送 `MirrorAllSnapshots`では、次の手順を実行します。

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

SnapMirrorデータ保護関係を更新する方法

更新は、設定したスケジュールに従って非同期に行われます。保持期間は、ソース上のSnapshotポリシーをミラーリングします。

ポリシーに基づく更新のたびに `MirrorAllSnapshots`、SnapMirrorはソースボリュームのSnapshotを作成し、そのSnapshotと前回の更新後に作成されたすべてのSnapshotを転送します。次のポリシーのコマンドの `MirrorAllSnapshots`出力では `snapmirror policy show`、次の点に注意してください。

- `Create Snapshot`は「`true`」で、`SnapMirror`が関係を更新するときに`Snapshot`が作成されることを示します `MirrorAllSnapshots`。
- `MirrorAllSnapshots`には、「sm_created」および「all_source_snapshots」というルールがあります。これは、SnapMirrorが関係を更新するときに、SnapMirrorで作成されたSnapshotと前回の更新以降に作成されたSnapshotの両方が転送されることを示します。

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

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

MirrorLatestポリシー

事前設定され `MirrorLatest`たポリシーは、SnapMirrorで作成されたSnapshotのみが初期化および更新時に転送される点を除き、とまったく同じように機能し `MirrorAllSnapshots`ます。

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

関連情報

- "snapmirror policy show"

ONTAP SnapMirror同期ディザスタリカバリの詳細

ONTAP 9 .5以降では、SnapMirror Synchronous（SM-S）テクノロジが、16 GB以上の

メモリを搭載したすべてのFASおよびAFFプラットフォーム、およびすべてのONTAP Selectプラットフォームでサポートされています。SnapMirror同期テクノロジはノード単位でライセンスされる機能で、ボリュームレベルの同期データレプリケーションを提供します。

この機能は、データ損失ゼロが求められる金融、医療などの規制対象の業界で、同期レプリケーションに関する規制や国の要件に対応します。

許可される**SnapMirror**同期処理

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

次の表に、プラットフォームタイプおよびONTAPリリース別に、HAペアごとに実行できるSnapMirror同期処理の数を示します。

プラットフォーム	ONTAP 9.14.1 からONTAP 9.11.1	ONTAP 9 10.1	ONTAP 9 .9.1	ONTAP 9.9.1より前のリリース
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

サポートされる機能

次の表に、SnapMirror同期およびONTAPリリースでサポートされる機能を示します。

機能	最初にサポートされたリリース	追加情報
SnapMirror同期関係のプライマリボリュームに対するウィルス対策	ONTAP 9.6	
アプリケーションで作成されたSnapshotレプリケーション	ONTAP 9.7	スナップショットに適切なラベルが付けられている場合は、 `snapshot create` CLI またはONTAP API を使用した操作では、 SnapMirror は、アプリケーションを停止した後、ユーザーが作成したスナップショットと外部スクリプトで作成されたスナップショットの両方を同期的に複製します。スナップショット ポリシーを使用して作成されたスケジュールされたスナップショットは複製されません。アプリケーションが作成したスナップショットの複製の詳細については、"NetAppナレッジベース: アプリケーションが作成したスナップショットをSnapMirror同期で複製する方法" 。
クローンの自動削除	ONTAP 9.6	

階層化ポリシーが「なし」、「Snapshot」、または「自動」のFabricPoolアグリゲートは、SnapMirror同期のソースとデスティネーションでサポートされます。	ONTAP 9.5	FabricPoolアグリゲートのデスティネーションボリュームを「すべて」の階層化ポリシーに設定することはできません。
FC	ONTAP 9.5	レイテンシが10ミリ秒を超えないすべてのネットワーク
FC-NVMe	ONTAP 9.7	
フアイルクロン	ONTAP 9.7	
SnapMirror同期関係のプライマリボリュームに対するFPolicy	ONTAP 9.6	
SnapMirror同期関係のプライマリボリュームに対するハードクォータとソフトクォータ	ONTAP 9.6	クォータルールはデスティネーションにレプリケートされないため、クォータデータベースはデスティネーションにレプリケートされません。
クラスタ内同期関係	ONTAP 9 .14.1	高可用性は、ソースボリュームとデスティネーションボリュームが別 々 のHAペアに配置されている場合に提供されます。クラスタ全体が停止すると、クラスタがリカバリされるまでボリュームにアクセスできなくなります。クラスタ内のSnapMirror同期関係が、同時処理の全体的な制限にHAペアあたりの関係数影響します。
iSCSI	ONTAP 9.5	
LUNクローンとNVMeネームスペースクローン	ONTAP 9.7	
アプリケーションで作成されたSnapshotによってバックアップされるLUNクローン	ONTAP 9.7	
混在プロトコルアクセス（NFS v3とSMB）	ONTAP 9.6	
NDMP / NDMPリストア	ONTAP 9 .13.1	でSnapMirror同期を使用するには、ソースクラスタとデスティネーションクラスタの両方でONTAP 9が実行されている必要があります。詳細については、を参照してください NDMPコピーを使用してデータを転送します。
AFF / ASAプラットフォームでのみ、無停止のSnapMirror同期処理（NDO）を実行できます。	ONTAP 9 12.1	ノンストップオペレーションをサポートしているため、ダウンタイムのスケジュールを設定することなく、一般的なメンテナンスタスクの多くを実行できます。サポートされる処理には、テイクオーバーとギブバック、およびボリューム移動があります（2つのクラスタのそれぞれで1つのノードが稼働している場合）。
NFS v4.2	ONTAP 9 10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	

NVMe / TCP	9.10.1	
メタデータ処理頻度の上限の削除	ONTAP 9.6	
TLS 1.2暗号化を使用した機密データの転送中のセキュリティ	ONTAP 9.6	
単一ファイルおよび部分ファイルのリストア	ONTAP 9 .13.1	
SMB 2.0以降	ONTAP 9.6	
SnapMirror同期ミラー-ミラーカスケード	ONTAP 9.6	SnapMirror同期関係のデスティネーションボリュームからの関係は、SnapMirror非同期関係である必要があります。
SVMディザスタリカバリ	ONTAP 9.6	* SnapMirror同期ソースは、SVMディザスタリカバリソースにすることもできます。たとえば、SnapMirror同期を一方のレッグとして、SVMディザスタリカバリをもう一方のレッグとして使用するファンアウト構成などです。* SnapMirror同期はデータ保護ソースのカスケードをサポートしていないため、SnapMirror同期ソースをSVMディザスタリカバリデスティネーションにすることはできません。デスティネーションクラスタでSVMディザスタリカバリのフリップ再同期を実行する前に、同期関係を解放する必要があります。* SVMディザスタリカバリではDPボリュームのレプリケーションがサポートされないため、SnapMirror同期デスティネーションをSVMディザスタリカバリソースにすることはできません。同期ソースの逆再同期を実行すると、SVMディザスタリカバリでデスティネーションクラスタのDPボリュームが除外されます。
ソースボリュームへのテープベースのリストア	ONTAP 9 .13.1	
NASのソースボリュームとデスティネーションボリューム間のタイムスタンプパリティ	ONTAP 9.6	ONTAP 9 .5からONTAP 9 .6にアップグレードした場合、タイムスタンプはソースボリューム内の新規および変更されたファイルについてのみレプリケートされます。ソースボリューム内の既存のファイルのタイムスタンプは同期されません。

サポートされない機能

SnapMirror同期関係では、次の機能はサポートされません。

- 整合グループ
- DP_Optimized（DPO）システム
- FlexGroupホリユウム
- FlexCacheホリユウム
- グローバルスロットル
- ファンアウト構成では、SnapMirror同期関係にできる関係は1つだけで、ソースボリュームからのその他の関係はすべてSnapMirror非同期関係にする必要があります。

- LUNノイトウ
- MetroClusterコウセイ
- SANアクセスLUNとNVMeアクセスLUNとNVMeネームスペースの混在は、同じボリュームまたはSVMではサポートされていません。
- SnapCenter
- SnapLockボリューム
- スナップショットの改ざん防止
- デスティネーションボリュームでのダンプとSMTapeを使用したテープバックアップまたはリストア
- ソースボリュームのスループットの下限（最小QoS）
- ボリュームSnapRestore
- VVol

動作モード

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

- * Syncモード* Syncモードでは'アプリケーションI/O処理はプライマリ・ストレージ・システムとセカンダリ・ストレージ・システムに並行して送信されます何らかの理由でセカンダリストレージへの書き込みが完了しなかった場合、アプリケーションはプライマリストレージへの書き込みを続行できます。エラー状態が修正されると、SnapMirror同期テクノロジは自動的にセカンダリストレージと再同期し、プライマリストレージからセカンダリストレージへのレプリケーションを同期モードで再開します。Syncモードでは、セカンダリレプリケーションに障害が発生するまでRPO=0とRTOは非常に低くなります。障害が発生すると、RPOとRTOは不確定になりますが、セカンダリレプリケーションに失敗した原因となった問題を修復して再同期が完了するまでの時間と同じです。
- * StrictSyncモード* SnapMirror同期は、オプションでStrictSyncモードで動作できます。何らかの理由でセカンダリストレージへの書き込みが完了しないと、アプリケーションI/Oが失敗し、プライマリストレージとセカンダリストレージが同一であることが保証されます。プライマリへのアプリケーションI/Oは、SnapMirror関係が `InSync`ステータスに戻るまで再開されません。プライマリストレージに障害が発生しても、フェイルオーバー後にデータを失うことなく、セカンダリストレージでアプリケーションI/Oを再開できます。StrictSyncモードでは、RPOは常にゼロであり、RTOは非常に低くなります。

関係のステータス

SnapMirror同期関係のステータスは、 `InSync`通常運用時は常にの状態になります。何らかの理由でSnapMirror転送が失敗した場合、デスティネーションはソースと同期されておらず、 `OutofSync`ステータスがになる可能性があります。

SnapMirror同期関係の場合は、 `InSync` `OutofSync`一定の間隔で関係のステータスまたは）が自動的にチェックされます。関係のステータスがの場合、 `OutofSync`ONTAPは自動再同期プロセスを自動的にトリガーして関係を `InSync`ステータスに戻します。自動再同期は、ソースまたはデスティネーションでの計画外のストレージフェイルオーバーやネットワークの停止などの処理が原因で転送が失敗した場合にのみトリガーされます。 `snapmirror quiesce`やなどの処理をユーザが開始した `snapmirror break`場合、自動再同期はトリガーされません。

`OutofSync`StrictSyncモードでSnapMirror同期関係のステータスがになると、プライマリボリュームに対するI/O処理がすべて停止します。 `OutofSync`同期モードでのSnapMirror同期関係の状態はプライマリに影響を与えず、プライマリボリュームでI/O処理が許可されます。

関連情報

- "NetAppテクニカルレポート4733：『SnapMirror synchronous configuration and best practices』"
- "スナップミラーの破損"
- "スナップミラーの静止"

デフォルトの**ONTAP**データ保護ポリシー

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

デフォルトのポリシーではデータ保護関係のニーズを満たせない場合は、対応できます"カスタムポリシーを作成する"。

デフォルトの保護ポリシーと説明のリスト

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

名前	説明	ポリシータイプ
非同期	SnapMirrorの非同期バックアップポリシー。最新のアクティブファイルシステムと日単位および週単位のSnapshotを1時間の転送スケジュールでミラーリングします。	非同期
AutomatedFailOver（自動フェールオーバー）	レプリケーションに失敗してもクライアントI/Oが中断されない、RTOゼロのSnapMirror同期ポリシー。	同期
AutomatedFailOverDuplex	SnapMirror同期ポリシー（RTOゼロ保証、双方向の同期レプリケーション）	同期
CloudBackupDefault	dailyルールを含むバックアップポリシー。	非同期
継続的	S3バケットのミラーリング用のポリシー。	継続的
DailyBackup	日次ルールと日次転送スケジュールが設定されたバックアップポリシー。	非同期
DPDefault	すべてのSnapshotと最新のアクティブファイルシステムをミラーリングするSnapMirror非同期ポリシー。	非同期
MirrorAllSnapshots	すべてのSnapshotと最新のアクティブファイルシステムをミラーリングするSnapMirror非同期ポリシー。	非同期
MirrorAllSnapshotsDiscardNetwork	すべてのSnapshotと最新のアクティブファイルシステム（ネットワーク構成を除く）をミラーリングするためのSnapMirror非同期ポリシー。	非同期

名前	説明	ポリシータイプ
MirrorAndVault	最新のアクティブファイルシステムと日単位および週単位のSnapshotをミラーリングするための、SnapMirrorの非同期およびバックアップポリシーです。	非同期
MirrorAndVaultDiscardNetwork	SnapMirrorの非同期バックアップポリシー。最新のアクティブファイルシステムと、日単位と週単位のSnapshot（ネットワーク設定を除く）をミラーリングします。	非同期
MirrorLatest	最新のアクティブファイルシステムをミラーリングするためのSnapMirror非同期ポリシー。	非同期
SnapCenterSync	アプリケーションで作成されたSnapshot設定を使用するSnapCenter用SnapMirror同期のポリシー。	同期
StrictSync	レプリケーションエラー時にクライアントアクセスが中断されるSnapMirror同期のポリシー。	同期
同期	レプリケーションエラー時にクライアントアクセスが中断されないSnapMirror同期のポリシー。	同期
ユニファイド7年	7年間保持するユニファイドSnapMirrorポリシー	非同期
XDPDefault	日次ルールと週次ルールを含むバックアップポリシー。	非同期

ONTAP StrictSyncポリシーと**Sync**ポリシーでサポートされるワークロードの詳細

StrictSyncポリシーとSyncポリシーでは、FC、iSCSI、FC-NVMeの各プロトコルを使用したLUNベースのすべてのアプリケーションに加え、データベース、VMware、クォータ、SMBなどのエンタープライズアプリケーションについてはNFSv3プロトコルとNFSv4プロトコルがサポートされます。ONTAP 9 .6以降では、EDA（電子設計自動化）、ホームディレクトリ、ソフトウェアビルドワークロードなどのエンタープライズファイルサービスにSnapMirror同期を使用できます。

Sync.5では、ONTAP 9ポリシーでNFSv3またはNFSv4ワークロードを選択する際に、いくつかの重要な側面について考慮する必要があります。ワークロードによる読み取り/書き込み処理のデータ量は、Syncポリシーでは高い読み取り/書き込みIOワークロードを処理できるため、考慮する必要はありません。ONTAP 9 .5では、ファイルの作成、ディレクトリの作成、ファイル権限の変更、ディレクトリ権限の変更が大量に発生するワークロード（「メタデータ比率の高いワークロード」と呼ばれます）は適さない場合があります。メタデータ比率の高いワークロードの典型的な例は、複数のテストファイルを作成し、自動化を実行してファイルを削除するDevOpsワークロードです。もう1つの例は、コンパイル時に複数の一時ファイルを生成する並列ビルドワークロードです。メタデータの書き込みアクティビティの比率が高いと、ミラー間の同期が一時的に解除され、クライアントからの読み取りI/Oと書き込みI/Oが停止する可能性があります。

ONTAP 9 .6以降ではこれらの制限がなくなり、ホームディレクトリやソフトウェアビルドワークロードなどのマルチユーザ環境を含むエンタープライズファイルサービスのワークロードにSnapMirror同期を使用できるようになりました。

関連情報

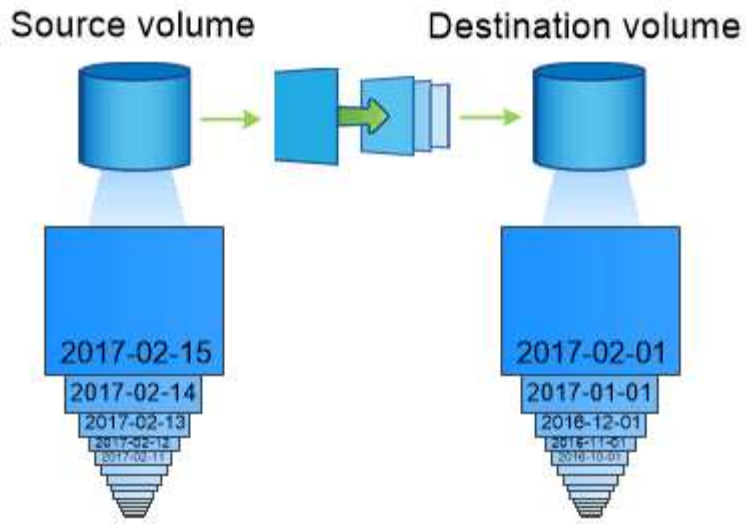
"SnapMirror同期の設定とベストプラクティス"

ONTAP SnapMirrorテクノロジを使用したヴォールトアーカイブの詳細

SnapMirrorバックアップポリシーは、ONTAP 9.3以降のSnapVaultテクノロジに代わるものです。SnapMirrorバックアップポリシーは、標準への準拠やその他のガバナンス関連の目的で、ディスクツーディスクのSnapshotレプリケーションに使用します。SnapMirror関係では通常、ソースボリューム内のSnapshotのみがデスティネーションに含まれますが、SnapVaultデスティネーションでは、より長期間にわたって作成されたポイントインタイムSnapshotが保持されます。

たとえば、ビジネスに関する政府会計規制に準拠するために、データの月次スナップショットを20年間にわたって保持することができます。SnapVaultストレージからデータを提供する必要はないため、デスティネーションシステムでは低速で低コストのディスクを使用できます。

次の図は、SnapMirrorのバックアップデータ保護関係を示しています。



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

バックアップデータ保護関係を初期化する方法

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

デフォルトのバックアップポリシーに基づくベースライン転送では `XDPDefault`、ソースボリュームのSnapshotが作成され、そのコピーおよびコピーが参照するデータブロックがデスティネーションボリュームに転送されます。SnapMirror関係とは異なり、バックアップバックアップにはベースラインに古いSnapshotは含まれません。

バックアップデータ保護関係を更新する方法

更新は、設定したスケジュールに従って非同期に行われます。関係のポリシーで定義するルールによって、更新に含める新しいSnapshotと保持するコピーの数が決まります。ポリシーで定義されたラベル（「毎月」など）は、ソースのSnapshotポリシーで定義された1つ以上のラベルと一致する必要があります。そうしないと、レプリケーションが失敗します。

ポリシーに基づく更新のたびに、 XDPDefault`SnapMirrorは前回の更新以降に作成されたSnapshotを転送します（Snapshotのラベルがポリシールールで定義されたラベルに一致する場合）。次のポリシーのコマンドの `XDPDefault`出力では `snapmirror policy show、次の点に注意してください。

- Create Snapshot`は「false」で、SnapMirrorによる関係の更新時にSnapshotが作成されないことを示します。 `XDPDefault
- `XDPDefault`には、「daily」および「weekly」というルールがあります。これは、SnapMirrorが関係を更新するときに、ソース上のラベルが一致するすべてのSnapshotが転送されることを示します。

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

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

関連情報

- "snapmirror policy show"

ONTAP SnapMirrorユニファイドレプリケーションの詳細

SnapMirror_unified replication _ は、同じデスティネーションボリュームでディザスタリカバリとアーカイブを設定できます。ユニファイドレプリケーションが適切な場合は、必要なセカンダリストレージの量を削減し、ベースライン転送の数を制限し、ネットワークトラフィックを削減できます。

一元化されたデータ保護関係を初期化する方法

SnapMirrorと同様に、一元化されたデータ保護機能を初めて起動したときにベースライン転送が実行されます。関係のSnapMirrorポリシーは、ベースラインと更新の内容を定義します。

デフォルトの一元化されたデータ保護ポリシーに基づくベースライン転送では `MirrorAndVault`、ソースボリュームのSnapshotが作成され、そのコピーおよびコピーが参照するデータブロックがデスティネーションボリュームに転送されます。バックアップアーカイブと同様に、一元化されたデータ保護ではベースラインに古いSnapshotは含まれません。

一元化されたデータ保護関係を更新する方法

ポリシーに基づく更新のたびに `MirrorAndVault`、SnapMirrorはソースボリュームのSnapshotを作成し、そのSnapshotと前回の更新後に作成されたSnapshot（Snapshotポリシーのルールで定義されたラベルに一致するラベルがある場合）を転送します。次のポリシーのコマンドの `MirrorAndVault`出力では `snapmirror policy show`、次の点に注意してください。

- `Create Snapshot`は「`true`」で、`SnapMirror`が関係を更新するときに`Snapshot`が作成されることを示します `MirrorAndVault`。
- `MirrorAndVault`には、「sm_created」、「daily」、および「weekly」というルールがあります。これは、SnapMirrorが関係を更新するときに、SnapMirrorで作成されたSnapshotとソース上のラベルが一致するSnapshotの両方が転送されることを示します。

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

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

Unified7year ポリシー

事前設定された `Unified7year`ポリシーは、とまったく同じように機能します。ただし、4番目のルールでは、 `MirrorAndVault`月単位のSnapshotが転送され、7年間保持されます。

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

データ破損の可能性からデータを保護

ユニファイドレプリケーションでは、ベースライン転送の内容が、初期化時にSnapMirrorで作成されたSnapshotに制限されます。更新のたびに、SnapMirrorはソースのSnapshotをもう1つ作成し、そのSnapshotと、Snapshotポリシーのルールで定義されたラベルに一致するラベルを持つ新しいSnapshotを転送します。

最後に転送されたSnapshotのコピーをデスティネーションに作成することで、更新されたSnapshotが破損する可能性を防ぐことができます。この「ローカルコピー」はソース上の保持ルールに関係なく保持されるため、SnapMirrorによって転送されたSnapshotがソースで使用できなくなった場合でも、そのコピーをデスティネーションで使用できます。

ユニファイドデータレプリケーションを使用する状況

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

ユニファイドレプリケーションが適切かどうかを判断する際の重要な要素は、アクティブファイルシステムの変更率です。たとえば、データベーストランザクションログの時間単位のSnapshotを保持するボリュームには、従来のミラーの方が適している場合があります。

関連情報

- "snapmirror policy show"

ONTAPデータ保護のデスティネーションボリュームが自動的に拡張されるタイミング

ソースボリュームが拡張された場合、デスティネーションボリュームを含むアグリゲートに利用可能なスペースがあれば、データ保護ミラー転送の実行時にデスティネーションボリュームのサイズが自動的に拡張されます。

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

デフォルトでは、データ保護ボリュームはオートサイズモードに設定され `grow_shrink`ます。オートサイズモードでは、使用済みスペースの量に応じてボリュームが拡張または縮小されます。データ保護ボリューム

のmax-autosizeはFlexVolの最大サイズと同じで、プラットフォームによって異なります。例：

- FAS8200：DPボリュームのデフォルトのmax-autosize = 100TB

詳細については、を参照してください "NetApp Hardware Universe"。

ONTAPデータ保護のファンアウト構成とカスケード構成の詳細

a_fan-out_deployment を使用すると、データ保護を複数のセカンダリシステムに拡張できます。a_cascade _deployment を使用して、データ保護を 3 次システムに拡張できます。

ファンアウト構成とカスケード構成はどちらも、SnapMirror DR、SnapVault、ユニファイドレプリケーションの任意の組み合わせをサポートします。ONTAP 9.5以降では、SnapMirror同期関係で1つ以上のSnapMirror非同期関係を使用したファンアウト構成がサポートされます。ファンアウト構成でSnapMirror同期関係にできる関係は1つだけで、ソースボリュームからの残りの関係はすべてSnapMirror非同期関係にする必要があります。SnapMirror同期関係はカスケード構成もサポートされます（ONTAP 9.6以降）。ただし、SnapMirror同期関係のデスティネーションボリュームからの関係はSnapMirror非同期関係である必要があります。SnapMirrorアクティブ同期（ONTAP 9.13.1以降でサポート）では、ファンアウト構成もサポートされます。

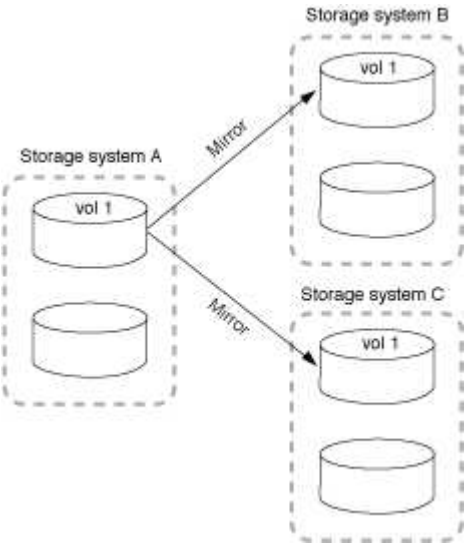
ファンイン導入を使用すると、複数のプライマリシステムと単一のセカンダリシステムの間にデータ保護関係を作成できます。各関係で、セカンダリシステム上の異なるボリュームを使用する必要があります。

ファンアウト構成またはカスケード構成に含まれているボリュームの再同期には時間がかかる可能性があることに注意してください。ステータスが「準備中」と長時間報告されるSnapMirror関係が表示されることも珍しくありません。

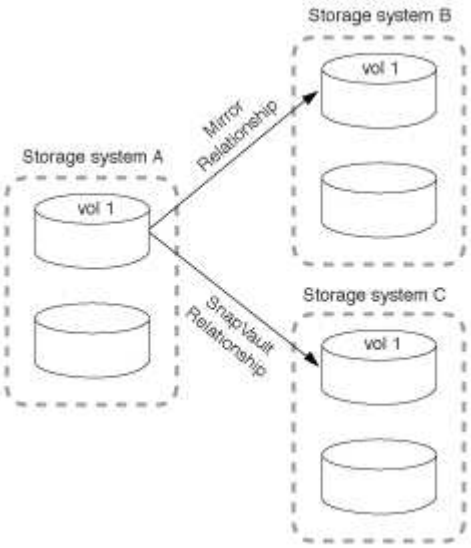
ファンアウト構成の仕組み

SnapMirror は、 _ multiple-mirrors _ および _ mirror -vault_fan-out 構成をサポートします。

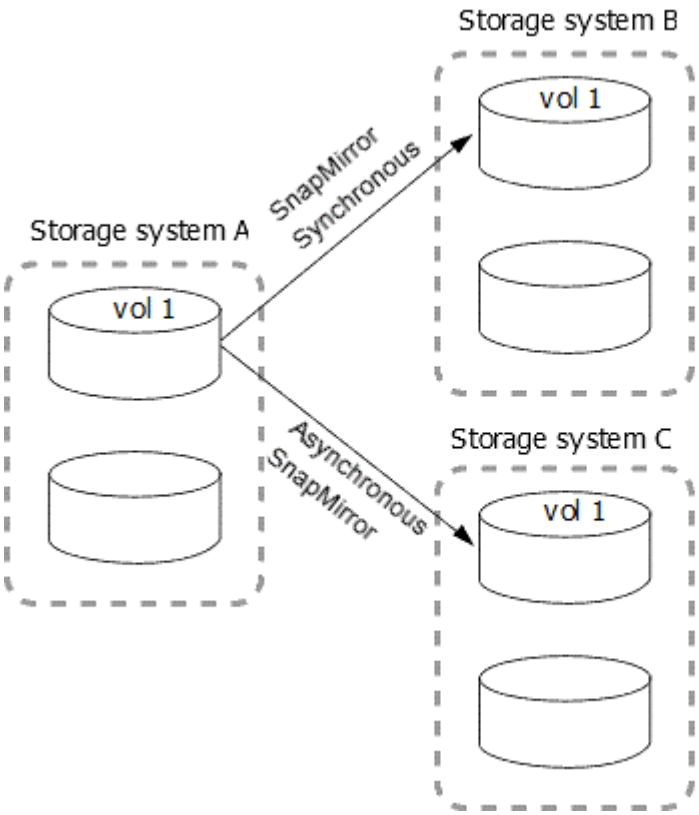
複数ミラーファンアウト構成では、ソースボリュームから複数のセカンダリボリュームへのミラー関係が確立されます。



ミラー-ヴォールトファンアウト構成では、ソースボリュームからセカンダリボリュームへのミラー関係と、別のセカンダリボリュームへのSnapVault関係が確立されます。



ONTAP 9 5以降では、ファンアウト構成でSnapMirror同期関係を確立できます。ただし、ファンアウト構成で確立できるSnapMirror同期関係は1つだけで、ソースボリュームからのその他の関係はすべてSnapMirror非同期関係にする必要があります。



カスケード構成の仕組み

SnapMirror は、 _ mirror - 、 _ mirror - vault_ 、 *vault - mirror* 、 _vault-vault-cascade の構成をサポートしています。

ミラー-ミラーカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームにミラーリ

ングされ、そのセカンダリボリュームが3番目のボリュームにミラーリングされます。セカンダリボリュームが使用できなくなった場合は、新しいベースライン転送を実行せずに、プライマリボリュームと3番目のボリュームの間の関係を同期できます。

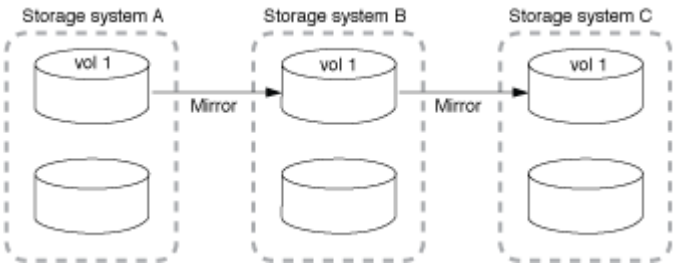
カスケード ボリュームの関係では、 ONTAP 9 のすべてのバージョンにおいて、長期保存 (LTR) スナップショットはカスケードの最後のSnapMirror宛先ボリュームでのみサポートされます。カスケード内の中間のボリュームで LTR スナップショットを有効にすると、バックアップとスナップショットが失われます。カスケードの中間ボリュームでLTRスナップショットが有効になっているサポートされていない構成の場合は、テクニカルサポートに連絡して、"NetAppナレッジベース: 長期保存 (LTR) スナップショットが有効になっているボリュームのカスケード接続はサポートされていません"援助をお願いします。

次のONTAPバージョンでは、最終的なSnapMirror宛先ボリュームを除くカスケード内のどのボリュームでもLTR スナップショットを有効にできません。

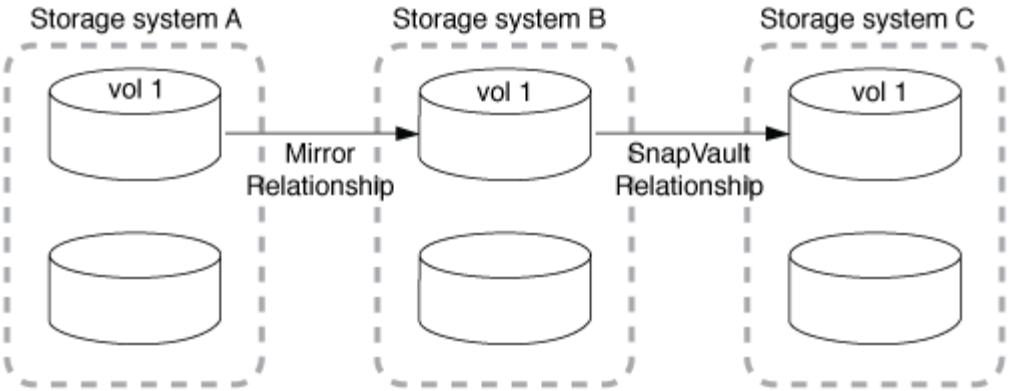
- 9.15.1以降
- 9.14.1P2およびP4からP14
- 9.13.1P9からP17
- 9.12.1 P12からP19
- 9.11.1P15からP20
- 9.10.1P18からP20
- 9.9.1P20

詳細はこちら"長期保存スナップショット"。

ONTAP 9 .6以降では、ミラー-ミラーカスケード構成でSnapMirror同期関係がサポートされます。SnapMirror同期関係を確立できるのは、プライマリボリュームとセカンダリボリュームだけです。セカンダリボリュームと3番目のボリュームの関係は非同期である必要があります。



ミラー-ヴォールトカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームにミラーリングされ、そのセカンダリボリュームが3番目のボリュームに保存されます。



Vault-mirror および Vault-Vault カスケード展開もサポートされています。

- ヴォールト-ミラーカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームに保存され、そのセカンダリボリュームが3番目のボリュームにミラーリングされます。
- ヴォールト - ヴォールトカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームに保存され、そのセカンダリボリュームが 3 番目のボリュームに保存されます。

関連情報

- SnapMirrorアクティブな同期を使用してファンアウト構成で保護を再開

ONTAP SnapMirrorのライセンスについて

ONTAP 9 .3以降では、ONTAPインスタンス間のレプリケーションのライセンスが簡易化されました。ONTAP 9リリースでは、SnapMirrorライセンスでバックアップ関係とミラー関係の両方がサポートされます。SnapMirrorライセンスを使用すると、バックアップとディザスタリカバリの両方のユースケースでONTAPレプリケーションをサポートできます。

ONTAP 9.3より前のリリースでは、ONTAPインスタンス間の_vault_relationshipsには別のSnapVault ONTAPライセンスが必要でした。この場合、DPインスタンスが保持期間の長いバックアップユースケースに対応するためにより多くのSnapshotを保持できるように、ONTAPインスタンス間の_mirror_relationshipsにはSnapMirrorライセンスが必要でした。ONTAP 8.xおよび9.xリリースでは、SnapMirrorライセンスとSnapVaultライセンスの両方が引き続き使用され、サポートされます。

SnapVaultライセンスは引き続き機能し、ONTAP 8.xと9.xの両方のリリースでサポートされますが、SnapMirrorライセンスをSnapVaultライセンスの代わりに使用して、ミラー構成とバックアップ構成の両方に使用できます。

ONTAP非同期レプリケーションの場合、ONTAP 9 .3以降では、単一のユニファイドレプリケーションエンジンを使用して拡張データ保護モード（XDP）ポリシーがSnapMirror設定されます。XDPライセンスは、ミラーポリシー、バックアップポリシー、またはミラーバックアップポリシーに対して設定できます。ソースとデスティネーションの両方のクラスタにSnapMirrorライセンスが必要です。SnapVaultライセンスは、SnapMirrorライセンスがすでにインストールされている場合は必要ありません。SnapMirror非同期永久ライセンスは、新しいAFFおよびFASシステムにインストールされるONTAP ONEソフトウェアスイートに含まれています。

データ保護設定の制限は、ONTAPのバージョン、ハードウェアプラットフォーム、インストールされているライセンスなど、いくつかの要因で決まります。詳細については、を参照してください "Hardware Universe"。

SnapMirror同期ライセンス

ONTAP 9 .5以降では、SnapMirror同期関係がサポートされます。SnapMirror同期関係を作成するには、次のライセンスが必要です。

- ソースクラスタとデスティネーションクラスタの両方にSnapMirror同期ライセンスが必要です。

  SnapMirror同期ライセンスはに含まれてい"ONTAP Oneライセンススイート"ます。

  2019年6月より前にPremium BundleまたはFlash Bundleでシステムを購入した場合は、NetAppサポートサイトからNetAppマスターキーをダウンロードして、必要なSnapMirror同期ライセンスを取得できます "マスターライセンスキー"。

- ソースクラスタとデスティネーションクラスタの両方にSnapMirrorライセンスが必要です。

SnapMirrorクラウドライセンス

ONTAP 9.8以降では、SnapMirrorクラウドライセンスが、ONTAPインスタンスからオブジェクトストレージエンドポイントへのSnapshotの非同期レプリケーションを提供します。レプリケーションターゲットは、オンプレミスのオブジェクトストアとS3およびS3互換のパブリッククラウドオブジェクトストレージサービスの両方を使用して設定できます。SnapMirrorのクラウド関係は、ONTAPシステムから認定済みのオブジェクトストレージターゲットへサポートされます。

SnapMirror Cloudはスタンドアロンライセンスとしては提供されていません。1つのONTAPクラスタに必要なライセンスは1つだけです。SnapMirrorクラウドライセンスに加えて、SnapMirror非同期ライセンスも必要です。

SnapMirrorクラウド関係を作成するには、次のライセンスが必要です。

- オブジェクトストアエンドポイントに直接レプリケートするためのSnapMirrorライセンスとSnapMirrorクラウドライセンスの両方。
- マルチポリシーレプリケーションワークフロー（ディスクツーディスクツークラウドなど）を設定する場合は、すべてのONTAPインスタンスにSnapMirrorライセンスが必要です。一方、SnapMirrorクラウドライセンスは、オブジェクトストレージエンドポイントに直接レプリケートするソースクラスタにのみ必要です。

ONTAP 9.9.1以降では、 "System Managerを使用したSnapMirrorクラウドレプリケーション" 。

認定されたSnapMirrorクラウドサードパーティアプリケーションのリストは、NetAppのWebサイトで公開されています。

Data Protection Optimizedライセンス

Data Protection Optimized（DPO）ライセンスの販売は終了し、現在のプラットフォームではDPOはサポートされません。ただし、サポート対象のプラットフォームにDPOライセンスがインストールされている場合、NetAppはそのプラットフォームの販売終了までサポート提供を継続します。

DPOはONTAP Oneライセンス バンドルには含まれていないため、DPOライセンスがシステムにインストールされている場合はONTAP Oneライセンス バンドルにアップグレードできません。

サポートされるプラットフォームの詳細については、を参照してください "Hardware Universe"。

ONTAP DPOシステムの機能拡張

ONTAP 9.6以降では、DP_Optimized（DPO）ライセンスをインストールすると、サポートされるFlexVolの最大数が増加します。ONTAP 9.4以降では、DPOライセンスのあるシステムでSnapMirrorバックオフ、ボリューム間のバックグラウンド重複排除、ドナーとしてのSnapshotブロックの使用、およびコンパクションがサポートされます。

ONTAP 9.6 以降では、セカンダリシステムまたはデータ保護システムでサポートされる FlexVol の最大数が増加し、 FlexVol ボリュームをノードあたり最大 2 、 500 個まで、フェイルオーバーモードでは最大 5 、 000 個まで拡張できるようになりました。FlexVolボリュームの増加はで有効になります"DP_Optimized（DPO）ライセンス"。ソースノードとデスティネーションノードの両方には引き続きが"SnapMirrorライセンス"必要です。

DPO .4以降では、ONTAP 9システムの次の機能拡張が行われています。

- SnapMirror バックオフ： DPO システムでは、レプリケーショントラフィックにクライアントのワークロードと同じ優先度が与えられます。

  SnapMirrorバックオフは、DPOシステムではデフォルトで無効になっています。

- ボリュームのバックグラウンド重複排除とボリューム間のバックグラウンド重複排除： DPO システムでは、ボリュームのバックグラウンド重複排除とボリューム間のバックグラウンド重複排除が有効になります。

  既存データを重複排除するには、コマンドを実行し `storage aggregate efficiency cross-volume-dedupe start -aggregate *aggregate_name* -scan-old-data true`ます。パフォーマンスへの影響を少なくするために、このコマンドはピーク時を避けて実行することを推奨します。

  の詳細については `storage aggregate efficiency cross-volume-dedupe start`、を"ONTAP コマンド リファレンス"参照してください。

- Snapshotブロックをドナーとして使用することによる削減効果：アクティブなファイルシステムでは使用できないがSnapshotに含まれているデータブロックは、ボリューム重複排除のドナーとして使用されます。

  Snapshotにトラップされたデータと新しいデータを重複排除することができるため、Snapshotブロックを効率的に共有することもできます。ドナースペースを増やすと、特にボリュームに多数のSnapshotがある場合は、削減効果が高まります。

- コンパクション： DPO システムでは、データコンパクションはデフォルトで有効になります。

ONTAP SnapMirrorコマンドでのパス名のパターンマッチングについて

パターンマッチングを使用すると、コマンドでソースパスとデスティネーションパスを指定できます `snapmirror`。

`snapmirror`コマンドでは、という形式の完全修飾パス名を使用します `vserver:volume`。SVM 名を入力せずにパス名を省略できます。省略した場合、`snapmirror`コマンドではユーザのローカルSVMコンテキストが使用されます。

SVMの名前が「vserver1」、ボリュームの名前が「vol1」とすると、完全修飾パス名はになります `vserver1:vol1`。

パス名にアスタリスク（*）をワイルドカードとして使用すると、一致する完全修飾パス名を選択できます。次の表に、ワイルドカードを使用して特定範囲のボリュームを選択する例を示します。

`*`	すべてのパスに一致します。
`vs*`	SVM名の先頭がであるすべてのSVMおよびボリュームが一致します `vs`。
`:*src`	ボリューム名にテキストが含まれているすべてのSVMが一致します `src`。
`:vol`	ボリューム名の先頭がであるすべてのSVMが一致します `vol`。

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source               Destination  Mirror        Relationship  Total
Last
Path          Type   Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapMirror関係処理の拡張クエリについて説明します。

拡張クエリを使用すると、複数の SnapMirror 関係に対して SnapMirror 処理を一度に実行できます。たとえば、初期化されていない SnapMirror 関係が複数ある場合に、それらの関係を 1 つのコマンドで初期化できます。

タスクの内容

拡張クエリは、次の SnapMirror 処理に適用できます。

- 初期化されていません
- 休止されていた関係を再開

- 解除した関係を再同期して
- アイドル状態の関係を更新中です
- 関係のデータ転送を中止しています

ステップ

1. 多数の関係に対して SnapMirror 処理を実行します。

   snapmirror command {-state state } *

   次のコマンドは、状態のSnapMirror関係を初期化し `Uninitialized`ます。

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   の詳細については snapmirror initialize、を"ONTAPコマンド リファレンス"参照してください。

SnapMirror関係に互換性がある**ONTAP**のバージョン

SnapMirrorデータ保護関係を作成する前に、ソースボリュームとデスティネーションボリュームで互換性のあるONTAPバージョンが実行されている必要があります。ONTAPをアップグレードする前に、現在のONTAPバージョンがSnapMirror関係のターゲットのONTAPバージョンと互換性があることを確認する必要があります。

ユニファイドレプリケーション関係

「 xdmp` 」タイプの SnapMirror 関係では、オンプレミスまたは Cloud Volumes ONTAP リリースを使用します。

ONTAP 9 .9.0以降：

- ONTAP 9 .x.0リリースはクラウドのみのリリースであり、Cloud Volumes ONTAPシステムをサポートします。リリースバージョンのあとにアスタリスク（*）が表示されている場合、クラウドのみのリリースです。

  ONTAP 9.16.0は、をサポートするため、クラウドのみのルールの例外です。"ASA r2システム"リリースバージョンのあとのプラス記号（+）は、ASA R2でサポートされているリリースを示します。ASA R2システムでは、他のASA R2システムとのSnapMirror関係のみがサポートされます。

- ONTAP 9 .x.1リリースは一般リリースであり、オンプレミスシステムとCloud Volumes ONTAPシステムの両方をサポートします。

  いる場合、"高度な容量分散"ONTAP 9.16.1以降を実行しているクラスタのボリュームでが有効になってONTAP 9.16.1より前のバージョンのONTAPを実行しているクラスタへのSnapMirror転送はサポートされません。

  双方向の互換性があります。

• ONTAPバージョン 9.4 以降の相互運用性*

ONTAP バージョン…	ONTAP の以前のバージョンとの相互運用性…																				
	9.17.1	9.16.1	9.16.0以上	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4
9.17.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.0以上	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.0*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.14.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.14.0*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.13.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ

9.13.0*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ
9.12.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.12.0*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	いいえ	いいえ
9.11.1	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.11.0*	いいえ	いいえ	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	いいえ	いいえ
9.10.1	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.10.0*	いいえ	いいえ	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ
9.9.1	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.9.0*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	いいえ
9.8	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.7	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ

9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*

SnapMirror同期関係

SnapMirror同期は、ONTAPクラウドインスタンスではサポートされません。

ONTAPバージョン…	ONTAP の以前のバージョンとの相互運用性…												
	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.17.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.14.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.13.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.12.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.11.1	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ
9.10.1	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.9.1	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.8	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ

9.7	いいえ	いいえ	いいえ	いいえ	* はい *	* はい *	いいえ	いいえ	* はい *	* はい *	* はい *	* はい *	* はい *	
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	* はい *	* はい *	* はい *	* はい *	
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	* はい *	* はい *	* はい *	

SnapMirror SVMディザスタリカバリ関係

SVMディザスタリカバリのデータと**SVM**保護の場合：

SVMディザスタリカバリは、同じバージョンのONTAPを実行するクラスタ間でのみサポートされます。バージョンに依存しないレプリケーションは**SVM**レプリケーションではサポートされません。

SVM移行のための**SVM**ディザスタリカバリの場合：

- ソース上のONTAPの以前のバージョンから、デスティネーション上のONTAPの同じバージョンまたはそれ以降のバージョンへのレプリケーションが単一方向でサポートされます。
- 次の表に示すように、ターゲットクラスタのONTAPのオンプレミスバージョンが2つ以上ないか、クラウドのメジャーバージョンが2つ以上ないようにする必要があります（ONTAP 9.9.0以降）。
  - 長期的なデータ保護のユースケースでは、レプリケーションはサポートされません。

リリースバージョンのあとにアスタリスク（*）が表示されている場合、クラウドのみのリリースです。

サポートを確認するには、左側の表の列でソースバージョンを確認し、一番上の行でデスティネーションバージョンを確認します（類似バージョンの場合はDR/Migration、新しいバージョンの場合はMigrationのみ）。

ソース	デスティネーション																				
	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1
9.4	DR/移行	移行	移行																			
9.5		DR/移行	移行	移行																		
9.6			DR/移行	移行	移行																	
9.7				DR/移行	移行	移行																
9.8					DR/移行	移行	移行															

9.9.0*						DR/移行	移行	移行	移行	移行	移行										
9.9.1							DR/移行	移行	移行	移行	移行										
9.10.0*								DR/移行	移行	移行	移行	移行	移行								
9.10.1									DR/移行	移行	移行	移行	移行								
9.11.0*										DR/移行	移行	移行	移行	移行	移行						
9.11.1											DR/移行	移行	移行	移行	移行						
9.12.0*												DR/移行	移行	移行	移行	移行	移行				
9.12.1													DR/移行	移行	移行	移行	移行				
9.13.0*														DR/移行	移行	移行	移行	移行	移行		
9.13.1															DR/移行	移行	移行	移行	移行		
9.14.0*																DR/移行	移行	移行	移行	移行	
9.14.1																	DR/移行	移行	移行	移行	移行	
9.15.0*																		DR/移行	移行	移行	移行	移行
9.15.1																			DR/移行	移行	移行	移行
9.16.0																				DR/移行	移行	移行
9.16.1																					DR/移行	移行

9.1 7.1																					DR /移 行

SnapMirrorテイサスタリカハリカンケイ

タイプが「 `D」 でポリシータイプが「 async 」の SnapMirror 関係の場合：

DPタイプのミラーは、ONTAP 9 .11.1以降では初期化できません。ONTAP 9 12.1では完全に廃止されています。詳細については、を参照してください "データ保護SnapMirror関係の廃止"。

次の表で、左側の列はソースボリュームのONTAPバージョン、上部の列はデスティネーションボリュームで使用できるONTAPバージョンを示しています。

ソース	デスティネーション								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.10.1	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.9.1	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.8	いいえ	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ
9.7	いいえ	いいえ	○	○	○	いいえ	いいえ	いいえ	いいえ
9.6	いいえ	いいえ	いいえ	○	○	○	いいえ	いいえ	いいえ
9.5	いいえ	いいえ	いいえ	いいえ	○	○	○	いいえ	いいえ
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	○	○	○	いいえ
9.3	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	○	○	○

双方向の互換性はありません。

ONTAP SnapMirrorの制限事項

データ保護関係を作成する前に、SnapMirrorの基本的な制限事項を確認しておく必要があります。

- 1つのデスティネーションボリュームに設定できるソースボリュームは1つだけです。

  1つのソースボリュームに複数のデスティネーションボリュームを含めることができます。デスティネーションボリュームは、あらゆるタイプのSnapMirrorレプリケーション関係のソースボリュームにすることができます。

- アレイモデルに応じて、1つのソースボリュームから最大8個または16個のデスティネーションボリュームをファンアウトできます。特定の構成の詳細については、を参照してください"Hardware Universe"。
- SnapMirror DR関係のデスティネーションにファイルをリストアすることはできません。
- ソースまたはデスティネーションのSnapVaultボリュームを32ビットにすることはできません。

- SnapVault関係のソースボリュームをFlexCloneボリュームにすることはできません。

  関係は機能しますが、FlexCloneが提供する効率化機能は維持されません。

SnapMirrorボリュームレプリケーションの設定

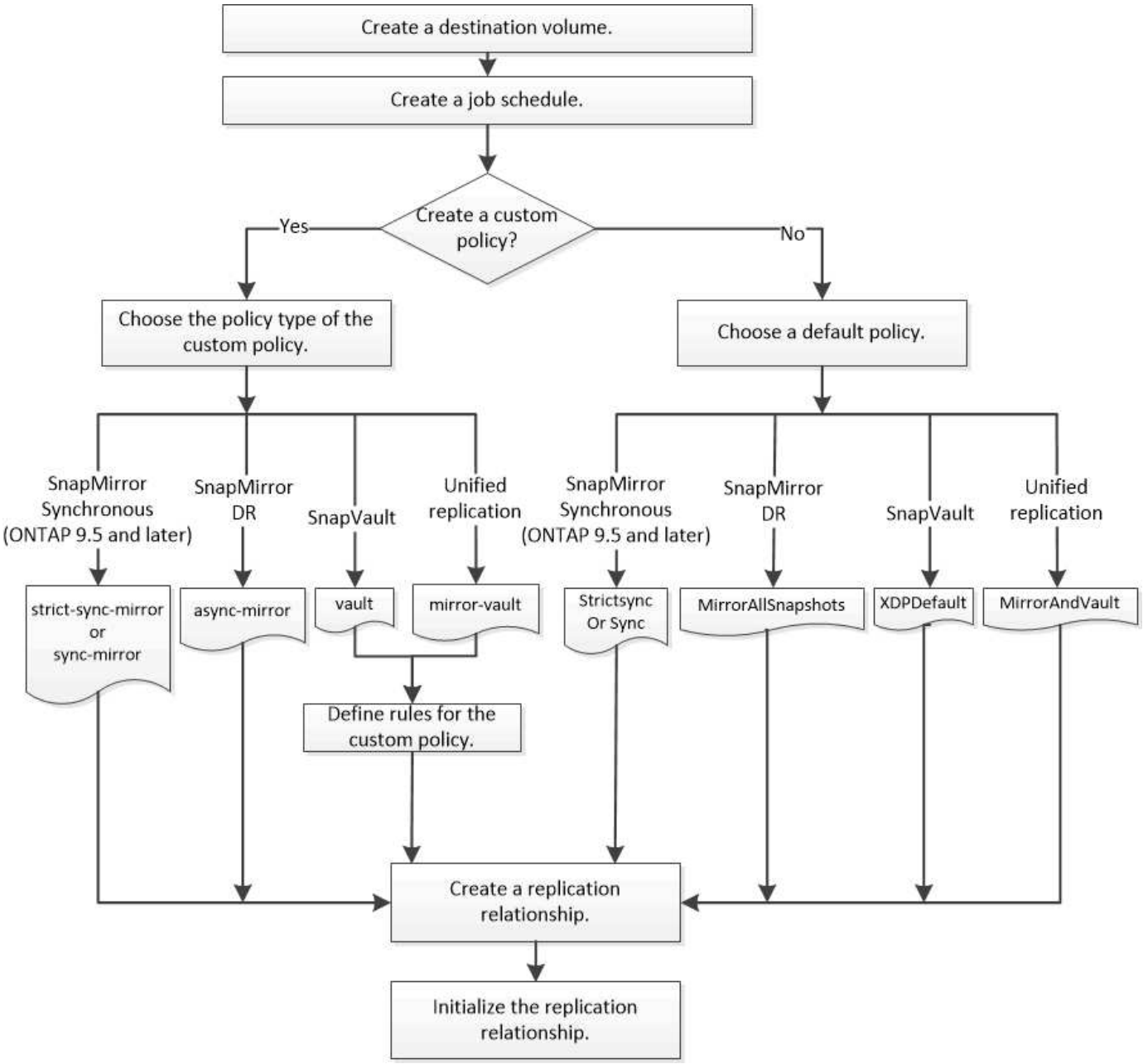
ONTAP SnapMirrorレプリケーションのワークフロー

SnapMirror には、 SnapMirror DR 、アーカイブ（旧 SnapVault ）、ユニファイドレプリケーションの 3 種類のデータ保護関係があります。同じ基本的なワークフローに従って、各タイプの関係を設定できます。

ONTAP 9 .9.1の一般提供開始以降では、"SnapMirrorアクティブ同期"目標復旧時間ゼロ（ゼロRTO）または透過的アプリケーションフェイルオーバー（TAF）が提供され、SAN環境でビジネスクリティカルなアプリケーションを自動的にフェイルオーバーできます。

SnapMirrorデータ保護関係の各タイプのワークフローは同じです（デスティネーションボリュームの作成、ジョブスケジュールの作成、ポリシーの指定、関係の作成と初期化）。

ONTAP 9 3以降では、コマンドを使用してデータ保護関係をワンステップで設定できます `snapmirror protect`。を使用する場合でも、 `snapmirror protect`ワークフローの各手順を理解する必要があります。



関連情報

- "SnapMirror保護"

ONTAP SnapMirrorレプリケーション関係をワンステップで設定

ONTAP 9.3以降では、 `snapmirror protect`データ保護関係を 1 つのステップで構成するコマンド。レプリケートするボリュームのリスト、宛先クラスタ上の SVM、ジョブ スケジュール、およびSnapMirrorポリシーを指定します。 `snapmirror protect`残りはやります。

開始する前に

- ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

  "クラスタとSVMのピアリング"

- デスティネーションボリュームの言語は、ソースボリュームの言語と同じである必要があります。

タスクの内容

コマンドは `snapmirror protect`、指定したSVMに関連付けられているアグリゲートを選択します。SVMにアグリゲートが関連付けられていない場合は、クラスタ内のすべてのアグリゲートから選択されます。アグリゲートの選択は、空きスペースの量とアグリゲート上のボリュームの数に基づいて行われます。

`snapmirror protect`コマンドは次の手順を実行します。

- レプリケートするボリュームのリスト内の各ボリュームについて、適切なタイプとリザーブスペースを持つデスティネーションボリュームを作成します。
- 指定したポリシーに適したレプリケーション関係を設定します。
- 関係を初期化します。

デスティネーションボリュームの名前は、の形式になり `*source_volume_name_dst*` ます。既存の名前と競合する場合は、コマンドによってボリューム名に数字が追加されます。コマンドオプションでプレフィックスまたはサフィックス（あるいはその両方）を指定できます。サフィックスは、システムが指定したサフィックスを置き換え `dst` ます。

ONTAP 9.4 以降では、宛先ボリュームに最大 1019 個のスナップショットを含めることができます。 ONTAP 9.3 以前では、宛先ボリュームには最大 251 個のスナップショットを含めることができます。

初期化には時間がかかることがあります。 `snapmirror protect`では、初期化が完了してからジョブが終了するまで待機しません。そのため、初期化がいつ完了するかを確認するには、コマンドではなくコマンドを `job show`使用する必要があり `snapmirror show` ます。

ONTAP 9 .5以降では `snapmirror protect`、コマンドを使用してSnapMirror同期関係を作成できます。

詳細はこちら `snapmirror protect`の中で"ONTAPコマンド リファレンス" 。

ステップ

1. レプリケーション関係をワンステップで作成して初期化します。

   このコマンドを実行する前に、山かっこ内の変数を必要な値に置き換える必要があります。

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。この `-auto-initialize`オプションのデフォルトは「true」です。

   次の例は、デフォルトのポリシーを使用して、SnapMirror DR関係を作成して初期化し `MirrorAllSnapshots` ます。

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

必要に応じてカスタムポリシーを使用できます。詳細については、を参照してください "カスタムレプリケーションポリシーの作成"。

次の例は、デフォルトのポリシーを使用して、SnapVault関係を作成して初期化し `XDPDefault`ます。

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

次の例は、デフォルトのポリシーを使用して、ユニファイドレプリケーション関係を作成して初期化し `MirrorAndVault`ます。

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

次の例は、デフォルトの `Sync`ポリシーを使用して、SnapMirror同期関係を作成して初期化します。

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

SnapVaultポリシーとユニファイドレプリケーションポリシーの場合は、デスティネーションで最後に転送されたSnapshotのコピーを作成するスケジュールを定義すると便利です。詳細については、を参照してください "デスティネーションでローカルコピーを作成するスケジュールの定義"。

終了後

コマンドを使用し `snapmirror show`て、SnapMirror関係が作成されたことを確認します。

の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "ジョブの表示"

レプリケーション関係を一度に**1**ステップずつ設定

ONTAP SnapMirrorデスティネーションボリュームを作成する

デスティネーションでコマンドを使用すると、デスティネーションボリュームを作成で

き `volume create`ます。デスティネーションボリュームのサイズは、ソースボリュームと同じかそれ以上である必要があります。の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. デスティネーションボリュームを作成します。

   `volume create -vserver *SVM* -volume volume -aggregate *aggregate* -type DP -size *size*`

   次の例は、という名前の2GBのデスティネーションボリュームを作成し `volA_dst`ます。

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

ONTAP SnapMirrorレプリケーションジョブスケジュールを作成します。

ジョブスケジュールは、スケジュールが割り当てられているデータ保護関係をSnapMirrorが自動的に更新するタイミングを決定します。System Managerまたはコマンドを使用して、レプリケーションジョブスケジュールを作成できます `job schedule cron create`。の詳細については `job schedule cron create`、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

ジョブスケジュールは、データ保護関係の作成時に割り当てます。ジョブスケジュールを割り当てない場合は、関係を手動で更新する必要があります。

手順

レプリケーションジョブスケジュールは、System ManagerまたはONTAP CLIを使用して作成できます。

System Manager

1. [保護]>[概要]に移動し、[ローカルポリシー設定]*を展開します。
2. [スケジュール]*ペインで、をクリックします →。
3. [スケジュール]ウィンドウで、をクリックします + Add。
4. [スケジュールの追加]ウィンドウで、スケジュール名を入力し、コンテキストとスケジュールタイプを選択します。
5. [保存（ Save ）] をクリックします。

CLI

1. ジョブスケジュールを作成します。

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

`-dayofweek`、および `-hour`では `-month`、ジョブを毎月、曜日、および時間ごとに実行するように指定できます `all`。

ONTAP 9 .10.1以降では、ジョブスケジュールにSVMを含めることができます。

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

Volume SnapMirror関係のFlexVolでサポートされる最小スケジュール（RPO）は5分です。Volume SnapMirror関係のFlexGroupボリュームでサポートされる最小スケジュール（RPO）は30分です。

次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

SnapMirrorレプリケーションポリシーをカスタマイズする

カスタムの**ONTAP SnapMirror**レプリケーションポリシーを作成する

関係のデフォルトポリシーが適切でない場合は、カスタムレプリケーションポリシーを作成できます。たとえば、ネットワーク転送でデータを圧縮したり、SnapMirrorによ

るSnapshot転送の試行回数を変更したりできます。

レプリケーション関係の作成時には、デフォルトまたはカスタムのポリシーを使用できます。カスタムアーカイブ（旧SnapVault）またはユニファイドレプリケーションポリシーの場合は、初期化と更新の際に転送するSnapshotを決定する1つ以上の_rules_を定義する必要があります。デスティネーションでローカルSnapshotを作成するスケジュールを定義することもできます。

レプリケーションポリシーの _policy type_of によって、サポートされる関係のタイプが決まります。次の表に、使用可能なポリシータイプを示します。

ポリシータイプ	関係タイプ
非同期ミラー	SnapMirror DR
バックアップ	SnapVault
ミラー-バックアップ	ユニファイドレプリケーション
strict-sync-mirror	StrictSyncモードでのSnapMirror同期（ONTAP 9 5以降でサポート）
同期ミラー	同期モードでのSnapMirror同期（ONTAP 9 5以降でサポート）

カスタムレプリケーションポリシーを作成する場合は、デフォルトポリシーに基づいてポリシーをモデル化することを推奨します。

手順

カスタムのデータ保護ポリシーは、System ManagerまたはONTAP CLIで作成できます。ONTAP 9.11.1以降では、System Managerを使用してカスタムのミラーポリシーとバックアップポリシーを作成したり、従来のポリシーを表示して選択したりできます。この機能は、ONTAP 9.8のONTAP 9.8P12以降のパッチでも利用できます。

ソースとデスティネーションの両方のクラスタにカスタムの保護ポリシーを作成します。

System Manager

1. [保護]>[概要]>[ローカルポリシー設定]*をクリックします。
2. [保護ポリシー]*で、をクリックし →ます。
3. [保護ポリシー]*ペインで、をクリックします + Add 。
4. 新しいポリシー名を入力し、ポリシーのスコープを選択します。
5. ポリシータイプを選択します。バックアップ専用ポリシーまたはミラーのみのポリシーを追加するには、*非同期*を選択し、*従来のポリシータイプを使用*をクリックします。
6. 必須フィールドに入力します。
7. [保存（ Save ）] をクリックします。
8. もう一方のクラスタで同じ手順を繰り返します。

CLI

1. カスタムレプリケーションポリシーを作成します。

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

ONTAP 9.5以降では、パラメータを使用して、SnapMirror同期関係の共通のSnapshotスケジュールを作成するスケジュールを指定でき `-common-snapshot-schedule`ます。デフォルトでは、SnapMirror同期関係の共通のSnapshotスケジュールは1時間です。SnapMirror同期関係のSnapshotスケジュールには、30~2時間の値を指定できます。

次の例は、データ転送のためのネットワーク圧縮を有効にするSnapMirror DR用のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

次の例は、SnapVaultのカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

次の例は、ユニファイドレプリケーション用のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

次の例は、StrictSyncモードでSnapMirror同期関係のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

の詳細については `snapmirror policy create`、を"ONTAPコマンド リファレンス"参照してください。

終了後

ポリシータイプが「vault」および「mairror-vault」の場合は、初期化と更新の際に転送するSnapshotを決定するルールを定義する必要があります。

使用 `snapmirror policy show` SnapMirrorポリシーが作成されたことを確認するコマンド。

詳細はこちら `snapmirror policy show`の中で"ONTAPコマンド リファレンス" 。

ONTAP SnapMirrorポリシーのルールを定義する

ポリシータイプがまたは `mirror-vault`のカスタムポリシーの場合 `vault`は、初期化と更新の際に転送する`Snapshot`を決定するルールを少なくとも`1`つ定義する必要があります。または `mirror-vault`ポリシータイプを使用してデフォルトポリシーのルールを定義することもできます `vault`。

タスクの内容

ポリシータイプがまたは `mirror-vault`のすべてのポリシー `vault`に、レプリケートする`Snapshot`を指定するルールが必要です。たとえば、ルールは `bi-monthly`、SnapMirrorラベルが割り当てられたSnapshotのみをレプリケートするように指定し `bi-monthly`ます。SnapMirrorラベルは、ソースでSnapshotポリシーを設定するときに指定します。

各ポリシータイプは、1つ以上のシステム定義ルールに関連付けられます。これらのルールは、ポリシータイプを指定するとポリシーに自動的に割り当てられます。次の表は、システム定義のルールを示しています。

システム定義のルール	ポリシータイプで使用されます	結果
sm_created	async-mirror、mirror-vault、Sync、StrictSync	SnapMirrorで作成されたSnapshotは、初期化と更新の際に転送されます。
すべてのソーススナップショット	非同期ミラー	ソース上の新しいSnapshotは、初期化と更新の際に転送されます。
毎日	ハツクアツフ、ミラ-vault	ソース上のSnapMirrorラベルの新しいSnapshotが `daily`初期化および更新の際に転送されます。

毎週	ハツクアツフ、ミラ-vault	ソース上のSnapMirrorラベルの新しいSnapshotが `weekly`初期化および更新の際に転送されます。
毎月	ミラー-バックアップ	ソース上のSnapMirrorラベルの新しいSnapshotが `monthly`初期化および更新の際に転送されます。
app_consistent	Sync、StrictSync	ソースでSnapMirrorラベルのSnapshotが `app_consistent`デスティネーションに同期的にレプリケートされます。ONTAP 9.7以降でサポートされます。

「 async 」ポリシータイプを除き、デフォルトポリシーまたはカスタムポリシーに追加のルールを必要に応じて指定できます。例：

- デフォルトの `MirrorAndVault`ポリシーでは、ソースの`Snapshot`（`SnapMirror`ラベル）を照合する `bi-monthly`ルールを作成できます `bi-monthly`。
- ポリシータイプのカスタムポリシーの場合 `mirror-vault`は、ソースの`Snapshot`（`SnapMirror`ラベル）を照合する `bi-weekly`ルールを作成できます `bi-weekly`。

ステップ

1. ポリシーのルールを定義します。

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   次の例は、SnapMirrorラベルのルールをデフォルト `MirrorAndVault`ポリシーに追加します `bi-monthly`。

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   次の例は、SnapMirrorラベルのルールをカスタム `my_snapvault`ポリシーに追加します `bi-weekly`。

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   次の例は、SnapMirrorラベルのルールをカスタム `Sync`ポリシーに追加します `app_consistent`。

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

の詳細については `snapmirror policy add-rule`、を"ONTAPコマンド リファレンス"参照してください。

その後、このSnapMirrorラベルに一致するSnapshotをソースクラスタからレプリケートできます。

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

ONTAP SnapMirrorスケジュールを定義してデスティネーションにローカルコピーを作成する

SnapVault関係とユニファイドレプリケーション関係の場合は、最後に転送されたSnapshotのコピーをデスティネーションに作成することで、更新したSnapshotが破損する可能性を防ぐことができます。この「ローカルコピー」はソース上の保持ルールに関係なく保持されるため、SnapMirrorによって転送されたSnapshotがソースで使用できなくなった場合でも、そのコピーをデスティネーションで使用できます。

タスクの内容

ローカルコピーを作成するスケジュールは、 `-schedule`オプションの `snapmirror policy add-rule`指示。

ステップ

1. デスティネーションでローカルコピーを作成するスケジュールを定義します。

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   ジョブスケジュールの作成方法の例については、を参照してください"レプリケーションジョブスケジュールの作成"。

   次の例は、ローカルコピーを作成するスケジュールをデフォルトポリシーに追加します `MirrorAndVault`。

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   次の例は、ローカルコピーを作成するスケジュールをカスタムポリシーに追加します `my_unified`。

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

   の詳細については `snapmirror policy add-rule`、を"ONTAPコマンド リファレンス"参照してください。

プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、_データ保護関係と呼ばれます。_コマンドを使用して、SnapMirror DR、SnapVault、またはユニファイドレプリケーションのデータ保護関係を作成できます。 `snapmirror create`

> この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"レプリケーション関係を作成します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ONTAP 9 .11.1以降では、System Managerを使用して、事前に作成されたカスタムのミラーポリシーとバックアップポリシーを選択したり、従来のポリシーを表示して選択したりできます。また、ボリュームやStorage VMを保護する際に、保護ポリシーで定義されている転送スケジュールを上書きしたりできます。この機能は、ONTAP 9 .8P12以降のONTAP 9 .8のパッチでも使用できます。

> ONTAP 9 .8P12以降のONTAP 9 .8パッチリリースを使用していて、System Managerを使用してSnapMirrorを設定している場合は、ONTAP 9 .9.1またはONTAP 9 .10.1P10以降のパッチリリースを使用してONTAP 9 .9.1P13以降およびONTAP 9 .10.1P10以降のパッチリリースをアップグレードする必要があります。

開始する前に

- ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

  "クラスタとSVMのピアリング"

- デスティネーションボリュームの言語は、ソースボリュームの言語と同じである必要があります。

タスクの内容

ONTAP 9 .3までは、DPモードで起動されるSnapMirrorとXDPモードで起動されるSnapMirrorでは、バージョン依存性に対するアプローチが異なり、異なるレプリケーションエンジンが使用されていました。

- DP モードで起動する SnapMirror では、プライマリストレージとセカンダリストレージの ONTAP バージョンを同じにする必要がある、バージョンに依存するレプリケーションエンジンを使用していました。

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- XDP モードで起動する SnapMirror では、バージョンに依存しないレプリケーションエンジンを使用していました。そのため、プライマリストレージとセカンダリストレージの ONTAP バージョンが異なっていてもかまいませんでした。

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

パフォーマンスの向上に伴い、バージョンに依存するモードで得られるレプリケーションスループットのわずかな利点よりも、バージョンに依存しないSnapMirrorの大きな利点が大きくなります。このため、XDP .3以降では、ONTAP 9モードが新しいデフォルトになり、コマンドラインまたは新規または既存のスクリプトでのDPモードの呼び出しは自動的にXDPモードに変換されます。

既存の関係には影響しません。すでにDPタイプの関係は、引き続きDPタイプになります。次の表は、想定される動作を示しています。

指定するモード	タイプ	デフォルトポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	XDPDefault（SnapVault）

以下の手順の例も参照してください。

変換の例外は次のとおりです。

- SVMデータ保護関係のデフォルトは引き続きDPモードです。

  デフォルトポリシーでXDPモードを取得するには、XDPを明示的に指定します `MirrorAllSnapshots`。

- 負荷共有データ保護関係のデフォルトは引き続きDPモードです。
- SnapLockデータ保護関係のデフォルトは引き続きDPモードです。
- 次のクラスタ全体のオプションを設定した場合、DPの明示的な呼び出しは引き続きデフォルトでDPモードになります。

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DPを明示的に呼び出さない場合、このオプションは無視されます。

ONTAP 9.14.1以降では `-backoff-level` 、、、の各コマンドにオプションが追加され、 `snapmirror create` `snapmirror modify` `snapmirror restore` 関係ごとにバックオフレベルを指定できるようになりました。オプションは、FlexVol SnapMirror関係でのみサポートされます。オプションのコマンドでは、クライアント処理によるSnapMirrorバックオフレベルを指定します。バックオフ値には、high、medium、noneのいずれかを指定できます。デフォルト値は高です。

ONTAP 9 .5以降では、SnapMirror同期関係がサポートされます。

ONTAP 9.4 以降では、宛先ボリュームに最大 1019 個のスナップショットを含めることができます。 ONTAP 9.3 以前では、宛先ボリュームには最大 251 個のスナップショットを含めることができます。

手順

レプリケーション関係は、System ManagerまたはONTAP CLIを使用して作成できます。

System Manager

1. 保護するボリュームまたはLUNを選択します。**[ストレージ]>[ボリューム]**または[ストレージ]>[LUN]*をクリックし、目的のボリュームまたはLUNの名前をクリックします。
2. をクリックします Protect
3. デスティネーションクラスタとStorage VMを選択
4. デフォルトでは非同期ポリシーが選択されます。同期ポリシーを選択するには、*[その他のオプション]*をクリックします。
5. [保護]*をクリックします。
6. 選択したボリュームまたはSnapMirrorの*[ローカルまたはリモート]*タブをクリックして、保護が正しく設定されていることを確認します。

CLI

1. デスティネーションクラスタから、レプリケーション関係を作成します。

   このコマンドを実行する前に、山かっこ内の変数を必要な値に置き換える必要があります。

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   `schedule`パラメータは、SnapMirror同期関係を作成する場合は使用できません。

   次の例は、デフォルトのポリシーを使用してSnapMirror DR関係を作成し `MirrorLatest`ます。

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   次の例は、デフォルトのポリシーを使用してSnapVault関係を作成し `XDPDefault`ます。

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   次の例は、デフォルトのポリシーを使用してユニファイドレプリケーション関係を作成し `MirrorAndVault`ます。

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault
   ```

次の例は、カスタムポリシーを使用してユニファイドレプリケーション関係を作成します `my_unified`。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

次の例は、デフォルトの `Sync`ポリシーを使用して、SnapMirror同期関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

次の例は、デフォルトの `StrictSync`ポリシーを使用して、SnapMirror同期関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

次の例は、SnapMirror DR関係を作成します。DPタイプは自動的にXDPに変換され、ポリシーは指定されません。デフォルトのポリシーは次のとおり `MirrorAllSnapshots`です。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

次の例は、SnapMirror DR関係を作成します。タイプまたはポリシーが指定されていない場合、ポリシーはデフォルトでポリシーに設定され `MirrorAllSnapshots`ます。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

次の例は、SnapMirror DR関係を作成します。ポリシーが指定されていない場合、デフォルトのポリシーがポリシーに設定され `XDPDefault`ます。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

次の例は、事前定義されたポリシーを使用してSnapMirror同期関係を作成し `SnapCenterSync`ます。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

事前定義されたポリシー `SnapCenterSync`のタイプはです `Sync`。このポリシーは、「app_consistent」のを使用して作成されたすべてのSnapshotをレプリケートし`snapmirror-label`ます。

終了後

コマンドを使用し`snapmirror show`て、SnapMirror関係が作成されたことを確認します。

の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "SnapMirrorフェイルオーバーテストボリュームの作成と削除"です。

ONTAPで実行するその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic（ONTAP 9 .7以前で使用可能）	"SnapVault によるボリュームのバックアップの概要"

関連情報

- "スナップミラー作成"

ONTAP SnapMirrorレプリケーション関係を初期化する

すべての関係タイプで初期化を実行すると、*baseline transfer*：が実行され、ソースボリュームのSnapshotが作成されて、そのコピーおよびコピーが参照するすべてのデータブロックがデスティネーションボリュームに転送されます。それ以外の転送の内容はポリシーによって異なります。

開始する前に

ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

"クラスタとSVMのピアリング"

タスクの内容

初期化には時間がかかる場合があります。ベースライン転送はオフピークの時間帯に実行することを推奨します。

ONTAP 9 .5以降では、SnapMirror同期関係がサポートされます。

ノードの再起動、テイクオーバー/ギブバック、パニックなど、何らかの理由でファイルシステムが再起動された場合、初期化は自動的に再開されず、手動で再起動する必要があることに注意してください。

ステップ

1. レプリケーション関係を初期化します。

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を初期化し `volA`ます。

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPのミラー-ヴォールト構成で共通のSnapshotを確保する

使用することができます `snapmirror snapshot-owner create`ミラー・ヴォールト構成において、セカンダリサーバ上にラベル付きスナップショットを保存するコマンドです。これにより、ヴォールト関係の更新時に共通のスナップショットが確保されます。

タスクの内容

ミラー-ヴォールトファンアウト構成またはカスケード構成を組み合わせて使用する場合は、ソースボリュームとデスティネーションボリュームに共通のSnapshotが存在しないと更新が失敗することに注意してください。

ミラー-ヴォールトファンアウト構成またはカスケード構成のミラー関係では、SnapMirrorでは更新の実行前に必ずソースボリュームのSnapshotが作成されるため、これが問題になることはありません。

ただし、SnapMirrorではバックアップ関係の更新時にソースボリュームのSnapshotが作成されないため、バックアップ関係で問題になる可能性があります。バックアップ関係のソースとデスティネーションの両方に共通のSnapshotを少なくとも1つ確保するには、を使用する必要が `snapmirror snapshot-owner create`あります。"データ保護のファンアウト構成とカスケード構成の詳細"です。

手順

1. ソースボリュームで、保持するラベル付きのSnapshotに所有者を割り当てます。

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   次の例は、Snapshotの所有者として `snap1`を割り当て `ApplicationA`ます。

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   詳細はこちら `snapmirror snapshot-owner create`の中で"ONTAPコマンド リファレンス" 。

2. の説明に従って、ミラー関係を更新します"手動によるレプリケーション関係の更新"。

   または、ミラー関係のスケジュールされた更新が行われるまで待つこともできます。

3. ラベル付きのSnapshotをSnapVaultデスティネーションに転送します。

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

   次の例は、**Snapshot**を転送します。 **snap1**

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   ラベルが付いたSnapshotはバックアップ関係の更新時に保持されます。

   の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

4. ソースボリュームで、ラベル付きのSnapshotから所有者を削除します。

   ```
   snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot
   snapshot -owner owner
   ```

   次の例は、Snapshotの所有者 `snap1`としてを削除し `ApplicationA`ます。

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   の詳細については `snapmirror snapshot-owner delete`、を"ONTAPコマンド リファレンス"参照してください。

例：**ONTAP SnapMirror**ヴォールト-ヴォールトカスケードの設定

レプリケーション関係を一度に 1 ステップずつ設定する方法の具体例を示します。この例で設定したヴォールト-ヴォールトカスケード構成を使用すると、ラベル付きの251個を超えるSnapshotを保持できます `my-weekly`。

開始する前に

ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

タスクの内容

この例では次のことを前提としています。

- SnapMirrorラベル、 `my-weekly`、および `my-monthly`を使用してソースクラスタでSnapshotを設定しておき `my-daily`ます。
- セカンダリデスティネーションクラスタと3番目のデスティネーションクラスタでというデスティネーションボリュームを設定しておき `volA`ます。
- セカンダリデスティネーションクラスタと3番目のデスティネーションクラスタでというレプリケーションジョブスケジュールを設定しておき `my_snapvault`ます。

次の例は、 2 つのカスタムポリシーに基づいてレプリケーション関係を作成する方法を示しています。

- このポリシーで `snapvault_secondary`は、7個の日単位Snapshot、52個の週単位Snapshot、180個の月単位Snapshotがセカンダリデスティネーションクラスタに保持されます。
- は、 `snapvault_tertiary policy`3次デスティネーションクラスタに250個の週単位Snapshotを保持します。

手順

1. セカンダリデスティネーションクラスタで、ポリシーを作成し `snapvault_secondary`ます。

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment "Policy on secondary for vault to vault cascade" -vserver
   svm_secondary
   ```

2. セカンダリデスティネーションクラスタで、ポリシーのルールを定義し `my-daily`ます。

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. セカンダリデスティネーションクラスタで、ポリシーのルールを定義し `my-weekly`ます。

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-weekly -keep 52 -vserver svm_secondary
   ```

4. セカンダリデスティネーションクラスタで、ポリシーのルールを定義し `my-monthly`ます。

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-monthly -keep 180 -vserver svm_secondary
   ```

5. セカンダリデスティネーションクラスタで、ポリシーを検証します。

   ```
   cluster_secondary::> snapmirror policy show snapvault_secondary -instance
   ```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. セカンダリデスティネーションクラスタで、ソースクラスタとの関係を作成します。

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. セカンダリデスティネーションクラスタで、ソースクラスタとの関係を初期化します。

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. 3次デスティネーションクラスタで、ポリシーを作成し `snapvault_tertiary`ます。

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. 3次デスティネーションクラスタで、ポリシーのルールを定義し `my-weekly`ます。

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. 3次デスティネーションクラスタで、ポリシーを確認します。

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                      Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
             Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. 3次デスティネーションクラスタで、セカンダリクラスタとの関係を作成します。

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. 3 番目のデスティネーションクラスタで、セカンダリクラスタとの関係を初期化します。

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

関連情報

- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror policy add-rule"
- "snapmirror policy create"
- "snapmirror policy show"

SnapMirrorボリュームのレプリケーションを管理します。

既存のONTAP SnapMirror DPタイプの関係をXDPに変換する

XDP 12.1以降にアップグレードする場合ONTAP 9は、アップグレード前にDPタイプの関係をXDPに変換する必要があります。ONTAP 9.12.1以降では、DPタイプの関係はサポートされません。既存のDPタイプの関係を簡単にXDPに変換して、バージョンに依存しないSnapMirrorを活用できます。

ONTAP 9.12.1にアップグレードする前に、ONTAP 9.12.1以降のリリースにアップグレードする前に、既存のDPタイプの関係をXDPに変換する必要があります。

タスクの内容

- SnapMirrorは、既存のDPタイプの関係をXDPに自動的に変換しません。関係を変換するには、既存の関係を解除して削除し、新しいXDP関係を作成して関係を再同期する必要があります。
- 変換を計画するときは、XDP SnapMirror関係のバックグラウンド準備とデータウェアハウジングフェーズに時間がかかることに注意してください。ステータスが「準備中」と長時間報告されるSnapMirror関係が表示されることも珍しくありません。

> SnapMirror関係のタイプをDPからXDPに変換すると、オートサイズやスペースギャランティなどのスペース関連の設定はデスティネーションにレプリケートされなくなります。

手順

1. デスティネーションクラスタから、SnapMirror関係のタイプがDP、ミラーの状態がSnapMirrored、関係のステータスがIdle、関係が正常であることを確認します。

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   次の例は、コマンドの出力を示してい `snapmirror show`ます。

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

関係設定の既存の情報を追跡するために、コマンド出力のコピーを保持しておくと便利 `snapmirror show`です。の詳細については `snapmirror show、を"ONTAPコマンドリファレンス"参照してください。

2. ソースボリュームとデスティネーションボリュームで、両方のボリュームに共通のSnapshotがあることを確認します。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、ソースボリュームとデスティネーションボリュームの出力を示してい `volume snapshot show`ます。

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. 変換中にスケジュールされた更新が実行されないようにするには、既存のDPタイプの関係を休止します。

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を休止し `volA`ます。

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

の詳細については `snapmirror quiesce`、を"ONTAPコマンド リファレンス"参照してください。

4. 既存のDPタイプの関係を解除します。

```
snapmirror break -destination-path <SVM:volume>
```

このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を解除し `volA`ます。

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

5. デスティネーションボリュームでSnapshotの自動削除が有効になっている場合は無効にします。

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

次の例は、デスティネーションボリュームでSnapshotの自動削除を無効にし `volA_dst`ます。

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. 既存のDPタイプの関係を削除します。

```
snapmirror delete -destination-path <SVM:volume>
```

の詳細については `snapmirror-delete`、を"ONTAPコマンド リファレンス"参照してください。

> このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を削除し `volA`ます。

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. ソースで元のSVMディザスタリカバリ関係を解放します。

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

次の例は、SVMディザスタリカバリ関係をリリースします。

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

の詳細については `snapmirror release`、を"ONTAPコマンド リファレンス"参照してください。

8. コマンドで保持した出力を使用して、新しいXDPタイプの関係を作成でき `snapmirror show`ます。

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

新しい関係では、同じソースボリュームとデスティネーションボリュームを使用する必要があります。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

> このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、 `svm1`デフォルトのポリシーを使用して `MirrorAllSnapshots`、の `svm_backup`ソースボリュームとデスティネーションボリューム `volA_dst`の間にSnapMirrorディザスタリカバリ関係を作成します `volA`。

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. ソースボリュームとデスティネーションボリュームを再同期します。

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

再同期時間を改善するには、 `-quick-resync`オプションですが、ストレージ効率の節約が失われる可能性があることに注意してください。

> このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を再同期し `volA`ます。

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

詳細はこちら `snapmirror resync`の中で"ONTAPコマンド リファレンス" 。

10. Snapshotの自動削除を無効にした場合は、再度有効にします。

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

終了後

1. コマンドを使用し `snapmirror show`て、SnapMirror関係が作成されたことを確認します。

   の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

2. SnapMirror XDPデスティネーションボリュームでSnapMirrorポリシーの定義に従ってSnapshotの更新が開始されたら、ソースクラスタからコマンドの出力を使用し `snapmirror list-destinations`て新しいSnapMirror XDP関係を表示します。

DPタイフノカンケイニカンスルシヨウサイシヨウホウ

ONTAP 9.3以降では、XDPモードがデフォルトであり、コマンドラインまたは新規または既存のスクリプトでのDPモードの呼び出しは自動的にXDPモードに変換されます。

既存の関係には影響しません。すでにDPタイプの関係は、引き続きDPタイプになります。ONTAP 9.5以降では、データ保護モードを指定しない場合、またはXDPモードを関係タイプとして指定した場合にデフォルトポ

リシーがMirrorAndVaultになります。次の表は、想定される動作を示しています。

指定するモード	タイプ	デフォルトポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAndVault（ユニファイドレプリケーション）
XDP	XDP	MirrorAndVault（ユニファイドレプリケーション）

次の表に示すように、さまざまな状況でXDPに割り当てられたデフォルトポリシーによって、変換時に以前のタイプと同等の機能が維持されます。もちろん、ユニファイドレプリケーションのポリシーなど、必要に応じてさまざまなポリシーを使用できます。

指定するモード	ポリシー	結果
DP	MirrorAllSnapshots	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault
ユニファイドレプリケーション	XDP	MirrorAllSnapshots
SnapMirror DR	XDPDefault	SnapVault

変換の例外は次のとおりです。

- ONTAP 9 .3以前のSVMデータ保護関係のデフォルトは引き続きDPモードです。

  ONTAP 9 .4以降では、SVMデータ保護関係のデフォルトがXDPモードに変更されました。

- ルートボリュームの負荷共有データ保護関係のデフォルトは引き続きDPモードです。
- ONTAP 9 .4以前のSnapLockデータ保護関係のデフォルトは引き続きDPモードです。

  XDP 5以降ONTAP 9では、SnapLockデータ保護関係のデフォルトがXDPモードに変更されました。

- 次のクラスタ全体のオプションを設定した場合、DPの明示的な呼び出しは引き続きデフォルトでDPモードになります。

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DPを明示的に呼び出さない場合、このオプションは無視されます。

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"

ONTAP SnapMirror関係のタイプを変換する

ONTAP 9 .5以降では、SnapMirror同期がサポートされています。SnapMirror非同期関係からSnapMirror同期関係への変換（またはその逆）は、ベースライン転送を実行せずに実行できます。

タスクの内容

SnapMirrorポリシーを変更してSnapMirror非同期関係とSnapMirror同期関係をまたはその逆に変換することはできません。

手順

- * SnapMirror非同期関係からSnapMirror同期関係への変換*

  a. デスティネーションクラスタから、SnapMirror非同期関係を削除します。

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. ソースクラスタから、共通のSnapshotを削除せずにSnapMirror関係を解放します。

  ```
  snapmirror release -relationship-info-only true -destination-path
  <destination_SVM>:<destination_volume>
  ```

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  c. デスティネーションクラスタから、SnapMirror同期関係を作成します。

  ```
  snapmirror create -source-path src_SVM:src_volume -destination-path
  <destination_SVM>:<destination_volume> -policy sync-mirror
  ```

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  d. SnapMirror同期関係を再同期します。

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- * SnapMirror同期関係からSnapMirror非同期関係への変換*

  a. デスティネーションクラスタから、既存のSnapMirror同期関係を休止します。

  ```
  snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
  ```

  ```
  cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
  ```

  b. デスティネーションクラスタから、SnapMirror非同期関係を削除します。

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  c. ソースクラスタから、共通のSnapshotを削除せずにSnapMirror関係を解放します。

  ```
  snapmirror release -relationship-info-only true -destination-path
  <destination_SVM:destination_volume>
  ```

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  d. デスティネーションクラスタから、SnapMirror非同期関係を作成します。

  ```
  snapmirror create -source-path src_SVM:src_volume -destination-path
  <destination_SVM:destination_volume> -policy MirrorAllSnapshots
  ```

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  e. SnapMirror同期関係を再同期します。

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"

- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"

ONTAP SnapMirror同期関係のモードの変換

ONTAP 9 .5以降では、SnapMirror同期関係がサポートされます。SnapMirror同期関係のモードはStrictSyncからSyncに（またはその逆）変換できます。

タスクの内容

SnapMirror同期関係のポリシーを変更してモードを変換することはできません。

手順

1. デスティネーションクラスタから、既存のSnapMirror同期関係を休止します。

   ```
   snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
   ```

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. デスティネーションクラスタから、既存のSnapMirror同期関係を削除します。

   ```
   snapmirror delete -destination-path <destination_SVM>:<destination_volume>
   ```

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. ソースクラスタから、共通のSnapshotを削除せずにSnapMirror関係を解放します。

   ```
   snapmirror release -relationship-info-only true -destination-path
   <destination_SVM>:<destination_volume>
   ```

   ```
   cluster1::> snapmirror release -relationship-info-only true -destination
   -path vs1_dr:vol1
   ```

4. デスティネーションクラスタから、SnapMirror同期関係の変換先のモードを指定して、SnapMirror同期関係を作成します。

   ```
   snapmirror create -source-path vs1:vol1 -destination-path
   <destination_SVM>:<destination_volume> -policy Sync|StrictSync
   ```

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. デスティネーションクラスタから、SnapMirror関係を再同期します。

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"

ONTAP SnapMirrorフェイルオーバーテストボリュームの作成と削除

ONTAP 9 14.1以降では、System Managerを使用してボリュームクローンを作成し、アクティブなSnapMirror関係を中断せずにSnapMirrorフェイルオーバーとディザスタリカバリをテストできます。テストが完了したら、関連するデータをクリーンアップしてテストボリュームを削除できます。

SnapMirrorフェイルオーバーテストボリュームを作成します。

タスクの内容

- 同期およびSnapMirror非同期関係に対してフェイルオーバーテストを実行できます。
- ディザスタリカバリテストを実行するためにボリュームクローンを作成します。
- クローンボリュームは、SnapMirrorデスティネーションと同じStorage VMに作成されます。
- FlexVol関係とFlexGroup SnapMirror関係を使用できます。
- 選択した関係にテスト用のクローンがすでに存在する場合、その関係に別のクローンを作成することはできません。
- SnapLockバックアップ関係はサポートされません。

開始する前に

- クラスタ管理者である必要があります。
- ソースとデスティネーションのクラスタにSnapMirrorライセンスがインストールされている必要があります。

手順

1. デスティネーションクラスタで、*[保護]>[関係]*を選択します。
2. 関係ソースの横にあるを選択 ⋮ し、*[フェイルオーバーのテスト]*を選択します。
3. [フェイルオーバーのテスト]ウィンドウで、*[フェイルオーバーのテスト]*を選択します。
4. [ストレージ]>[ボリューム]*を選択し、テストフェイルオーバーボリュームが表示されることを確認します。
5. [ストレージ]>[共有]*を選択します。

6. を選択し 、*[共有]*を選択します。
7. ウィンドウで、[共有名]*フィールドに共有の名前を入力します。
8. フィールドで[参照]を選択し、テストクローンボリュームを選択して[保存]*を選択します。
9. ウィンドウの下部で、[保存]*を選択します。
10. [ストレージ]>[共有]*ペインで、作成した共有を探し、を選択して共有情報を表示し ます。
11. [SMB/CIFS Access]*で、共有のアクセスパスをコピーするかメモします（例：）`\\123.456.7.890\failover_test`。
12. SMBアクセスパスを使用してクライアント上で共有を開き、テスト用ボリュームに読み取りおよび書き込み機能があることを確認します。

フェイルオーバーデータをクリーンアップし、テストボリュームを削除する

フェイルオーバーテストが完了したら、テストボリュームに関連付けられているすべてのデータをクリーンアップして削除できます。

手順

1. デスティネーションクラスタで、*[保護]>[関係]*を選択します。
2. 関係ソースの横にあるを選択 し、*[テストフェイルオーバーのクリーンアップ]*を選択します。
3. ウィンドウで、[クリーンアップ]*を選択します。
4. [ストレージ]>[ボリューム]*を選択し、テストボリュームが削除されたことを確認します。

SnapMirror DRデスティネーションボリュームからのデータの提供

ONTAP SnapMirrorデスティネーションボリュームを書き込み可能にする

デスティネーションボリュームからクライアントにデータを提供するには、デスティネーションボリュームを書き込み可能にする必要があります。ソースを使用できなくなったときにミラーデスティネーションからデータを提供するには、デスティネーションへのスケジュールされた転送を中止してから、SnapMirror関係を解除してデスティネーションを書き込み可能にします。

タスクの内容

このタスクはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

手順

デスティネーションボリュームを書き込み可能にするには、System ManagerまたはONTAP CLIを使用します。

System Manager

1. 保護関係を選択します。*[保護]>[関係]*をクリックし、目的のボリューム名をクリックします。
2. をクリックします。⋮
3. スケジュールされた転送を停止します。*一時停止*をクリックします。
4. デスティネーションを書き込み可能にします。*[解除]*をクリックします。
5. メインの*[関係]*ページに移動して、関係の状態が「切断」と表示されていることを確認します。

次のステップ

デスティネーションボリュームを書き込み可能にしたあとに実行する必要があり "レプリケーション関係を逆再同期する" ます。

無効にしたソースボリュームが再び使用できるようになったら、関係をもう一度逆再同期して、現在のデータを元のソースボリュームにコピーする必要があります。

CLI

1. デスティネーションへのスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間のスケジュールされた転送を停止します `volA`。

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

の詳細については `snapmirror quiesce`、を"ONTAPコマンド リファレンス"参照してください。

2. デスティネーションへの実行中の転送を停止します。

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

ⓘ この手順は、SnapMirror同期関係（ONTAP 9 5以降でサポート）では必要ありません。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の実行中の転送を停止します `volA`。

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror abort`、を"ONTAPコマンド リファレンス"参照してください。

3. SnapMirror DR関係を解除します。

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst` の間の関係を解除し `volA`ます。

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

次のステップ

デスティネーションボリュームを書き込み可能にしたあとに実行する必要があり "レプリケーション関係を再同期する" ます。

ONTAPで実行するその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic（ONTAP 9 .7以前で使用可能）	"ボリュームディザスタリカバリの概要"

データアクセス用の**ONTAP SnapMirror**デスティネーションボリュームの設定

デスティネーションボリュームを書き込み可能にしたら、ボリュームをデータアクセス用に設定する必要があります。NAS クライアント、 NVMe サブシステム、および SAN ホストは、ソースボリュームが再アクティブ化されるまでの間、デスティネーションボリュームのデータにアクセスできます。

NAS環境：

1. ソースボリュームがソースSVMでマウントされていたのと同じジャンクションパスを使用して、NASボリュームをネームスペースにマウントします。
2. デスティネーションボリュームのSMB共有に適切なACLを適用します。
3. デスティネーションボリュームにNFSエクスポートポリシーを割り当てます。
4. デスティネーションボリュームにクォータルールを適用します。
5. クライアントをデスティネーションボリュームにリダイレクトします。
6. NFS共有とSMB共有をクライアントに再マウントします。

SAN 環境の場合：

1. ボリューム内のLUNを適切なイニシエータグループにマッピングします。
2. iSCSIの場合、SANホストイニシエータからSAN LIFへのiSCSIセッションを作成します。
3. SANクライアントで、ストレージの再スキャンを実行して接続されているLUNを検出します。

NVMe環境については、を参照してください"SAN管理"。

元の**ONTAP SnapMirror**ソースボリュームを再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソースボリュームとデスティネーションボリュームの間で元のデータ保護関係を再確立できます。

タスクの内容

- 次の手順は、元のソースボリュームのベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、この手順を実行する前に、データの提供元のボリュームと元のソースボリュームの間の関係を作成して初期化する必要があります。
- XDP SnapMirror関係のバックグラウンド準備とデータウェアハウジングフェーズには時間がかかることがあります。ステータスが「準備中」と長時間報告されるSnapMirror関係が表示されることも珍しくありません。

手順

1. 元のデータ保護関係を反転します。

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   の詳細については `snapmirror resync`、を"ONTAPコマンド リファレンス"参照してください。

   > このコマンドは、元のソース SVM または元のソース クラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。ソースとデスティネーションに共通のSnapshotが存在しない場合、コマンドは失敗します。を使用し `snapmirror initialize` て関係を再初期化します。の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、上の `svm1`元のソースボリュームとデータの提供元のボリューム `volA_dst`の間の関係を反転し `volA`svm_backup`ます。

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. 元のソースへのデータアクセスを再確立する準備ができたら、元のデスティネーションボリュームへのアクセスを停止します。その方法の1つとして、元のデスティネーションSVMを停止します。

   `vserver stop -vserver` *`SVM`*

このコマンドは元のデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。このコマンドは、元のデスティネーションSVM全体へのユーザアクセスを停止します。他の方法を使用して元のデスティネーションボリュームへのアクセスを停止することもできます。

次の例は、元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

の詳細については `vserver stop`、を"ONTAPコマンド リファレンス"参照してください。

3. 反転した関係を更新します。

`snapmirror update -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

このコマンドは元のソースSVMまたはソースクラスタから実行する必要があります。

次の例は、の `svm_backup`データの提供元のボリュームとの元のソースボリュームの `volA`間の関係を更新します `volA_dst svm1`。

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

4. 元のソースSVMまたはソースクラスタから、反転した関係のスケジュールされた転送を停止します。

`snapmirror quiesce -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

このコマンドは元のソースSVMまたはソースクラスタから実行する必要があります。

次の例は、の `svm_backup`元のデスティネーションボリュームとの元のソースボリューム `volA`の間のスケジュールされた転送を停止します `volA_dst svm1`。

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

の詳細については `snapmirror quiesce`、を"ONTAPコマンド リファレンス"参照してください。

5. 最後の更新が完了し、関係のステータスが「Quiesced」と表示されたら、元のソースSVMまたは元のソースクラスタから次のコマンドを実行して、反転した関係を解除します。

`snapmirror break -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

このコマンドは元のソースSVMまたはソースクラスタから実行する必要があります。

次の例は、の `svm_backup`元のデスティネーションボリュームとの元のソースボリュームの `volA`間の関係を解除し `volA_dst`svm1`ます。

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

6. 元のソースSVMまたはソースクラスタから、反転したデータ保護関係を削除します。

`snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

このコマンドは元のソースSVMまたはソースクラスタから実行する必要があります。

次の例は、上の `svm1`元のソースボリュームとデータの提供元のボリューム `volA_dst`の間の反転した関係を削除します `volA svm_backup`。

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

の詳細については `snapmirror delete`、を"ONTAPコマンド リファレンス"参照してください。

7. 元のデスティネーションSVMまたはデスティネーションクラスタから反転した関係を解放します。

`snapmirror release -source-path SVM:volume -destination-path SVM:volume`

このコマンドは元のデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、上の `svm_backup`元のデスティネーションボリュームと上の `svm1`元のソースボリューム `volA`の間の反転した関係をリリースします `volA_dst`。

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

の詳細については `snapmirror release`、を"ONTAPコマンド リファレンス"参照してください。

8. 元のデスティネーションから元のデータ保護関係を再確立します。

`snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

次の例は、の `svm1`元のソースボリュームとの元のデスティネーションボリューム `volA_dst`の間の関係を再確立し `volA`svm_backup`ます。

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror resync`、を"ONTAPコマンド リファレンス"参照してください。

9. 必要に応じて、元のデスティネーションSVMを起動します。

   `vserver start -vserver` *SVM*

   次の例は、元のデスティネーションSVMを起動します。

```
cluster_dst::> vserver start svm_backup
```

   の詳細については `vserver start`、を"ONTAPコマンド リファレンス"参照してください。

終了後

コマンドを使用し `snapmirror show`て、SnapMirror関係が作成されたことを確認します。

の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

SnapMirrorデスティネーションボリュームからのファイルのリストア

ONTAP SnapMirrorデスティネーションからファイル、LUN、NVMeネームスペースをリストアする

単一ファイル、LUN、一連のファイルまたはLUNをSnapshotからリストアしたり、NVMeネームスペースをSnapMirrorデスティネーションボリュームからリストアしたりできます。NVMe.7以降では、SnapMirror同期デスティネーションからONTAP 9ネームスペースをリストアすることもできます。ファイルは元のソースボリュームにリストアすることも、別のボリュームにリストアすることもできます。

開始する前に

SnapMirror同期デスティネーション（ONTAP 9 .5以降でサポート）からファイルまたはLUNをリストアするには、まず関係を削除して解放する必要があります。

タスクの内容

ファイルまたはLUNのリストア先のボリューム（デスティネーションボリューム）が読み書き可能ボリュームである必要があります。

- ソースボリュームとデスティネーションボリュームに共通のSnapshotがある場合（通常は元のソースボリュームにリストアする場合）、SnapMirrorは_増分リストア_を実行します。
- それ以外の場合、SnapMirrorは_ベースラインリストア_を実行します。指定したSnapshotとSnapshotが参照するすべてのデータブロックがデスティネーションボリュームに転送されます。

手順

1. デスティネーションボリューム内のSnapshotの一覧を表示します。

```
volume snapshot show -vserver <SVM> -volume volume
```

の詳細については `volume snapshot show`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、デスティネーション上のSnapshotを示してい `vserverB:secondary1`ます。

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. SnapMirrorデスティネーションボリューム内のSnapshotから、単一ファイルまたはLUN、あるいは一連のファイルまたはLUNをリストアします。

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

> このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次のコマンドは、ファイルと `file2`ファイルを元のデスティネーションボリューム内の `secondary1`Snapshotから `daily.2013-01-25_0010`、元のソースボリュームのアクティブファイルシステム内の同じ場所に `primary1`リストアします `file1`。

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

次のコマンドは、ファイルと `file2`ファイルを元のデスティネーションボリューム内の `secondary1`Snapshotから `daily.2013-01-25_0010`、元のソースボリュームのアクティブファイルシステム内の別の場所に `primary1`リストアします `file1`。

@記号に続くパスがデスティネーションファイルのパスで、元のソースボリュームのルートからのパスが指定されています。この例では、 `file1`がにリストアされ、`file2`が `/dir2.new/file2`にリストアされ `/dir1/file1.new`primary1`ます。

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

次のコマンドは、ファイルと `file3`ファイルを元のデスティネーションボリューム内の `secondary1`Snapshotから `daily.2013-01-25_0010`、元のソースボリュームのアクティブファイルシステム内の別の場所に `primary1`リストアし、から `snap1`のアクティブファイルシステム内の同じ場所に `primary1`リストアし `file1`ます。 `file2`

この例では、ファイルが `file1`にリストアされ `/dir1/file1.new`、`file3`にリストアされ `/dir3.new/file3`ます。

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

関連情報

- "スナップミラー復元"

SnapMirrorデスティネーションボリューム内のSnapshotからボリューム全体の内容をリストアできます。ボリュームの内容は元のソースボリュームにリストアすることも、別のボリュームにリストアすることもできます。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"データを復元します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

リストア処理のデスティネーションボリュームは次のいずれかである必要があります。

- 読み書き可能ボリューム。このケースでは、ソースボリュームとデスティネーションボリュームに共通のSnapshotがある場合（通常は元のソースボリュームにリストアする場合）、SnapMirrorは_増分リストア_を実行します。

> ⓘ 共通のSnapshotがない場合、コマンドは失敗します。空の読み書き可能なボリュームにボリュームの内容をリストアすることはできません。

- 空のデータ保護ボリューム。この場合、SnapMirrorは_baseline restore_を実行します。指定したSnapshotとSnapshotが参照するすべてのデータブロックがソースボリュームに転送されます。

ボリュームの内容のリストアはシステム停止を伴う処理です。リストア処理を実行しているときに、SnapVaultプライマリ ボリューム上でSMBトラフィックを実行してはなりません。

リストア処理のデスティネーション ボリュームで圧縮が有効になっていて、ソース ボリュームで圧縮が有効になっていない場合は、デスティネーション ボリュームで圧縮を無効にします。リストア処理が完了したら、圧縮を再度有効にする必要があります。

デスティネーション ボリュームに対して定義されたクォータ ルールは、リストアの実行前に非アクティブ化されます。コマンドを使用すると、リストア処理の完了後にクォータルールを再アクティブ化できます `volume quota modify`。

ボリューム内のデータが失われたり破損したりした場合は、以前のSnapshotからリストアしてデータをロールバックできます。

この手順では、ソースボリュームの現在のデータを以前のバージョンのSnapshotのデータに置き換えます。このタスクはデスティネーションクラスタで実行する必要があります。

手順

ボリュームの内容は、System ManagerまたはONTAP CLIを使用してリストアできます。

System Manager

1. [保護]>[関係]*をクリックし、ソースボリュームの名前をクリックします。
2. をクリックし ⋮ 、*[リストア]*を選択します。
3. [ソース]*では、ソースボリュームがデフォルトで選択されます。ソース以外のボリュームを選択する場合は、「 * その他のボリューム」をクリックします。
4. [デスティネーション]*で、リストアするSnapshotを選択します。
5. ソースとデスティネーションが別 々 のクラスタにある場合は、リモートクラスタで*[保護]>[関係]*をクリックしてリストアの進捗状況を監視します。

CLI

1. デスティネーションボリューム内のSnapshotの一覧を表示します。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、デスティネーション上のSnapshotを示してい `vserverB:secondary1`ます。

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. SnapMirrorデスティネーションボリューム内のSnapshotからボリュームの内容をリストアします。

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
```

```
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

このコマンドは元のソースSVMまたはソースクラスタから実行する必要があります。

次のコマンドは、元のデスティネーションボリュームの `secondary1`Snapshotから `daily.2013-01-25_0010`元のソースボリュームの内容をリストアします `primary1。

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. リストアしたボリュームを再マウントし、ボリュームを使用するすべてのアプリケーションを再起動します。

ONTAPで実行するその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic（ONTAP 9 .7以前で使用可能）	"SnapVault によるボリュームリストアの概要"

関連情報

- "スナップミラー復元"
- "volume snapshot show"

ONTAP SnapMirrorレプリケーション関係を手動で更新する

ソースボリュームが移動されたために更新が失敗した場合は、レプリケーション関係の手動更新が必要になることがあります。

タスクの内容

レプリケーション関係を手動で更新するまで、SnapMirrorは移動したソースボリュームからの転送をすべて中止します。

ONTAP 9 .5以降では、SnapMirror同期関係がサポートされます。これらの関係ではソースボリュームとデスティネーションボリュームは常に同期されていますが、セカンダリクラスタのビューは1時間ごとにのみプライマリと同期されます。デスティネーションのポイントインタイムデータを表示する場合は、 `snapmirror update`コマンドを実行して手動更新を実行する必要があります。

ステップ

1. レプリケーション関係を手動で更新します。

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> このコマンドは、デスティネーション SVM またはデスティネーション クラスタから実行する必要があります。ソースとデスティネーションに共通のSnapshotが存在しない場合、コマンドは失敗します。を使用し `snapmirror initialize` て関係を再初期化します。の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を更新し `volA`ます。

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapMirrorレプリケーション関係を再同期する

デスティネーションボリュームを書き込み可能にしたあと、ソースボリュームとデスティネーションボリュームに共通のSnapshotが存在しないために更新が失敗したあと、または関係のレプリケーションポリシーを変更する場合は、レプリケーション関係の再同期が必要になります。

ONTAP 9 8以降では、System Managerを使用して逆再同期処理を実行して既存の保護関係を削除し、ソースボリュームとデスティネーションボリュームの機能を入れ替えることができます。その後、デスティネーションボリュームを使用してデータを提供しながら、ソースを修理または交換し、ソースを更新し、システムの元の構成を再確立します。

タスクの内容

- 再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。
- ファンアウト構成またはカスケード構成に含まれているボリュームの再同期には時間がかかることがあります。ステータスが「準備中」と長時間報告されるSnapMirror関係が表示されることも珍しくありません。

> System Managerでは、クラスタ内の関係との逆再同期はサポートされません。クラスタ内の関係に対する逆再同期処理は、ONTAP CLIを使用して実行できます。

手順

このタスクは、System ManagerまたはONTAP CLIを使用して実行できます。ONTAP CLIを使用する場合の手順は、デスティネーションボリュームを書き込み可能にするか、レプリケーション関係を更新するかに関係なく同じです。

System Managerの逆再同期

"関係を解除する"デスティネーションを書き込み可能にしたら、関係を逆再同期します。

1. デスティネーションクラスタで、 * Protection > Relationships * をクリックします。
2. 逆にする解除した関係にカーソルを合わせ、をクリックし⋮て*[逆再同期]*を選択します。
3. ウィンドウで、[逆再同期]*をクリックします。
4. 「 * Relationships * 」で、関係の「 * Transfer Status * 」を表示して、逆再同期の進捗を監視します。

次のステップ

元のソースが再び使用可能になったら、反転した関係を解除してもう一度逆再同期処理を実行することで、元の関係を再確立できます。逆再同期プロセスでは、データを元のソースに提供しているサイトからの変更がすべてコピーされ、元のソースが再び読み取り/書き込み可能になります。

System Managerの再同期

1. ［ * 保護 ］ > ［ 関係 * ］ の順にクリックします。
2. 再同期する関係にカーソルを合わせ、をクリックし⋮て*[解除]*を選択します。
3. 関係の状態が「切断」と表示されたら、をクリックし⋮、*[再同期]*を選択します。
4. [関係]*で、関係の状態を確認して再同期の進捗を監視します。再同期が完了すると、状態が「mirrored」に変わります。

CLI

1. ソースボリュームとデスティネーションボリュームを再同期します。

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

ⓘ このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、のソースボリュームとのデスティネーションボリュームの間の関係を再同期し `volA svm1 volA_dst` `svm_backup`ます。

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror resync`、を"ONTAPコマンド リファレンス"参照してください。

コマンドと `snapmirror release`コマンドを使用して、ボリュームレプリケーション関係を削除できます `snapmirror delete`。その後、不要なデスティネーションボリュームを手動で削除できます。

タスクの内容

`snapmirror release`コマンドは、SnapMirrorで作成されたSnapshotをソースから削除します。オプションを使用すると、Snapshotを保持できます `-relationship-info-only`。

手順

1. レプリケーション関係を休止します。

   ```
   snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>
   ```

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   の詳細については snapmirror quiesce、を"ONTAPコマンド リファレンス"参照してください。

2. （オプション）デスティネーションボリュームを読み取り/書き込みボリュームにする必要がある場合は、レプリケーション関係を解除します。デスティネーションボリュームを削除する場合やボリュームの読み取り/書き込みが不要な場合は、この手順を省略できます。

   ```
   snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

   の詳細については snapmirror break、を"ONTAPコマンド リファレンス"参照してください。

3. レプリケーション関係を削除します。

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   このコマンドはデスティネーションクラスタまたはデスティネーションSVMから実行する必要があります。

   次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を削除し `volA`ます。

```
cluster_dst::> snapmirror delete -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror delete`、を"ONTAPコマンド リファレンス"参照してください。

4. ソースSVMからレプリケーション関係情報を解放します。

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> このコマンドはソースクラスタまたはソースSVMから実行する必要があります。

次の例は、指定したレプリケーション関係の情報をソースSVMからリリースします `svm1`。

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

の詳細については `snapmirror release`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapMirrorボリュームの**Storage Efficiency**を管理します。

SnapMirrorでは、ソースボリュームとデスティネーションボリュームでストレージ効率が維持されます。ただし、デスティネーションボリュームでポストプロセスデータ圧縮が有効になっている場合は除きます。この場合、デスティネーションボリュームではすべてのストレージ効率が失われます。この問題を解決するには、デスティネーションボリュームでポストプロセス圧縮を無効にし、関係を手動で更新してから、Storage Efficiencyを再度有効にする必要があります。

タスクの内容

コマンドを使用すると、ボリュームで効率化が有効になっているかどうかを確認できます `volume efficiency show`。の詳細については `volume efficiency show`、を"ONTAPコマンド リファレンス"参照してください。

SnapMirrorがストレージ効率を維持しているかどうかを確認するには、SnapMirror監査ログを表示して転送の説明を確認します。転送の説明にと表示された場合は `transfer_desc=Logical Transfer with Storage Efficiency`、SnapMirrorでストレージ効率が維持されています。転送の説明にと表示された場合は `transfer_desc=Logical Transfer`、SnapMirrorでストレージ効率が維持されていません。例：

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

開始する前に

- ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

  "クラスタとSVMのピアリング"

- デスティネーションボリュームでポストプロセス圧縮を無効にする必要があります。
- ストレージを使用した論理転送：ONTAP 9.3以降では、Storage Efficiencyを再度有効にするための手動更新が不要になりました。SnapMirrorは、ポストプロセス圧縮が無効になっていることを検出すると、スケジュールされた次回の更新時にStorage Efficiencyを自動的に再度有効にします。ソースとデスティネーションの両方でONTAP 9.3を実行している必要があります。
- ONTAP 9 .3以降では、デスティネーションボリュームが書き込み可能になったあとに、AFFシステムでStorage Efficiencyの設定がFASシステムとは異なる方法で管理されます。
  - 宛先ボリュームを書き込み可能にした後、 `snapmirror break`コマンドを実行すると、ボリュームのキャッシュポリシーが自動的に設定されます。 `auto` (デフォルト)。

    この動作はFlexVolにのみ該当し、FlexGroupには該当しません。

    の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

  - 再同期時に、キャッシュポリシーは自動的に設定されます。 `none`元の設定に関係なく、重複排除とインライン圧縮は自動的に無効になります。必要に応じて、設定を手動で変更する必要があります。

Storage Efficiencyを有効にした状態での手動更新には時間がかかる場合があります。この処理はオフピークの時間帯に実行することを推奨します。

手順

1. レプリケーション関係を更新し、Storage Efficiencyを再度有効にします。

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

このコマンドは、デスティネーション SVM またはデスティネーション クラスタから実行する必要があります。ソースとデスティネーションに共通のSnapshotが存在しない場合、コマンドは失敗します。を使用し `snapmirror initialize` て関係を再初期化します。の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA_dst`の間の関係を更新し `volA`、Storage Efficiencyを再度有効にします。

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapMirrorグローバルスロットルの使用

グローバルネットワークスロットルは、すべてのSnapMirror転送とSnapVault転送にノードレベルで使用できます。

タスクの内容

SnapMirrorグローバルスロットルは、送受信のSnapMirror転送およびSnapVault転送で使用する帯域幅を制限します。この制限は、クラスタ内のすべてのノードで適用されます。

たとえば、送信スロットルが100Mbpsに設定されている場合、クラスタ内の各ノードの送信帯域幅は100Mbpsに設定されます。グローバルスロットルを無効にすると、すべてのノードで無効になります。

データ転送速度はビット/秒（bps）で表されることがよくありますが、スロットル値は1秒あたりのキロバイト数（KBps）で入力する必要があります。

ONTAP 9 .9.1以前のリリースでは、このスロットルは転送や負荷共有ミラー転送には影響しません `volume move`。ONTAP 9.10.0以降では、オプションを指定してボリューム移動処理を調整できます。詳細については、を参照してください "ONTAP 9.10以降でボリューム移動を調整する方法"。

グローバルスロットルは、SnapMirror転送およびSnapVault転送の関係ごとのスロットル機能と連携します。関係ごとのスロットルは、関係ごとの転送の帯域幅の合計がグローバルスロットルの値を超えるまで適用され、超えるとグローバルスロットルが適用されます。スロットル値を指定すると `0`、グローバルスロットルが無効になります。

SnapMirrorグローバルスロットルは、同期中のSnapMirror同期関係には影響しません。ただし、初期化処理などの非同期転送フェーズを実行する場合や非同期イベントの発生後にSnapMirror同期関係に影響します。そのため、SnapMirror同期関係でグローバルスロットルを有効にすることは推奨されません。

手順

1. グローバルスロットルを有効にします。

   ```
   options -option-name replication.throttle.enable on|off
   ```

   次に、でSnapMirrorグローバルスロットルをイネーブルにする例を示し `cluster_dst`ます。

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. デスティネーションクラスタで受信転送に使用される総帯域幅の最大値を指定します。

   ```
   options -option-name replication.throttle.incoming.max_kbs <KBps>
   ```

   推奨される最小スロットル帯域幅は4KB/秒（KBps）、最大値は2TB /秒（Tbps）です。このオプションのデフォルト値はで、使用される総帯域幅に制限はあり `unlimited`ません。

   次に、受信転送で使用される総帯域幅の最大値を100メガビット/秒（Mbps）に設定する例を示します。

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   100メガビット/秒（Mbps）= 12500キロバイト/秒（kbps）

3. ソースクラスタで送信転送に使用される総帯域幅の最大値を指定します。

   ```
   options -option-name replication.throttle.outgoing.max_kbs <KBps>
   ```

   推奨される最小スロットル帯域幅は4kbps、最大スロットル帯域幅は2Tbpsです。このオプションのデフォルト値はで、使用される総帯域幅に制限はあり `unlimited`ません。パラメータ値は、1秒あたりのキロバイト数（kbps）で指定します。

   次の例は、送信転送で使用される合計帯域幅の最大値を100Mbpsに設定する方法を示しています。

   ```
   cluster_src::> options -option-name
   replication.throttle.outgoing.max_kbs 12500
   ```

SnapMirror SVMレプリケーションを管理します。

ONTAP SnapMirror SVMレプリケーションの詳細

SnapMirrorを使用すると、SVM間のデータ保護関係を作成できます。このタイプのデータ保護関係では、SVMのすべてまたは一部の設定がNFSエクスポートおよびSMB共有からRBACにレプリケートされます。また、SVMが所有するボリューム内のデータもレプリケートされます。

サポートされている関係タイプ

レプリケート可能なのはデータ提供用SVMのみです。サポートされているデータ保護関係タイプは次のとおりです。

- _ SnapMirror DR、_。通常、デスティネーションにはソース上に現在あるSnapshotのみが含まれます。

  ONTAP 9.9.1以降では、mirror-vaultポリシーを使用している場合にこの動作が変更されます。ONTAP 9.9.1以降では、ソースとデスティネーションで異なるSnapshotポリシーを作成できます。デスティネーションのSnapshotはソースのSnapshotで上書きされません。

- スケジュールされた通常の処理、更新、および再同期の実行中に、ソースからデスティネーションに上書きされることはありません
- 解除処理の実行中に削除されることはありません。
- 逆再同期処理の実行中は削除されません。ONTAP 9 .9.1以降を使用するmirror-vaultポリシーを使用してSVMディザスタ関係を設定する場合、ポリシーは次のように動作します。
- ソースのユーザ定義のSnapshotポリシーはデスティネーションにコピーされません。
- システム定義のSnapshotポリシーはデスティネーションにコピーされません。
- ユーザ定義およびシステム定義のSnapshotポリシーとのボリュームの関連付けはデスティネーションにコピーされません。+ SVM

- *SnapMirror* 統合レプリケーション では、宛先は DR と長期保存の両方に対して構成されます。

SnapMirrorユニファイドレプリケーションの詳細については、を参照してください"SnapMirrorユニファイドレプリケーションの基本"。

レプリケーションポリシーの _policy type_of によって、サポートされる関係のタイプが決まります。次の表に、使用可能なポリシータイプを示します。

ポリシータイプ	関係タイプ
非同期ミラー	SnapMirror DR
ミラー-バックアップ	ユニファイドレプリケーション

ONTAP 9では、**SVM**レプリケーションのデフォルトは**DP**から**XDP**に変更されます。**4**

ONTAP 9 .4以降では、SVMデータ保護関係のデフォルトがXDPモードに変更されました。ONTAP 9 .3以前のSVMデータ保護関係のデフォルトは引き続きDPモードです。

XDPのデフォルト値は既存の関係には影響しません。すでにDPタイプの関係は、引き続きDPタイプになります。次の表に、想定される動作を示します。

指定するモード	タイプ	デフォルトポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	MirrorAndVault（ユニファイドレプリケーション）

DP関係からXDP関係への変換に関する情報およびその他の詳細については、を参照してください。"既存のONTAP DPタイプの関係をXDPに変換する"

バージョンに依存しないレプリケーションはSVMレプリケーションではサポートされません。SVMディザスタリカバリ設定では、フェイルオーバーおよびフェイルバック処理をサポートするために、デスティネーションSVMがソースSVMクラスタと同じバージョンのONTAPを実行しているクラスタである必要があります。

"SnapMirror関係に互換性があるONTAPのバージョン"

SVMの設定のレプリケート方法

SVMレプリケーション関係の内容は、次のフィールドの組み合わせによって決まります。

- コマンドのオプション `snapmirror create`は `-identity-preserve true`、SVMの設定全体をレプリケートします。

  オプションは `-identity-preserve false`、SVMのボリュームと認証と許可の設定、およびに記載されているプロトコルとネームサービスの設定のみをレプリケートします"SVMディザスタリカバリ関係でレプリケートされる設定"。

- コマンドのオプションを `snapmirror policy create`使用する `-discard-configs network`と、ソースとデスティネーションのSVMが異なるサブネットにある場合に使用するLIFと関連ネットワークの設定がSVMレプリケーション対象から除外されます。
- コマンドのオプションを `volume modify`使用すると `-vserver-dr-protection unprotected`、指定したボリュームがSVMレプリケーション対象から除外されます。

それ以外の場合、SVMレプリケーションはボリュームレプリケーションとほぼ同じです。SVMレプリケーションには、ボリュームレプリケーションとほぼ同じワークフローを使用できます。

サポートの詳細

次の表は、SnapMirror SVMレプリケーションのサポートの詳細を示しています。

リソースまたは機能	サポートの詳細
ドウニュウタイプ	• 単一のソースから単一のデスティネーション • ONTAP 9 .4以降、ファンアウト。ファンアウトできるのは2つのデスティネーションのみです。 デフォルトでは、-identity-preserve trueの関係はソースSVMごとに1つだけ指定できます。
関係タイプ	• SnapMirrorディザスタ リカバリ • SnapMirrorユニファイド レプリケーション
レプリケーションの範囲	クラスタ間のみ。同じクラスタ内のSVMをレプリケートすることはできません。

自律型ランサムウェア対策	• ONTAP 9.12.1以降でサポート。詳細については、を参照してください "自律型ランサムウェア対策"。
整合グループの非同期サポート	ONTAP 9 14.1以降では、整合グループが存在する場合に、SVMディザスタリカバリ関係が最大32個サポートされます。詳細については、およびを参照してください "整合グループの保護" "整合グループの制限"。
FabricPool	ONTAP 9.6以降では、FabricPoolでSnapMirror SVMレプリケーションがサポートされます。SVM DR関係では、ソースボリュームとデスティネーションボリュームでFabricPoolアグリゲートを使用する必要はありませんが、同じ階層化ポリシーを使用する必要があります。 ONTAP 9.12.1以降では、FabricPoolボリュームとFlexGroupボリュームが連動してSnapMirror SVMレプリケーションがサポートされます。9.12.1より前のバージョンでは、これらの機能のいずれか2つが連携して動作していましたが、3つすべてが連携するわけではありませ

MetroCluster	ONTAP 9.11.1以降では、MetroCluster構成内のSVMディザスタ リカバリ関係のソースとデスティネーション両方を、追加のSVMディザスタ リカバリ構成のソースにすることができます。 ONTAP 9.5以降のMetroCluster構成では、SnapMirror SVMレプリケーションがサポートされます。 • ONTAP 9.10.Xより前のリリースでは、MetroCluster構成をSVMディザスタ リカバリ関係のデスティネーションにすることはできません。 • ONTAP 9 .10.1以降のリリースでは、MetroCluster構成を移行目的でのみSVMディザスタリカバリ関係のデスティネーションにすることができます。この構成は、に記載されている必要なすべての要件を満たしている必要があります "TR-4966：『Migrating a SVM into a MetroCluster 解決策』"。 • SVMディザスタリカバリ関係のソースとして使用できるのは、MetroCluster構成のアクティブなSVMだけです。 スイッチオーバー前の同期元のSVMと、スイッチオーバー後の同期先のSVMがソースになります。 • MetroCluster構成が安定した状態のときはMetroClusterの同期先のSVMがオンラインでないため、同期先のSVMをSVMディザスタリカバリ関係のソースにすることはできません。 • 同期元のSVMがSVMディザスタリカバリ関係のソースである場合は、ソースのSVMディザスタリカバリ関係の情報がMetroClusterパートナーにレプリケートされます。 • スイッチオーバーおよびスイッチバックの処理中に、SVMディザスタリカバリデスティネーションへのレプリケーションが失敗することがあります。 ただし、スイッチオーバーまたはスイッチバックのプロセスが完了すると、SVMディザスタリカバリの次回のスケジュールされた更新は成功します。
整合グループ	ONTAP 9 14.1以降でサポートされています。詳細については、を参照してください 整合グループの保護。
ONTAP S3	SVMディザスタ リカバリではサポートされません。

SnapMirror Synchronous	SVMディザスタ リカバリではサポートされません。
バージョンに依存しない	サポートされません。
ボリューム暗号化	• ソースで暗号化されたボリュームがデスティネーションで暗号化されます。 • オンボード キー マネージャまたはKMIPサーバをデスティネーションで設定する必要があります。 • 新しい暗号化キーはデスティネーションで生成されます。 • ボリューム暗号化をサポートするノードがデスティネーションに含まれていない場合、レプリケーションは成功しますが、デスティネーション ボリュームは暗号化されません。

SVMディザスタリカバリ関係でレプリケートされる設定

次の表に、オプションと `snapmirror policy create -discard-configs network`オプションの相互作用を示し `snapmirror create -identity-preserve`ます。

レプリケートされる設定		**-identity-preserve true**		**-identity-preserve false**
		設定されていないポリシー **-discard-configs network**	セット付きポリシー **-discard-configs network**	
ネットワーク	NAS LIF	○	いいえ	いいえ
LIFのKerberos設定	○	いいえ	いいえ	SAN LIF
いいえ	いいえ	いいえ	ファイアウォールポリシー	○
○	いいえ	サービスポリシー	○	○
いいえ	ルート	○	いいえ	いいえ
ブロードキャストドメイン	いいえ	いいえ	いいえ	サブネット
いいえ	いいえ	いいえ	IPspace	いいえ
いいえ	いいえ	SMB	SMB サーバ	○

○	いいえ	ローカルグループとローカルユーザ	○	○
○	権限	○	○	○
シャドウコピー	○	○	○	BranchCache
○	○	○	サーバオプション	○
○	○	サーバセキュリティ	○	○
いいえ	ホームディレクトリ、共有	○	○	○
シンボリックリンク	○	○	○	FPolicyポリシー、fsecurityポリシー、およびfsecurity NTFS
○	○	○	ネームマッピングとグループマッピング	○
○	○	監査情報	○	○
○	NFS	エクスポートポリシー	○	○
いいえ	エクスポートポリシールール	○	○	いいえ
NFSサーバ	○	○	いいえ	RBAC
セキュリティ証明書	○	○	いいえ	ログインユーザ、公開鍵、ロール、およびロールの設定
○	○	○	SSL	○
○	いいえ	ネームサービス	DNSおよびDNSホスト	○
○	いいえ	UNIXユーザおよびUNIXグループ	○	○

○	Kerberos Realm とKerberosキーブロック	○	○	いいえ
LDAPおよびLDAPクライアント	○	○	いいえ	ネットグループ
○	○	いいえ	NIS	○
○	いいえ	WebおよびWebアクセス	○	○
いいえ	ボリューム	オブジェクト	○	○
○	Snapshot とSnapshotポリシー	○	○	○
自動削除ポリシー	いいえ	いいえ	いいえ	効率化ポリシー
○	○	○	クォータポリシーとクォータポリシールール	○
○	○	リカハリキユウ	○	○
○	ルートボリューム	ネームスペース	○	○
○	ユーザデータ	いいえ	いいえ	いいえ
qtree	いいえ	いいえ	いいえ	クォータ
いいえ	いいえ	いいえ	ファイルレベルのQoS	いいえ
いいえ	いいえ	属性：ルートボリュームの状態、スペースギャランティ、サイズ、オートサイズ、およびファイル総数	いいえ	いいえ
いいえ	ストレージQoS	QoSポリシーグループ	○	○

○	ファイバチャネル（FC）	いいえ	いいえ	いいえ
iSCSI	いいえ	いいえ	いいえ	LUN
オブジェクト	○	○	○	igroup
いいえ	いいえ	いいえ	ポートセット	いいえ
いいえ	いいえ	シリアル番号	いいえ	いいえ
いいえ	SNMP	v3ユーザ	○	○

SVMディザスタリカバリのストレージ制限

次の表に、ストレージオブジェクトごとにサポートされる推奨されるボリュームおよびSVMディザスタリカバリ関係の最大数を示します。制限は多くの場合プラットフォームに依存することに注意してください。特定の構成の制限については、を参照して"Hardware Universe"ください。

ストレージオブジェクト	制限
SVM	300個のフレキシブルボリューム
HAペア	フレキシブルボリューム×1、000
クラスタ	128個のSVMディザスタ関係

関連情報

- "スナップミラー作成"
- "snapmirror policy create"

SVM設定のレプリケート

ONTAP SnapMirror SVMレプリケーションのワークフロー

SnapMirror SVMレプリケーションでは、デスティネーションSVMを作成し、レプリケーションジョブスケジュールを作成し、SnapMirror関係を作成して初期化します。

ニーズに最適なレプリケーションワークフローを決定する必要があります。

- "SVMの設定全体をレプリケートする"
- "LIFと関連ネットワーク設定をSVMレプリケーション対象から除外"
- "ネットワーク、ネームサービス、およびその他の設定をSVM設定から除外する"

ONTAP SnapMirrorデスティネーションSVMにボリュームを配置する際の基準

ソースSVMからデスティネーションSVMにボリュームをレプリケートするときは、アグリゲートの選択基準を理解しておくことが重要です。

アグリゲートは次の基準に基づいて選択されます。

- ボリュームは常にルート以外のアグリゲートに配置されます。
- ルート以外のアグリゲートの中から、利用可能な空きスペースとホストしている既存のボリュームの数に基づいてアグリゲートが選択されます。

  空きスペースが多くボリュームが少ないアグリゲートが優先されます。最も優先順位が高いアグリゲートが選択されます。

- FabricPoolアグリゲートのソースボリュームは、同じ階層化ポリシーを使用するデスティネーションのFabricPoolアグリゲートに配置されます。
- ソース SVM のボリュームが Flash Pool アグリゲートにある場合、デスティネーション SVM に Flash Pool アグリゲートがあり、そのアグリゲートに十分な空きスペースがあれば、そのアグリゲートにボリュームが配置されます。
- レプリケートするボリュームのオプションがに設定されている `volume`場合 `-space-guarantee`は、空きスペースがボリュームサイズよりも大きいアグリゲートのみが考慮されます。
- ボリュームのサイズは、ソースボリュームのサイズに基づいて、レプリケーション時にデスティネーション SVM で自動的に拡張されます。

  デスティネーション SVM のサイズを事前にリザーブする場合は、ボリュームのサイズを変更する必要があります。ソース SVM に基づいて、デスティネーション SVM でボリュームのサイズが自動的に縮小されることはありません。

ボリュームをアグリゲート間で移動する場合は、デスティネーションSVMでコマンドを使用できます `volume move`。

ONTAP SVMの設定全体をレプリケートする

SVMディザスタリカバリ（SVM DR）関係を作成して、あるSVMの設定を別のSVMにレプリケートすることができます。プライマリサイトで災害が発生した場合は、デスティネーションSVMを簡単にアクティブ化できます。

開始する前に

ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。詳細については、およびを参照して"クラスタピア関係を作成します。""SVM のクラスタ間ピア関係を作成します"ください。

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

このワークフローでは、デフォルトポリシーまたはカスタムレプリケーションポリシーをすでに使用していることを前提としています。

ONTAP 9.9.1以降では、mirror-vaultポリシーを使用すると、ソースSVMとデスティネーションSVMで異なるSnapshotポリシーを作成でき、デスティネーションのSnapshotがソースのSnapshotで上書きされることはありません。詳細については、を参照してください "SnapMirror SVMレプリケーションの概要"。

デスティネーションからこの手順を実行します。ソースStorage VMでSMBを設定している場合などに新しい保護ポリシーを作成する必要がある場合は、ポリシーを作成して* Identity preserve *オプションを使用する必要があります。詳細は、を参照してください "カスタムのデータ保護ポリシーを作成する"。

手順

このタスクは、System ManagerまたはONTAP CLIから実行できます。

System Manager

1. デスティネーションクラスタで、 * Protection > Relationships * をクリックします。
2. で、[保護]をクリックし、[Storage VM（DR）]*を選択します。
3. 保護ポリシーを選択します。カスタムの保護ポリシーを作成した場合は選択し、レプリケートするソースクラスタとStorage VMを選択します。新しいデスティネーションStorage VM名を入力して新しいデスティネーションStorage VMを作成することもできます。
4. 必要に応じて、デスティネーションの設定を変更してID保持を上書きし、ネットワークインターフェイスおよびプロトコルを含めるか除外するかを指定します。
5. [保存（ Save ）] をクリックします。

CLI

1. デスティネーションSVMを作成します。

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   SVM名は、ソースクラスタとデスティネーションクラスタで一意である必要があります。

   次の例は、という名前のデスティネーションSVMを作成し `svm_backup`ます。

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

   の詳細については `vserver create`、を"ONTAPコマンド リファレンス"参照してください。

2. デスティネーションクラスタから、コマンドを使用してSVMピア関係を作成し `vserver peer create`ます。

   詳細については、を参照してください "SVM のクラスタ間ピア関係を作成します"。

   の詳細については `vserver peer create`、を"ONTAPコマンド リファレンス"参照してください。

3. レプリケーションジョブスケジュールを作成します。

   ```
   job schedule cron create -name <job_name> -month <month> -dayofweek
   <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
   ```

   `-dayofweek`、および `-hour`では `-month`、ジョブを毎月、曜日、および時間ごとに実行するように指定できます `all`。

SVM SnapMirror関係のFlexVolボリュームでサポートされる最小スケジュール（RPO）は15分です。SVM SnapMirror関係にあるFlexGroupボリュームに対してサポートされる最小スケジュール（RPO）は30分です。

次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

の詳細については `job schedule cron create`、を"ONTAPコマンド リファレンス"参照してください。

4. デスティネーションSVMまたはデスティネーションクラスタから、レプリケーション関係を作成します。

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

オプションと `-destination-path`オプションで、`SVM`名のあとにコロン（：）を入力する必要があります `-source-path`。

次の例は、デフォルトのポリシーを使用してSnapMirror DR関係を作成し `MirrorAllSnapshots`ます。

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

次の例は、デフォルトのポリシーを使用してユニファイドレプリケーション関係を作成し `MirrorAndVault`ます。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

ポリシータイプがのカスタムポリシーを作成した場合 `async-mirror`、次の例はSnapMirror DR関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

ポリシータイプがのカスタムポリシーを作成した場合、 `mirror-vault`次の例はユニファイドレプリケーション関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

5. デスティネーションSVMを停止します。

```
vserver stop -vserver <SVM_name>
```

次の例は、svm_backupという名前のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop -vserver svm_backup
```

の詳細については `vserver stop`、を"ONTAPコマンド リファレンス"参照してください。

6. デスティネーションSVMまたはデスティネーションクラスタから、SVMレプリケーション関係を初期化します。

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。

次の例は、ソースSVMとデスティネーションSVM `svm_backup`の間の関係を初期化し `svm1`ます。

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

LIFと関連ネットワーク設定を**ONTAP SnapMirror SVM**レプリケーション対象から除外

ソースとデスティネーションのSVMが異なるサブネットにある場合は、コマンドのオプションを `snapmirror policy create`使用して、LIFと関連ネットワークの設定をSVMレプ

リケーション対象から除外でき `-discard-configs network`ます。

開始する前に

ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

詳細については、およびを参照して"クラスタピア関係を作成します。""SVM のクラスタ間ピア関係を作成します"ください。

タスクの内容

`-identity-preserve`SVMレプリケーション関係を作成するときに、コマンドのオプションを`snapmirror create`に設定する必要があります `true`。

手順

1. デスティネーションSVMを作成します。

   ```
   vserver create -vserver SVM -subtype dp-destination
   ```

   SVM名は、ソースクラスタとデスティネーションクラスタで一意である必要があります。

   次の例は、という名前のデスティネーションSVMを作成し `svm_backup`ます。

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. デスティネーションクラスタから、コマンドを使用してSVMピア関係を作成し `vserver peer create`ます。

   詳細については、を参照してください "SVM のクラスタ間ピア関係を作成します"。

   の詳細については `vserver peer create`、を"ONTAPコマンド リファレンス"参照してください。

3. ジョブスケジュールを作成します。

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   `-dayofweek`、および `-hour`では `-month`、ジョブを毎月、曜日、および時間ごとに実行するように指定できます `all`。

   SVM SnapMirror関係のFlexVolボリュームでサポートされる最小スケジュール（RPO）は15分です。SVM SnapMirror関係にあるFlexGroupボリュームに対してサポートされる最小スケジュール（RPO）は30分です。

   次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. カスタムレプリケーションポリシーを作成します。

   `snapmirror policy create -vserver` *SVM* `-policy` *policy* `-type async-mirror|vault|mirror-vault -comment` *comment* `-tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   次の例は、LIFを除外するSnapMirror DR用のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

   次の例は、LIFを除外するユニファイドレプリケーション用のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

   > 今後のフェイルオーバーとフェイルバックのシナリオに備えて、ソースクラスタに同じカスタムSnapMirrorポリシーを作成することを検討してください。

   の詳細については `snapmirror policy create`、を"ONTAPコマンド リファレンス"参照してください。

5. デスティネーションSVMまたはデスティネーションクラスタから次のコマンドを実行して、レプリケーション関係を作成します。

   `snapmirror create -source-path` *SVM*`:` `-destination-path` *SVM*`:` `-type DP|XDP -schedule` *schedule* `-policy` *policy* `-identity-preserve true|false -discard -configs true|false`

   > オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

   次の例は、LIFを除外するSnapMirror DR関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

   次の例は、LIFを除外するSnapMirrorユニファイドレプリケーション関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

6. デスティネーションSVMを停止します。

   `vserver stop`

   `SVM name`

   次の例は、svm_backupという名前のデスティネーションSVMを停止します。

   ```
   cluster_dst::> vserver stop -vserver svm_backup
   ```

7. デスティネーションSVMまたはデスティネーションクラスタから、レプリケーション関係を初期化します。

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   次の例は、ソースとデスティネーションの `svm_backup`間の関係を初期化し `svm1`ます。

   ```
   cluster_dst::> snapmirror initialize -source-path svm1: -destination
   -path svm_backup:
   ```

   の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

終了後

災害発生時のデータアクセス用に、デスティネーションSVMでネットワークとプロトコルを設定する必要があります。

関連情報

- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror policy create"

ONTAPを使用したSVMレプリケーション対象からネットワーク、ネームサービス、およびその他の設定を除外する

デスティネーションSVMとの競合や設定の違いを避けるために、ネットワーク、ネームサービス、およびその他の設定をSVMレプリケーション関係から除外することができます。

コマンドのオプションを `snapmirror create`使用すると、SVMのボリュームとセキュリティ設定だけをレ

プリケートできます `-identity-preserve false`。一部のプロトコルとネームサービスの設定も保持されます。

タスクの内容

保持されるプロトコルとネームサービスの設定のリストについては、を参照してください"SVM DR関係でレプリケートされる設定"。

開始する前に

ソースとデスティネーションのクラスタとSVMのピア関係が確立されている必要があります。

詳細については、およびを参照して"クラスタピア関係を作成します。""SVM のクラスタ間ピア関係を作成します"ください。

手順

1. デスティネーションSVMを作成します。

   `vserver create -vserver SVM -subtype dp-destination`

   SVM名は、ソースクラスタとデスティネーションクラスタで一意である必要があります。

   次の例は、という名前のデスティネーションSVMを作成し `svm_backup`ます。

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. デスティネーションクラスタから、コマンドを使用してSVMピア関係を作成し `vserver peer create`ます。

   詳細については、を参照してください "SVM のクラスタ間ピア関係を作成します"。

   の詳細については `vserver peer create`、を"ONTAPコマンド リファレンス"参照してください。

3. レプリケーションジョブスケジュールを作成します。

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   `-dayofweek`、および `-hour`では `-month`、ジョブを毎月、曜日、および時間ごとに実行するように指定できます `all`。

   SVM SnapMirror関係のFlexVolボリュームでサポートされる最小スケジュール（RPO）は15分です。SVM SnapMirror関係にあるFlexGroupボリュームに対してサポートされる最小スケジュール（RPO）は30分です。

   次の例は、土曜日の午前3時に実行するという名前のジョブスケジュールを作成します `my_weekly`。

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. ネットワーク、ネームサービス、およびその他の設定を除外してレプリケーション関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve false
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。このコマンドはデスティネーションSVMまたはデスティネーションクラスタから実行する必要があります。

次の例は、デフォルトのポリシーを使用して、SnapMirror DR関係を作成し`MirrorAllSnapshots`ます。この関係では、ネットワーク、ネームサービス、およびその他の設定がSVMレプリケーション対象から除外されます。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

次の例は、デフォルトのポリシーを使用して、ユニファイドレプリケーション関係を作成し`MirrorAndVault`ます。この関係から、ネットワーク、ネームサービス、およびその他の設定が除外されます。

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

ポリシータイプがのカスタムポリシーを作成した場合 `async-mirror`、次の例はSnapMirror DR関係を作成します。この関係では、ネットワーク、ネームサービス、およびその他の設定がSVMレプリケーション対象から除外されます。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

ポリシータイプがのカスタムポリシーを作成した場合 `mirror-vault`、次の例はユニファイドレプリケーション関係を作成します。この関係では、ネットワーク、ネームサービス、およびその他の設定がSVMレプリケーション対象から除外されます。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

5. デスティネーションSVMを停止します。

   `vserver stop`

   `SVM name`

   次の例は、dvs1という名前のデスティネーションSVMを停止します。

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. SMBを使用する場合は、SMBサーバも設定する必要があります。

   を参照して "SMB のみ： SMB サーバの作成"

7. デスティネーションSVMまたはデスティネーションクラスタから、SVMレプリケーション関係を初期化します。

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

   の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

終了後

災害発生時のデータアクセス用に、デスティネーションSVMでネットワークとプロトコルを設定する必要があります。

ONTAP SnapMirror SVM DR関係に使用するローカル階層を指定します

ディザスタリカバリSVMの作成後、コマンドでオプションを `vserver modify`使用して、`SVM DR`デスティネーションボリュームのホストに使用するローカル階層を制限できます `aggr-list`。

手順

1. デスティネーションSVMを作成します。

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. ディザスタリカバリSVMのaggr-listを変更して、ディザスタリカバリSVMのボリュームのホストに使用されるローカル階層を制限します。

   `cluster_dest::> vserver modify -vserver` *`SVM`* `-aggr-list <comma-separated-list>`

DR関係のONTAP SnapMirrorデスティネーションSVM用のSMBサーバを作成する

ソースSVMでSMB構成が使用されていて、をに `false`選択した場合は `identity-preserve`、デスティネーションSVM用のSMBサーバを作成する必要がありま

す。SnapMirror関係の初期化中に共有など、一部のSMB構成ではSMBサーバが必要になります。

手順

1. コマンドを使用して、デスティネーションSVMを起動し `vserver start`ます。

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

の詳細については `vserver start`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用して、 `vserver show`デスティネーションSVMの状態がであること、およびサブタイプがである `dp-destination`ことを確認します `running`。

```
destination_cluster::> vserver show
                                  Admin      Operational Root
Vserver  Type    Subtype          State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination   running    running       -         -
```

の詳細については `vserver show`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドを使用して、LIFを作成し `network interface create`ます。

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してください。

4. コマンドを使用して、ルートを作成し `network route create`ます。

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"ネットワーク管理"

の詳細については `network route create`、を"ONTAPコマンド リファレンス"参照してください。

5. コマンドを使用して、DNSを設定し `vserver services dns create`ます。

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

の詳細については `vserver services dns create`、を"ONTAPコマンド リファレンス"参照してください。

6. コマンドを使用して、優先ドメインコントローラを追加し `vserver cifs domain preferred-dc add`ます。

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

の詳細については `vserver cifs domain preferred-dc add`、を"ONTAPコマンド リファレンス"参照してください。

7. コマンドを使用して、SMBサーバを作成し `vserver cifs create`ます。

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

の詳細については `vserver cifs create`、を"ONTAPコマンド リファレンス"参照してください。

8. コマンドを使用して、デスティネーションSVMを停止し `vserver stop`ます。

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

の詳細については `vserver stop`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapMirror SVM DR関係からボリュームを除外する

デフォルトでは、ソースSVMのすべてのRWデータボリュームがレプリケートされます。保護する必要がないボリュームがソースSVMにある場合は、コマンドのオプションを `volume modify`使用して、ボリュームを`SVM`レプリケーション対象から除外できます `-vserver-dr-protection unprotected`。

手順

1. SVMレプリケーション対象からボリュームを除外します。

`volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected`

の詳細については `volume modify`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、ボリュームをSVMレプリケーション対象から除外し `volA_src`ます。

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

最初に除外したボリュームをあとでSVMレプリケーション対象に含める場合は、次のコマンドを実行します。

`volume modify -vserver SVM -volume volume -vserver-dr-protection protected`

次の例は、ボリュームをSVMレプリケーション対象に追加し `volA_src`ます。

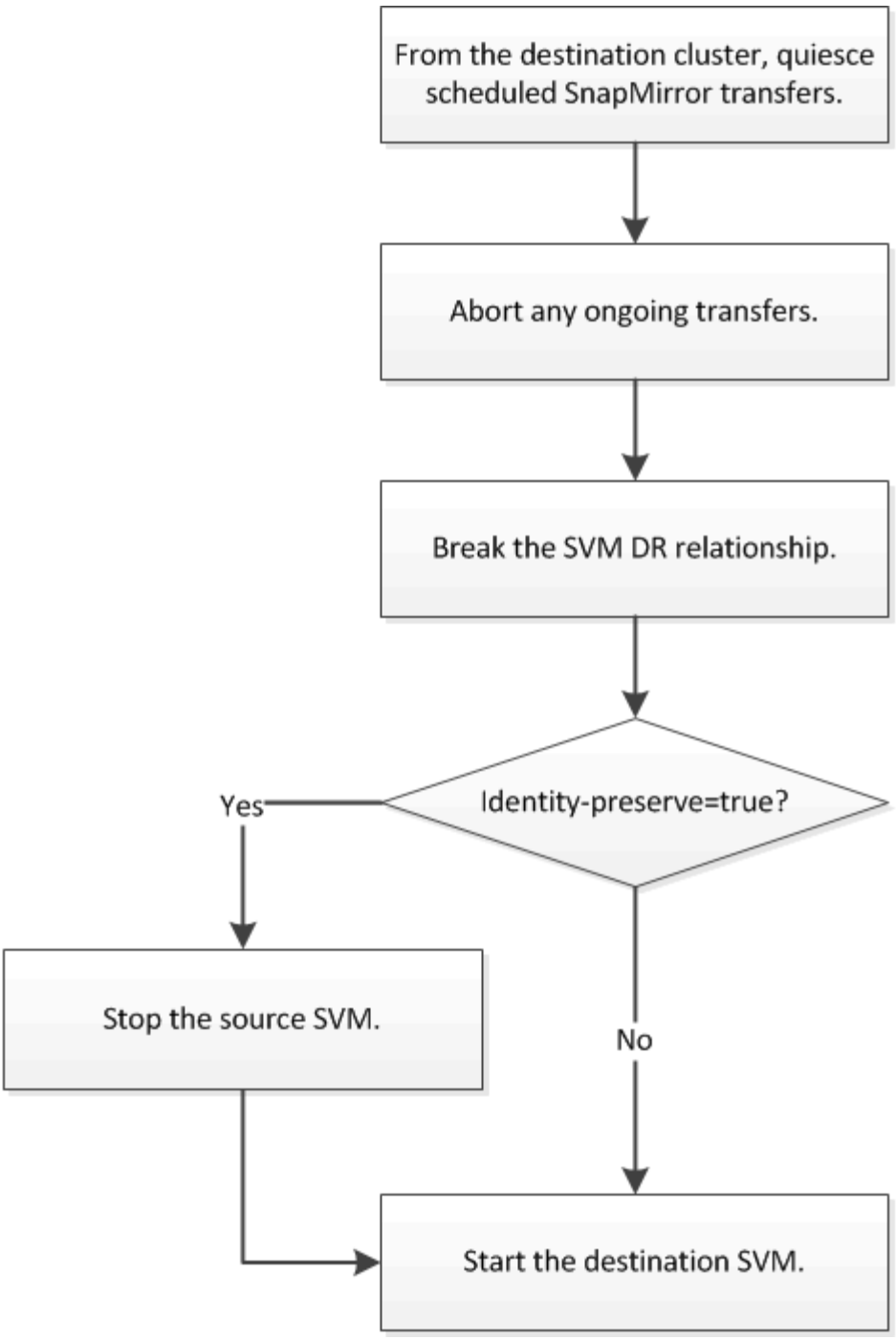
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. の説明に従って、SVMレプリケーション関係を作成して初期化します"SVMの設定全体のレプリケート"。

SnapMirror SVM DRデスティネーションからのデータの提供

ONTAP SnapMirror SVMディザスタリカバリのワークフロー

災害からリカバリし、デスティネーションSVMからデータを提供するには、デスティネーションSVMをアクティブ化する必要があります。デスティネーションSVMのアクティブ化では、スケジュールされたSnapMirror転送の停止、実行中のSnapMirror転送の中止、レプリケーション関係の解除、ソースSVMの停止、デスティネーションSVMの起動が実行されます。



ONTAP SnapMirror SVMデスティネーションボリュームを書き込み可能として設定

クライアントにデータを提供する前に、 SVM デスティネーションボリュームを書き込み可能にする必要があります。

この手順は、1つの例外を除き、ボリュームレプリケーションの手順とほとんど同じです。SVMレプリケーション関係の作成時にを設定した場合は `-identity-preserve true` 、デスティネーションSVMをアクティブ化する前にソースSVMを停止する必要があります。

タスクの内容

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ディザスタリカバリシナリオでは、ソースSVMとそのデータにアクセスできなくなるほか、前回の再同期後の更新に障害が発生したり破損したりする可能性があるため、ソースSVMからディザスタリカバリデスティネーションSVMへのSnapMirror更新を実行できません。

ONTAP 9.8以降では、System Managerを使用して、災害発生後にデスティネーションStorage VMをアクティブ化できます。デスティネーションStorage VMをアクティブ化すると、SVMデスティネーションボリュームが書き込み可能になり、クライアントにデータを提供できるようになります。

手順

このタスクは、System ManagerまたはONTAP CLIから実行できます。

System Manager

1. ソースクラスタにアクセスできる場合は、SVMが停止していることを確認します。* Storage > Storage VM*に移動し、SVMの* State *列を確認します。
2. ソースSVMの状態が「実行中」の場合は停止します。を選択し、*[停止]*を選択 ⋮ します。
3. デスティネーションクラスタで、目的の保護関係を探します。* Protection > Relationships *に移動します。
4. 目的のソースStorage VM名にカーソルを合わせ、をクリックし ⋮、*デスティネーションStorage VMのアクティブ化*を選択します。
5. ウィンドウで、[デスティネーションStorage VMをアクティブ化して関係を解除する]*を選択します。
6. [Activate （有効化）] をクリックします

CLI

1. 宛先 SVM または宛先クラスタから、SVM を静止して、宛先へのスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

ⓘ オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、ソースSVMとデスティネーションSVM `svm_backup`の間のスケジュールされた転送を停止します `svm1`。

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

の詳細については `snapmirror quiesce`、を"ONTAPコマンド リファレンス"参照してください。

2. デスティネーションSVMまたはデスティネーションクラスタから、デスティネーションへの実行中の転送を停止します。

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

ⓘ オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、ソースSVMとデスティネーションSVM `svm_backup`の間の実行中の転送を停止します `svm1`。

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

の詳細については `snapmirror abort`、を"ONTAPコマンド リファレンス"参照してください。

3. デスティネーションSVMまたはデスティネーションクラスタから、レプリケーション関係を解除します。

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> オプションと `-destination-path`オプションで、`SVM`名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、ソースSVMとデスティネーションSVM `svm_backup`の間の関係を解除し `svm1`ます。

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

4. SVMレプリケーション関係の作成時にを設定した場合は `-identity-preserve true`、ソースSVMを停止します。

```
vserver stop -vserver <SVM>
```

次の例は、ソースSVMを停止し `svm1`ます。

```
cluster_src::> vserver stop svm1
```

5. デスティネーション SVM を起動します。

```
vserver start -vserver <SVM>
```

次の例は、デスティネーションSVMを起動し `svm_backup`ます。

```
cluster_dst::> vserver start svm_backup
```

終了後

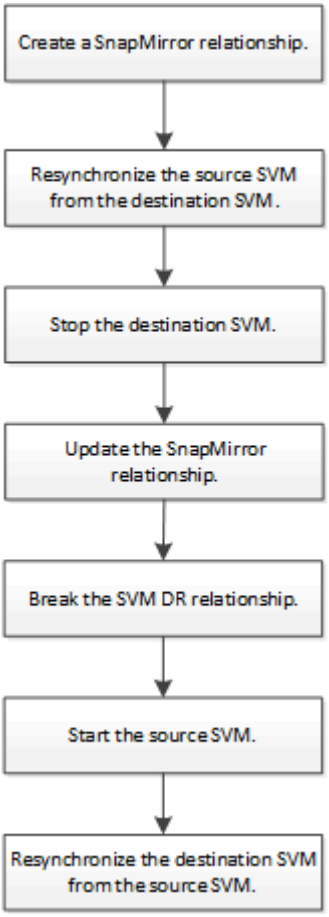
の説明に従って、データアクセス用のSVMデスティネーションボリュームを設定します"データアクセス

のためのデスティネーションボリュームの設定"。

SnapMirrorソースSVMを再アクティブ化する

ONTAP SnapMirrorソースSVMの再アクティブ化ワークフロー

災害発生後もソースSVMが残っている場合は、ソースSVMを再アクティブ化し、SVMディザスタリカバリ関係を再作成して保護できます。



元のONTAP SnapMirrorソースSVMを再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソースSVMとデスティネーションSVMの間で元のデータ保護関係を再確立できます。この手順は、1つの例外を除き、ボリュームレプリケーションの手順とほとんど同じです。ソースSVMを再アクティブ化する前に、デスティネーションSVMを停止する必要があります。

開始する前に

デスティネーションボリュームからのデータの提供中にデスティネーションボリュームのサイズを拡張した場合は、ソースボリュームを再アクティブ化する前に、元のソースボリュームを十分に拡張できるようにmax-autosizeを手動で増やす必要があります。

"デスティネーションボリュームが自動的に拡張されるタイミング"

タスクの内容

ONTAP 9 .11.1以降では、 `-quick-resync true snapmirror resync`SVM DR関係の逆再同期を実行する際にコマンドのCLIオプションを使用することで、ディザスタリカバリのリハーサル中の再同期時間を短縮できます。迅速な再同期を行うと、Data Warehouseの再構築とリストアの処理が省略されるため、本番環境への復帰にかかる時間を短縮できます。の詳細については `snapmirror resync、を"ONTAPコマンドリファレンス"参照してください。

> クイック再同期では、デスティネーションボリュームのストレージ効率が維持されません。クイック再同期を有効にすると、デスティネーションボリュームで使用されるボリュームスペースが増える可能性があります。

この手順は、元のソースボリュームのベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、この手順を実行する前に、データの提供元のボリュームと元のソースボリュームの間の関係を作成して初期化する必要があります。

ONTAP 9 8以降では、System Managerを使用して災害発生後にソースStorage VMを再アクティブ化できます。ソースStorage VMを再アクティブ化すると、デスティネーションStorage VMが停止し、ソースからデスティネーションへのレプリケーションが再度有効になります。

System Managerを使用してソースStorage VMを再アクティブ化すると、System Managerはバックグラウンドで次の処理を実行します。

- SnapMirror再同期を使用して、元のデスティネーションから元のソースへの逆方向のSVM DR関係を作成します。
- デスティネーションSVMを停止します。
- SnapMirror関係を更新します。
- SnapMirror関係を解除します。
- 元のSVMを再起動します。
- 元のソースから元のデスティネーションへのSnapMirror再同期を実行します。
- SnapMirror関係をクリーンアップします。

手順

このタスクは、System ManagerまたはONTAP CLIから実行できます。

System Manager

1. デスティネーションクラスタで、*[保護]>[関係]*をクリックし、必要な保護関係を特定します。
2. ソース関係の名前にカーソルを合わせ、をクリックし、*[ソースStorage VMの再アクティブ化]*を選択します。
3. ウィンドウで、[再アクティブ化]*をクリックします。
4. ［*関係*］ で、保護関係の ［*転送ステータス*］ を表示して、ソースの再アクティブ化の進行状況を監視します。再アクティブ化が完了すると、関係の状態は「mirrored」に戻ります。

CLI

1. 元のソースSVMまたはソースクラスタから、元のSVM DR関係と同じ設定、ポリシー、およびidentity-preserve設定を使用して、反転したSVM DR関係を作成します。

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元のSVMと元のソースSVM `svm1`の間に関係を作成します `svm_backup`。

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

2. 元のソースSVMまたはソースクラスタから次のコマンドを実行して、データ保護関係を反転します。

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

> ソースとデスティネーションに共通のSnapshotが存在しない場合、コマンドは失敗します。を使用し `snapmirror initialize`て関係を再初期化します。

次の例は、元のソースSVMとデータの提供元のSVM `svm_backup`の間の関係を反転します `svm1`。

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

quick-resyncオプションの使用例：

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. 元のソースSVMへのデータアクセスを再確立する準備ができたら、元のデスティネーションSVMを停止して、元のデスティネーションSVMに現在接続されているクライアントをすべて切断します。

```
vserver stop -vserver <SVM>
```

次の例は、現在データを提供している元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

4. コマンドを使用して、元のデスティネーションSVMの状態がstoppedであることを確認します `vserver show`。

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. 元のソースSVMまたはソースクラスタから次のコマンドを実行して反転した関係を最後に更新し、元のデスティネーションSVMから元のソースSVMにすべての変更を転送します。

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元である元のデスティネーションSVMと元のソースSVM `svm1`の間の関係を更新します,`svm_backup`。

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

6. 元のソースSVMまたはソースクラスタから次のコマンドを実行して、反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元のSVMと元のSVM `svm1`の間のスケジュールされた転送を停止します `svm_backup`。

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. 最後の更新が完了し、関係のステータスが「Quiesced」になったら、元のソースSVMまたはソースクラスタから次のコマンドを実行して反転した関係を解除します。

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元であった元のデスティネーションSVMと元のソースSVM `svm1`の間の関係を解除します `svm_backup`。

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

8. 元のソースSVMを停止していた場合は、元のソースクラスタから元のソースSVMを起動します。

```
vserver start -vserver <SVM>
```

次の例は、元のソースSVMを起動します。

```
cluster_src::> vserver start svm1
```

9. 元のデスティネーションSVMまたはデスティネーションクラスタから、元のデータ保護関係を再確立します。

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のソースSVMと元のデスティネーションSVM `svm_backup`の間の関係を再確立し `svm1`ます。

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. 元のソースSVMまたはソースクラスタから次のコマンドを実行して、反転したデータ保護関係を削除します。

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のデスティネーションSVMと元のソースSVM `svm1`の間の反転した関係を削除します `svm_backup`。

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. 元のデスティネーションSVMまたはデスティネーションクラスタから、反転したデータ保護関係を解放します。

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のデスティネーションSVM svm_backupと元のソースSVMの間の反転した関係をリリースします。 `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

終了後

コマンドを使用し `snapmirror show`て、SnapMirror関係が作成されたことを確認します。

の詳細については `snapmirror show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーの初期化"
- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"

FlexGroupボリューム用の元の**ONTAP SnapMirror**ソース**SVM**を再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソースSVMとデスティネーションSVMの間で元のデータ保護関係を再確立できます。FlexGroupボリュームを使用している場合に元のソースSVMを再アクティブ化するには、いくつかの追加手順を実行する必要があります。たとえば、元のSVM DR関係を削除し、元の関係を解除してから関係を反転する必要があります。また、スケジュールされた転送を停止する前に、反転した関係を解放して元の関係を再作成する必要があります。

手順

1. 元のデスティネーションSVMまたはデスティネーションクラスタから、元のSVM DR関係を削除します。

   ```
   snapmirror delete -source-path SVM: -destination-path SVM:
   ```

   オプションと `-destination-path`オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

   次の例は、元のソースSVM svm1と元のデスティネーションSVMの間の元の関係を削除します `svm_backup`。

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. 元のソースSVMまたはソースクラスタから、Snapshotを変更せずに元の関係を解放します。

   ```
   snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
   ```

`-only true`

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のソースSVM svm1と元のデスティネーションSVMの間の元の関係をリリースします `svm_backup`。

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. 元のソースSVMまたはソースクラスタから、元のSVM DR関係と同じ設定、ポリシー、およびidentity-preserve設定を使用して、反転したSVM DR関係を作成します。

`snapmirror create -source-path SVM: -destination-path SVM:`

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元のSVMと元のソースSVM `svm1` の間に関係を作成します `svm_backup`。

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. 元のソースSVMまたはソースクラスタから次のコマンドを実行して、データ保護関係を反転します。

`snapmirror resync -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

> ソースとデスティネーションに共通のSnapshotが存在しない場合、コマンドは失敗します。を使用し `snapmirror initialize` て関係を再初期化します。

次の例は、元のソースSVMとデータの提供元のSVM `svm_backup` の間の関係を反転します `svm1`。

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. 元のソースSVMへのデータアクセスを再確立する準備ができたら、元のデスティネーションSVMを停止して、元のデスティネーションSVMに現在接続されているクライアントをすべて切断します。

`vserver stop -vserver SVM`

次の例は、現在データを提供している元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

6. コマンドを使用して、元のデスティネーションSVMの状態がstoppedであることを確認します `vserver show`。

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

7. 元のソースSVMまたはソースクラスタから次のコマンドを実行して反転した関係を最後に更新し、元のデスティネーションSVMから元のソースSVMにすべての変更を転送します。

`snapmirror update -source-path SVM: -destination-path SVM:`

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（:）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元である元のデスティネーションSVMと元のソースSVM `svm1` の間の関係を更新します, `svm_backup`。

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

8. 元のソースSVMまたはソースクラスタから次のコマンドを実行して、反転した関係のスケジュールされた転送を停止します。

`snapmirror quiesce -source-path SVM: -destination-path SVM:`

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（:）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、データの提供元のSVMと元のSVM `svm1` の間のスケジュールされた転送を停止します `svm_backup`。

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

の詳細については `snapmirror quiesce`、を"ONTAPコマンド リファレンス"参照してください。

9. 最後の更新が完了し、関係のステータスが「Quiesced」になったら、元のソースSVMまたはソースクラスタから次のコマンドを実行して反転した関係を解除します。

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

   次の例は、データの提供元であった元のデスティネーションSVMと元のソースSVM `svm1` の間の関係を解除します `svm_backup`。

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

   の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

10. 元のソースSVMを停止していた場合は、元のソースクラスタから元のソースSVMを起動します。

    `vserver start -vserver SVM`

    次の例は、元のソースSVMを起動します。

    ```
    cluster_src::> vserver start svm1
    ```

11. 元のソースSVMまたはソースクラスタから、反転したSVM DR関係を削除します。

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    > オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

    次の例は、元のデスティネーションSVM svm_backupと元のソースSVMの間の反転した関係を削除します `svm1`。

    ```
    cluster_src::> snapmirror delete -source-path svm_backup: -destination
    -path svm1:
    ```

12. 元のデスティネーションSVMまたはデスティネーションクラスタから、Snapshotはそのまま残したまま反転した関係をリリースします。

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
-only true
```

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のデスティネーションSVM svm_backupと元のソースSVM svm1の間の反転した関係をリリースします。

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. 元のデスティネーションSVMまたはデスティネーションクラスタから、元の関係を再作成します。元のSVM DR関係と同じ設定、ポリシー、およびidentity-preserve設定を使用します。

```
snapmirror create -source-path SVM: -destination-path SVM:
```

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のソースSVMと元のデスティネーションSVM `svm_backup`の間の関係を作成し `svm1`ます。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. 元のデスティネーションSVMまたはデスティネーションクラスタから、元のデータ保護関係を再確立します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```

> オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

次の例は、元のソースSVMと元のデスティネーションSVM `svm_backup`の間の関係を再確立し `svm1`ます。

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーの初期化"

- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"

ONTAP SnapMirrorデスティネーション**SVM**上のデータを再同期する

ONTAP 9 .11.1では、ディザスタリカバリのリハーサルの実行時にData Warehouseの完全なリビルドをバイパスするオプションが導入されているため、本番環境への迅速な復帰が可能になりました。

ONTAP 9 8以降では、System Managerを使用して、解除した保護関係のソースStorage VMからデスティネーションStorage VMにデータおよび設定の詳細を再同期し、関係を再確立できます。

再同期処理は元の関係のデスティネーションからのみ実行できます。再同期では、ソースStorage VMのデータよりも新しいデスティネーションStorage VMのデータがすべて削除されます。

手順

このタスクは、System ManagerまたはONTAP CLIを使用して実行できます。

System Manager

1. デスティネーションから、必要な保護関係を選択します。*[保護]>[関係]*をクリックします。
2. 必要に応じて、［クイック再同期を実行する］を選択すると、災害復旧のリハーサル時にデータウェアハウスの完全な再構築をバイパスできます。
3. をクリックし、*[再同期]*をクリックします。
4. 「 * Relationships * 」で、関係の「 * Transfer Status * 」を表示して、再同期の進捗状況を監視します。

CLI

1. デスティネーションクラスタから、関係を再同期します。

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

関連情報

- "snapmirror resync"

ONTAP SnapMirrorボリュームDR関係をSVM DR関係に変換する

ソース上の各ボリューム（ルートボリュームを除く）をレプリケート中で、ソース上の各ボリューム（ルートボリュームを含む）の名前がデスティネーション上のボリュームと同じである場合は、ボリューム間のレプリケーション関係を、そのボリュームを所有するStorage Virtual Machine（SVM）間のレプリケーション関係に変換できます。

タスクの内容

必要に応じて、SnapMirror関係がアイドル状態のときにコマンドを使用して、 `volume rename`デスティネーションボリュームの名前を変更します。の詳細については `volume rename`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. デスティネーションSVMまたはデスティネーションクラスタから次のコマンドを実行して、ソースボリュームとデスティネーションボリュームを再同期します。

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   の詳細については `snapmirror resync`、を"ONTAPコマンド リファレンス"参照してください。

   再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

   次の例は、の `svm1`ソースボリュームとの `svm_backup`デスティネーションボリューム `volA`の間の関係を再同期し `volA`ます。

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. の説明に従って、ソースとデスティネーションのSVM間にSVMレプリケーション関係を作成します"SVMの設定のレプリケート"。

   レプリケーション関係を作成するときは、コマンドのオプションを `snapmirror create`使用する必要があります `-identity-preserve true`。

   の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

3. デスティネーションSVMを停止します。

   ```
   vserver stop -vserver SVM
   ```

   の詳細については `vserver stop`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、デスティネーションSVMを停止し `svm_backup`ます。

   ```
   cluster_dst::> vserver stop svm_backup
   ```

4. デスティネーションSVMまたはデスティネーションクラスタから次のコマンドを実行して、ソースとデスティネーションのSVMを再同期します。

   ```
   snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP
   -policy <policy>
   ```

オプションと `-destination-path` オプションで、SVM名のあとにコロン（:）を入力する必要があります `-source-path`。以下の例を参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、ソースSVMとデスティネーションSVM `svm_backup` の間の関係を再同期し `svm1` ます。

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

関連情報

- "スナップミラー作成"
- "snapmirror resync"

ONTAP SnapMirror SVMレプリケーション関係を削除する

コマンドと `snapmirror release` コマンドを使用して、SVMレプリケーション関係を削除できます `snapmirror delete`。その後、不要なデスティネーションボリュームを手動で削除できます。この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

タスクの内容

`snapmirror release` コマンドは、SnapMirrorで作成されたSnapshotをソースから削除します。オプションを使用すると、Snapshotを保持できます `-relationship-info-only`。

手順

1. デスティネーションSVMまたはデスティネーションクラスタから次のコマンドを実行して、レプリケーション関係を解除します。

   `snapmirror break -source-path SVM: -destination-path SVM:`

   オプションと `-destination-path` オプションで、SVM名のあとにコロン（:）を入力する必要があります `-source-path`。以下の例を参照してください。

   次の例は、ソースSVMとデスティネーションSVM `svm_backup` の間の関係を解除し `svm1` ます。

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

   の詳細については `snapmirror break`、を"ONTAPコマンド リファレンス"参照してください。

2. デスティネーション SVM またはデスティネーションクラスタから次のコマンドを実行して、レプリケーション関係を削除します。

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

   次の例は、ソースSVMとデスティネーションSVM `svm_backup`の間の関係を削除し `svm1`ます。

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

   の詳細については `snapmirror delete`、を"ONTAPコマンド リファレンス"参照してください。

3. ソースクラスタまたはソース SVM から次のコマンドを実行して、ソース SVM からレプリケーション関係情報をリリースします。

   `snapmirror release -source-path SVM: -destination-path SVM:`

   > オプションと `-destination-path` オプションで、SVM名のあとにコロン（：）を入力する必要があります `-source-path`。以下の例を参照してください。

   次の例は、指定したレプリケーション関係の情報をソースSVMからリリースします `svm1`。

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

   の詳細については `snapmirror release`、を"ONTAPコマンド リファレンス"参照してください。

SnapMirrorルートボリュームのレプリケーションを管理します。

ONTAP SnapMirrorルートボリュームレプリケーションの詳細

NAS 環境内のすべての SVM には一意のネームスペースがあります。オペレーティングシステムと関連情報を含む svm_root ボリュームは、ネームスペース階層へのエントリポイントです。ノードに障害やフェイルオーバーが発生したときに引き続きクライアントからデータにアクセスできるようにするには、 SVM ルートボリュームの負荷共有ミラーコピーを作成する必要があります。

SVMルートボリュームの負荷共有ミラーの主な目的は、負荷共有ではなく、ディザスタリカバリです。

- ルートボリュームが一時的に使用できなくなった場合は、負荷共有ミラーによって、ルートボリュームのデータへの読み取り専用アクセスが自動的に提供されます。

- ルートボリュームが完全に使用できなくなった場合は、いずれかの負荷共有ボリュームを昇格させて、ルートボリュームのデータへの書き込みアクセスを提供できます。

ONTAP負荷共有ミラー関係を作成して初期化する

クラスタ内のNASデータを提供するそれぞれのSVMルート ボリュームについて、負荷共有ミラー（LSM）を作成する必要があります。2 つ以上の HA ペアで構成されるクラスタの場合、HA ペアの両方のノードに障害が発生した場合でもクライアントが名前空間にアクセスできるようにするために、SVM ルート ボリュームの負荷共有ミラーを検討する必要があります。負荷共有ミラーは、単一のHAペアで構成されるクラスタには適していません。

開始する前に

ONTAP 9.16.1 以降では、負荷共有ミラー関係を作成するときに、デスティネーション SVM でストレージ制限を有効にすることはできません。

タスクの内容

同じノードにLSMを作成し、そのノードが使用できない場合は、単一点障害が発生します。また、クライアントから引き続きデータにアクセスできるようにするための2つ目のコピーは作成されません。ただし、ルートボリュームを含むノード以外のノードや別のHAペアにLSMを作成すると、障害が発生してもデータに引き続きアクセスできます。

たとえば、3つのノードにルートボリュームがある4ノードクラスタの場合は、次のようになります。

- HA 1のノード1のルートボリュームについて、HA 2のノード1またはHA 2のノード2にLSMを作成します。
- HA 1のノード2のルートボリュームについて、HA 2のノード1またはHA 2のノード2にLSMを作成します。
- HA 2のノード1のルートボリュームについて、HA 1のノード1またはHA 1のノード2にLSMを作成します。

手順

1. LSMのデスティネーションボリュームを作成します。

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

デスティネーションボリュームのサイズは、ルートボリュームと同じかそれ以上である必要があります。

ルートボリュームとデスティネーションボリュームの名前にサフィックス（、 `_m1`など）を付けることを推奨します `_root`。

の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

次の例は、に `cluster_src`ルートボリューム用の負荷共有ミラーボリュームを作成し `svm1_root`ます。

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "レプリケーションジョブスケジュールの作成"です。
3. SVMルートボリュームとLSMのデスティネーションボリュームの間に負荷共有ミラー関係を作成します。

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

次の例は、ルートボリュームと負荷共有ミラーボリューム `svm1_m1`の間に負荷共有ミラー関係を作成し `svm1_root`ます。

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

負荷共有ミラーのtype属性がからに `LS`変わります `DP`。

の詳細については `snapmirror create`、を"ONTAPコマンド リファレンス"参照してください。

4. 負荷共有ミラーを初期化します。

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

次の例は、ルートボリュームの負荷共有ミラーを初期化し `svm1_root`ます。

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

の詳細については `snapmirror initialize`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP負荷共有ミラー関係を更新する

負荷共有ミラー（LSM）関係は、SVM内のボリュームのマウントまたはアンマウント後、およびオプションを指定した処理 `junction-path`中に、SVMルートボリュームの負荷共有ミラー（LSM）関係が自動的に更新され `volume create`ます。スケジュールされた次回の更新前にLSM関係を更新する場合は、LSM関係を手動で更新できます。

負荷共有ミラー関係は、次の状況で自動的に更新されます。

- スケジュールされた更新の時間です
- マウントまたはアンマウント処理がSVMルートボリューム内のボリュームに対して実行される

- あ `volume create`コマンドが発行され、 `junction-path`オプション

  の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. 負荷共有ミラー関係を手動で更新します。

   このコマンドを実行する前に、山かっこ内の変数を必要な値に置き換える必要があります。

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   次の例は、ルートボリュームの負荷共有ミラー関係を更新し `svm1_root`ます。

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

   の詳細については `snapmirror update`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP負荷共有ミラーの昇格

ルートボリュームが完全に使用できなくなった場合は、負荷共有ミラー（LSM）ボリュームを昇格して、ルートボリュームのデータへの書き込みアクセスを提供できます。

開始する前に

このタスクを実行するには、advanced権限レベルのコマンドを使用する必要があります。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. LSMボリュームを昇格します。

   このコマンドを実行する前に、山かっこ内の変数を必要な値に置き換える必要があります。

   ```
   snapmirror promote -destination-path <SVM:volume>
   ```

   次の例は、ボリュームを新しいSVMルートボリュームに昇格し `svm1_m2`ます。

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

と入力し `y`ます。ONTAPはLSMボリュームを読み取り/書き込みボリュームにし、元のルートボリューム（アクセス可能な場合）を削除します。

> 最後の更新が最近行われなかった場合は、昇格されたルートボリュームに元のルートボリュームのデータがすべて含まれているとは限りません。

の詳細については `snapmirror promote`、を"ONTAPコマンド リファレンス"参照してください。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

4. ルートボリュームに使用した命名規則に従って、昇格されたボリュームの名前を変更します。

   このコマンドを実行する前に、山かっこ内の変数を必要な値に置き換える必要があります。

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   次の例は、昇格されたボリュームの名前をに `svm1_root`変更し `svm1_m2`ます。

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. の手順3~4の説明に従って、名前を変更したルートボリュームを保護します"負荷共有ミラー関係の作成と初期化"。

クラウドへのバックアップ

ONTAP SnapMirrorクラウドライセンスをインストールする

SnapMirrorクラウド関係は、認定済みの他社製バックアップアプリケーションを使用してオーケストレーションできます。ONTAP 9 .9.1以降では、System Managerを使用してSnapMirrorのクラウドレプリケーションをオーケストレーションすることもできま

す。System Managerを使用してオンプレミスのONTAPをオブジェクトストレージバックアップにオーケストレーションする場合は、SnapMirrorとSnapMirrorの両方のクラウド容量ライセンスが必要です。また、SnapMirrorクラウドAPIライセンスを要求してインストールする必要があります。

タスクの内容

SnapMirrorクラウドライセンスとSnapMirror S3ライセンスはクラスタライセンスであり、ノードライセンスではないため、ONTAP ONEライセンスバンドルには_not_deliveredが付属しています。これらのライセンスは、個別のONTAP One Compatibilityバンドルに含まれています。SnapMirrorクラウドを有効にする場合は、このバンドルをリクエストする必要があります。

また、System ManagerによるオブジェクトストレージへのSnapMirrorクラウドバックアップのオーケストレーションには、SnapMirrorクラウドAPIキーが必要です。このAPIライセンスはシングルインスタンスのクラスタ全体ライセンスであるため、クラスタ内のすべてのノードにインストールする必要はありません。

手順

ONTAP ONE Compatibility BundleとSnapMirrorクラウドAPIライセンスを要求してダウンロードし、System Managerを使用してインストールする必要があります。

1. ライセンスを付与するクラスタのクラスタUUIDを探して記録します。

   クラスタ用のONTAP One Compatibilityバンドルを注文する要求を送信するには、クラスタUUIDが必要です。

2. NetApp営業チームに連絡して、ONTAP ONE互換性バンドルをリクエストしてください。
3. NetAppサポートサイトの手順に従って、SnapMirrorクラウドAPIライセンスを要求します。

   "SnapMirrorクラウドAPIライセンスキーを要求"

4. ライセンスファイルを受け取ってダウンロードしたら、System Managerを使用してONTAPクラウド互換性NLFとSnapMirrorクラウドAPI NLFをクラスタにアップロードします。
   a. [クラスタ]>[設定]*をクリックします。
   b. ウィンドウで、[ライセンス]*をクリックします。
   c. [ライセンス]*ウィンドウで、をクリックします ＋ Add 。
   d. [* ライセンスの追加 *] ダイアログボックスで、 [* 参照] をクリックしてダウンロードした NLF を選択し、 [* 追加] をクリックしてファイルをクラスタにアップロードします。

関連情報

"SnapMirrorを使用したデータのクラウドへのバックアップ"

"NetAppソフトウェアライセンスの検索"

ONTAP SnapMirrorを使用したデータのクラウドへのバックアップ

ONTAP 9 9.1以降では、System Managerを使用して、クラウドにデータをバックアップしたり、クラウドストレージから別のボリュームにデータをリストアしたりできます。クラウドオブジェクトストアとしては、StorageGRIDまたはONTAP S3を使用できます。

ONTAP 9.16.1以降：

- SnapMirrorクラウドバックアップでは、ファンアウト関係がサポートされます。つまり、2つの異なるオブジェクトストアにSnapMirrorバックアップを同時に作成できます。ONTAP 9.16.1では、SnapMirrorクラウドで2つのファンアウト関係がサポートされます。ファンアウトは、2つのオブジェクトストアへのファンアウトと、2つの異なるオブジェクトストア内の1つまたは2つのバケットへのファンアウトです。3つ以上のファンアウト関係を作成しようとすると失敗します。
- SnapMirror Cloudでは、既存のを使用したより効率的な同期プロセスを使用して、クラウドに移行されたボリュームのバックアップをサポートしてい"ONTAP REST API"ます。この機能では、クラウドに移行されたボリュームから同じデスティネーションオブジェクトストアエンドポイントへのSnapMirrorクラウドバックアップがサポートされます。ベースラインの再処理を実行する必要はありません。FlexVolボリュームとFlexGroupボリュームの両方がサポートされます。

SnapMirrorクラウド機能を使用する前に、NetAppサポートサイトからSnapMirrorクラウドAPIライセンスキーを要求する必要があります"SnapMirrorクラウドAPIライセンスキーを要求"。手順に従って、ビジネス機会の簡単な説明を入力し、提供された電子メールアドレスに電子メールを送信してAPIキーを要求する必要があります。24時間以内に、APIキーの取得方法に関する詳細な説明を記載したEメールが送信されます。

クラウドオブジェクトストアを追加する

SnapMirrorクラウドバックアップを設定する前に、StorageGRIDまたはONTAP S3クラウドオブジェクトストアを追加する必要があります。

手順

1. [保護] 、 [概要] 、 [クラウドオブジェクトストア *] の順にクリックします。
2. をクリックします。 + Add

デフォルトのポリシーを使用したバックアップ

デフォルトのクラウド保護ポリシーであるDailyBackupを使用して、既存のボリュームに対してSnapMirrorクラウドバックアップを簡単に設定できます。

手順

1. [保護] 、 [概要] の順にクリックし、 [クラウドへのボリュームのバックアップ *] を選択します。
2. クラウドへの初めてのバックアップの場合は、図のようにSnapMirrorクラウドAPIライセンスキーをライセンスフィールドに入力します。
3. [* Authenticate and Continue] をクリックします。 *
4. ソースボリュームを選択
5. クラウドオブジェクトストアを選択します。
6. [保存（ Save ）] をクリックします。

カスタムのクラウドバックアップポリシーを作成する

SnapMirrorクラウドバックアップにデフォルトのDailyBackupクラウドポリシーを使用しない場合は、独自のポリシーを作成できます。

手順

1. [保護] 、 [概要] 、 [ローカルポリシーの設定] の順にクリックし、 [保護ポリシー *] を選択します。

2. [* 追加] をクリックし、新しいポリシーの詳細を入力します。
3. ［ * ポリシータイプ * ］ セクションで、 ［ クラウドにバックアップ ］ を選択してクラウドポリシーを作成していることを示します。
4. [保存（ Save ）] をクリックします。

[* Volumes]ページからバックアップを作成します

複数のボリュームのクラウドバックアップを一度に選択して作成する場合や、カスタムの保護ポリシーを使用する場合は、System Manager *[ボリューム]*ページを使用します。

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. クラウドにバックアップするボリュームを選択し、 * Protect * をクリックします。
3. [* Protect Volume] （ボリュームの保護）ウィンドウで、 [* More Options* （その他のオプション）] をクリックします。
4. ポリシーを選択します。

   デフォルトポリシー、DailyBackup、または作成したカスタムクラウドポリシーを選択できます。
5. クラウドオブジェクトストアを選択します。
6. [保存（ Save ）] をクリックします。

クラウドからリストア

System Managerを使用して、クラウドストレージからソースクラスタの別のボリュームにバックアップしたデータをリストアできます。

> ONTAP 9.16.1以降を使用していて、SnapMirrorクラウドの単一ファイルのFlexGroupボリュームへのリストアを実行する場合は、FlexGroupボリューム内の新しいディレクトリにのみファイルをリストアし、デスティネーションFlexGroupボリュームのきめ細かなデータをに設定する必要があります。 `advanced`オプションの設定の詳細 `-granular-data advanced`については、を参照してください"ファイルデータの再分散によるONTAP FlexGroupボリュームのバランス調整"。

手順

1. SnapMirrorとクラウド間関係のソースクラスタで、*[ストレージ]>[ボリューム]*をクリックします。
2. リストアするボリュームを選択します。
3. [クラウドにバックアップ *] タブを選択します。
4. リストアするソースボリュームの横にあるをクリックし ⋮ てメニューを表示し、*[リストア]*を選択します。
5. 「 * Source * 」で Storage VM を選択し、データのリストア先となるボリュームの名前を入力します。
6. [デスティネーション]*で、リストアするSnapshotを選択します。
7. [保存（ Save ）] をクリックします。

SnapMirrorクラウド関係を削除する

System Managerを使用して、クラウド関係を削除できます。

手順

1. [* ストレージ] 、 [ボリューム] の順にクリックし、削除するボリュームを選択します。
2. ソースボリュームの横にあるをクリックし ⋮ 、*[削除]*を選択します。
3. クラウドオブジェクトストアエンドポイントを削除する場合は、 * クラウドオブジェクトストアエンドポイントを削除（オプション） * を選択します。
4. [削除（ Delete ）] をクリックします。

クラウドオブジェクトストアを削除する

クラウドバックアップ関係に含まれていないクラウドオブジェクトストアは、System Managerを使用して削除できます。クラウドバックアップ関係に含まれているクラウドオブジェクトストアは削除できません。

手順

1. [保護] 、 [概要] 、 [クラウドオブジェクトストア *] の順にクリックします。
2. 削除するオブジェクトストアを選択し、をクリック ⋮ して*[削除]*を選択します。

NetApp Backup and Recoveryを使用してデータをバックアップする

ONTAP 9.9.1 以降では、System Manager を使用して、 NetApp Backup and Recovery サービスを使用してクラウドにデータをバックアップできます。

バックアップとリカバリでは、 FlexVol読み取り/書き込みボリュームとデータ保護 (DP) ボリュームがサポートされます。 ONTAP 9.12.1 以降、バックアップとリカバリではFlexGroupボリュームとSnapLockボリュームがサポートされます。

詳細はこちら"NetAppバックアップとリカバリ" 。

開始する前に

NetAppコンソールでアカウントを確立するには、次の手順を実行する必要があります。サービス アカウントには、「Account Admin」というロールを作成する必要があります（他のサービス アカウント ロールには、System Managerから接続を確立するために必要な権限がありません）。

1. "NetAppコンソールでアカウントを作成する" 。
2. "NetAppコンソールでコンソールエージェントを作成する"次のいずれかのクラウド プロバイダーを使用します。
   - Microsoft Azure
   - Amazon Web Services（AWS）
   - Google Cloud Platform（GCP）
   - StorageGRID（ONTAP 9.10.1）

ONTAP 9.10.1 以降では、 NetAppコンソールがオンプレミスで導入されている場合のみ、クラウド バックアップ プロバイダーとしてStorageGRIDを選択できます。コンソール エージェントはオンプレミスにインストールされ、 NetAppコンソール ソフトウェア アズ ア サービス (SaaS) アプリケーションを通じて利用できる必要があります。

3. "NetAppコンソールでNetAppバックアップとリカバリをサブスクライブする"(適切なライセンスが必要です)。
4. "NetAppコンソールを使用してアクセスキーと秘密キーを生成する" 。

NetAppコンソールでクラスタを登録する

コンソールまたはシステム マネージャを使用して、クラスタをNetAppコンソールに登録できます。

手順

1. System Manager で、「保護の概要」に移動します。
2. * NetAppバックアップおよびリカバリ* で、次の詳細を入力します。
   - クライアントID
   - クライアントシークレットキー
3. [Register and Continue] を選択します。

NetAppバックアップとリカバリを有効にする

クラスターがNetAppコンソールに登録されたら、 NetApp Backup and Recovery を有効にして、クラウドへの最初のバックアップを開始する必要があります。

手順

1. System Managerで、**[保護]>[概要]***を選択し、[Cloud Backup Service]*セクションまでスクロールします。
2. クライアント ID * と * クライアントシークレット * を入力します。

ONTAP 9.10.1以降では、*[クラウド使用コストの詳細を確認する]*を選択して、クラウド使用コストを確認できます。

3. [接続してCloud Backup Serviceを有効にする]*を選択します。
4. * NetAppバックアップとリカバリの有効化* ページで、選択したプロバイダーに応じて次の詳細を入力します。

クラウドプロバイダ	入力するデータ
Azure	• AzureサブスクリプションID • 地域 • リソースグループ名（既存または新規）

AWS	• AWSアカウントID • アクセスキー • シークレットキー • 地域
Google Cloud プロジェクト（ GCP ）	• Google Cloudプロジェクト名 • Google Cloud Accessキー • Google Cloudシークレットキー • 地域
StorageGRID (ONTAP 9.10.1 以降、 NetAppコンソールのオンプレミス展開のみ)	• サーバ • SGアクセスキー • SGシークレットキー

5. 保護ポリシー * を選択：
   - * 既存のポリシー * ：既存のポリシーを選択します。
   - * 新しいポリシー * ：名前を指定し、転送スケジュールを設定します。

     ONTAP 9 10.1以降では、AzureとAWSのどちらでアーカイブを有効にするかを指定できます。

     AzureまたはAWSでボリュームのアーカイブを有効にした場合、アーカイブを無効にすることはできません。

     AzureまたはAWSのアーカイブを有効にする場合は、次の項目を指定します。

     - ボリュームがアーカイブされるまでの日数。
     - アーカイブに保持するバックアップの数。最新のバックアップまでアーカイブする場合は、「0」（ゼロ）を指定します。
     - AWSの場合は、アーカイブストレージクラスを選択します。
6. バックアップするボリュームを選択します。
7. [保存（ Save ）] を選択します。

NetAppバックアップおよびリカバリに使用される保護ポリシーを編集します

NetApp Backup and Recovery で使用される保護ポリシーを変更できます。

手順

1. System Managerで、**[保護]>[概要]***を選択し、[Cloud Backup Service]*セクションまでスクロールします。
2. を選択し、*[編集]*を選択します。

3. 保護ポリシー * を選択：
   - * 既存のポリシー * ：既存のポリシーを選択します。
   - * 新しいポリシー * ：名前を指定し、転送スケジュールを設定します。

     ONTAP 9 10.1以降では、AzureとAWSのどちらでアーカイブを有効にするかを指定できます。

     AzureまたはAWSでボリュームのアーカイブを有効にした場合、アーカイブを無効にすることはできません。

     AzureまたはAWSのアーカイブを有効にする場合は、次の項目を指定します。

     - ボリュームがアーカイブされるまでの日数。
     - アーカイブに保持するバックアップの数。最新のバックアップまでアーカイブする場合は、「0」（ゼロ）を指定します。
     - AWSの場合は、アーカイブストレージクラスを選択します。
4. [保存（ Save ）] を選択します。

クラウド上の新しいボリュームや**LUN**を保護

新しいボリュームまたはLUNを作成するときに、ボリュームまたはLUNのクラウドへのバックアップを可能にするSnapMirror保護関係を確立できます。

開始する前に

- SnapMirrorライセンスが必要です。
- クラスタ間LIFを設定する必要があります。
- NTPを設定する必要があります。
- クラスタでONTAP 9.9.1以降が実行されている必要があります。

タスクの内容

次のクラスタ構成では、クラウド上の新しいボリュームまたはLUNを保護できません。

- クラスタをMetroCluster環境に含めることはできません。
- SVM-DRはサポートされません。
- FlexGroupボリュームは、 NetApp Backup and Recovery を使用してバックアップできません。

手順

1. ボリュームまたは LUN をプロビジョニングするときは、 System Manager の * Protection * ページで、 * SnapMirror を有効にする（ローカルまたはリモート） * チェックボックスを選択します。
2. バックアップとリカバリのポリシー タイプを選択します。
3. バックアップとリカバリが有効になっていない場合は、* NetAppバックアップとリカバリを使用してバックアップを有効にする*を選択します。

クラウド上の既存のボリュームまたは**LUN**を保護

既存のボリュームとLUNのSnapMirror保護関係を確立できます。

手順

1. 既存のボリュームまたはLUNを選択し、*[保護]*を選択します。
2. ボリュームの保護*ページで、保護ポリシーに NetApp Backup and Recoveryを使用したバックアップ*を指定します。
3. [保護]*を選択します。
4. [* 保護] ページで、 [SnapMirror を有効にする (ローカルまたはリモート)*] チェックボックスをオンにします。
5. * NetApp Backup and Recovery に接続して有効にする*を選択します。

バックアップファイルからのデータのリストア

データの復元、関係の更新、関係の削除などのバックアップ管理操作は、 NetAppコンソールを使用する場合にのみ実行できます。参照"バックアップファイルからのデータのリストア"詳細についてはこちらをご覧ください。

SnapLockテクノロジを使用したアーカイブとコンプライアンス

ONTAP SnapLockについて学ぶ

SnapLockは、規制やガバナンスに準拠するためにWORMストレージを使用して変更不可能な状態でファイルを保管する組織向けの、ハイパフォーマンスなコンプライアンスソリューションです。

SnapLockは、SEC 17a-4（f）、HIPAA、FINRA、CFTC、GDPRなどの規制に準拠するために、データの削除、変更、名前変更を防止するのに役立ちます。SnapLockを使用すると、指定した保持期間または無期限のいずれかで、ファイルを消去および書き込み不可の状態で保存およびコミットできる専用ボリュームを作成できます。SnapLockでは、CIFSやNFSなどの標準オープンファイルプロトコルを使用して、ファイルレベルでこの保持を実行できます。SnapLockでサポートされるオープンファイルプロトコルは、NFS（バージョン2、3、4）とCIFS（SMB 1.0、2.0、3.0）です。

SnapLockを使用すると、ファイルやSnapshotをWORMストレージにコミットし、WORMで保護されたデータの保持期間を設定できます。SnapLock WORMストレージでは、NetApp Snapshotテクノロジを使用し、SnapMirrorレプリケーションとSnapVaultバックアップをベーステクノロジとして活用して、データのバックアップリカバリ保護を実現できます。WORMストレージの詳細については、を参照してください"NetApp SnapLock - TR-4526を使用して準拠したWORMストレージを実現します"。

ファイルをWORM状態にコミットするには、アプリケーションを使用してNFSまたはCIFS経由でコミットできます。ファイルをWORM状態に自動的にコミットするには、SnapLockの自動コミット機能を使用します。追記可能 WORM ファイル _ を使用すると、ログ情報のように段階的に書き込まれるデータを保持できます。詳細については、を参照してください "ボリュームアペンドモードを使用して追記可能WORMファイルを作成する"。

SnapLockは、ほとんどのコンプライアンス要件を満たすデータ保護方法をサポートしています。

- SnapLock for SnapVaultを使用すると、セカンダリストレージ上のSnapshotをWORM方式で保護できます。を参照して "SnapshotをWORM状態にコミット"
- SnapMirrorを使用すると、ディザスタリカバリ用に地理的に離れた別の場所にWORMファイルをレプリケートできます。を参照して "WORMファイルのミラーリング"

SnapLockは、NetApp ONTAPのライセンスベースの機能です。1つのライセンスで、SnapLockを厳格なコンプライアンスモードで使用してSECルール17a-4（f）などの外部の要件を満たし、より緩やかなエンタープライズモードで使用して、デジタル資産の保護に関する社内で義務付けられている規制を満たすことができます。SnapLockライセンスはソフトウェアスイートの一部"ONTAP One"です。

SnapLockは、すべてのAFFシステムとFASシステム、およびONTAP Selectでサポートされています。SnapLockは、ソフトウェアのみのソリューションではなく、ハードウェアとソフトウェアが統合されたソリューションです。SEC 17a-4（f）など、ハードウェアとソフトウェアの統合ソリューションを必要とする厳しいWORM規制には、この区別が重要です。詳細については、を参照してください "ブローカーへのSECガイダンス-電子記憶媒体の使用に関するディーラー"。

SnapLockの機能

SnapLockを設定したら、次のタスクを実行できます。

- "ファイルをWORM状態にコミット"
- "セカンダリストレージのSnapshotをWORM状態にコミット"
- "ディザスタリカバリ用にWORMファイルをミラーリング"
- "訴訟時にリーガルホールドを使用してWORMファイルを保持"
- "privileged delete機能を使用したWORMファイルの削除"
- "ファイルの保持期間を設定する"
- "SnapLockボリュームを移動する"
- "Snapshotをロックしてランサムウェア攻撃から保護"
- "監査ログを使用したSnapLockの使用状況の確認"
- "SnapLock APIの使用"

SnapLock Complianceモードとエンタープライズモード

SnapLock ComplianceモードとEnterpriseモードでは、主に各モードでWORMファイルが保護されるレベルが異なります。

SnapLock モード	保護レベル	保持中のWORMファイル削除
Complianceモード	ディスクレベル	削除できません
Enterpriseモード	ファイルレベル	コンプライアンス管理者が監査済みの「特権削除」手順を使用して削除できる

保持期間の経過後、不要になったファイルはユーザが削除する必要があります。一度WORM状態にコミットされたファイルは、ComplianceモードかEnterpriseモードかに関係なく、保持期間が過ぎたあとも変更するこ

とはできません。

保持期間中または保持期間後にWORMファイルを移動することはできません。WORMファイルはコピーできますが、コピーしたファイルのWORM特性は保持されません。

次の表に、SnapLock ComplianceモードとEnterpriseモードでサポートされる機能の違いを示します。

機能	SnapLock Compliance	SnapLock Enterprise
privileged deleteを使用したファイルの有効化と削除	いいえ	○
ディスクの再初期化	いいえ	○
保持期間中のSnapLockアグリゲートおよびボリュームの削除	いいえ	○（SnapLock監査ログボリュームを除く）
アグリゲートまたはボリュームの名前変更	いいえ	○
NetApp以外のディスクを使用する	いいえ	いいえ
監査ログにSnapLockボリュームを使用する	○	はい（ONTAP 9 .5以降）

SnapLockでサポートされる機能とサポートされない機能

次の表に、SnapLock Complianceモード、SnapLock Enterpriseモード、またはその両方でサポートされる機能を示します。

機能	SnapLock Complianceでサポートされます	SnapLock Enterpriseでサポートされます
整合性グループ	いいえ	いいえ
暗号化されたボリューム	はい、詳細をご覧ください暗号化とSnapLock 。	はい、詳細をご覧ください暗号化とSnapLock 。
SnapLockアグリゲートでのFabricPoolの使用	いいえ	はい、ONTAP 9から始まります。8.詳細については、をご覧ください SnapLock Enterpriseアグリゲート上のFabricPool。
Flash Poolアグリゲート	はい。	はい。

FlexClone	SnapLockボリュームはクローニングできますが、SnapLockボリューム上のファイルはクローニングできません。	SnapLockボリュームはクローニングできますが、SnapLockボリューム上のファイルはクローニングできません。
FlexGroupホリユウム	はい、ONTAP 9 .11.1以降。詳細については、をご覧ください [flexgroup]。	はい、ONTAP 9 .11.1以降。詳細については、をご覧ください [flexgroup]。
LUN	いいえ。SnapLockの詳細については、こちらをご覧くださいLUNのサポート。	いいえ。SnapLockの詳細については、こちらをご覧くださいLUNのサポート。
MetroClusterコウセイ	はい、ONTAP 9から始まります。3.詳細については、をご覧ください MetroClusterのサポートMetroClusterのサポート。	はい、ONTAP 9から始まります。3.詳細については、をご覧ください MetroClusterのサポートMetroClusterのサポート。
マルチ管理者認証（MAV）	はい。ONTAP 9 13.1以降。詳細については、をご覧ください MAVサポート。	はい。ONTAP 9 13.1以降。詳細については、をご覧ください MAVサポート。
SAN	いいえ	いいえ
シングルファイルSnapRestore	いいえ	○
SnapMirrorアクティブ同期	いいえ	いいえ
SnapRestore	いいえ	○
SMTape	いいえ	いいえ
SnapMirror Synchronous	いいえ	いいえ
SSD	はい。	はい。
Storage Efficiency機能	○（ONTAP 9 .9.1以降）詳細については、をご覧ください Storage Efficiencyのサポート。	○（ONTAP 9 .9.1以降）詳細については、をご覧ください Storage Efficiencyのサポート。

SnapLock Enterpriseアグリゲート上の**FabricPool**

FabricPoolは、ONTAP 9以降のSnapLock Enterpriseアグリゲートでサポートされます。8.ただし、アカウントチームは、パブリッククラウドまたはプライベートクラウドに階層化されたFabricPoolデータは、クラウド管理者が削除できるためSnapLockで保護されなくなったことを理解していることを記載した製品差異申請を行う必要があります。

FabricPoolがパブリッククラウドまたはプライベートクラウドに階層化するデータは、クラウド管理者が削除できるため、SnapLockで保護されなくなります。

FlexGroupボリュウム

SnapLockでは、ONTAP 9 .11.1以降でFlexGroupボリュームがサポートされますが、次の機能はサポートされません。

- リーガルホールド
- イベントベースの保持
- SnapLock for SnapVault（ONTAP 9 12.1以降でサポート）

また、次の動作にも注意してください。

- FlexGroupボリュームのボリュームコンプライアンスクロック（VCC）は、ルートコンスティチュエントのVCCによって決まります。ルート以外のすべてのコンスティチュエントのVCCは、ルートVCCと密接に同期されます。
- SnapLock構成プロパティは、FlexGroup全体に対してのみ設定されます。個 々 のコンスティチュエントに、デフォルトの保持期間や自動コミット期間など、異なる設定プロパティを設定することはできません。

LUNのサポート

SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、Snapshotの改ざんはSnapMirrorソースボリュームとLUNを含むデスティネーションボリュームの両方でサポートされます。

MetroClusterのサポート

MetroCluster構成でのSnapLockのサポートは、SnapLock ComplianceモードとSnapLock Enterpriseモードで異なります。

SnapLock Compliance

- ONTAP 9 .3以降では、ミラーされていないMetroClusterアグリゲートでSnapLock Complianceがサポートされます。
- ONTAP 9 .3以降では、ミラーされたアグリゲートでSnapLock Complianceがサポートされますが、アグリゲートを使用してSnapLock監査ログボリュームをホストする場合にのみサポートされます。
- SVM固有のSnapLock設定は、MetroClusterを使用してプライマリサイトとセカンダリサイトにレプリケートできます。

SnapLock Enterprise

- SnapLock Enterpriseアグリゲートがサポートされています。
- ONTAP 9 .3以降では、privileged deleteを使用するSnapLock Enterpriseアグリゲートがサポートされます。
- SVM固有のSnapLock設定は、MetroClusterを使用して両方のサイトにレプリケートできます。

MetroCluster構成とコンプライアンスクロック

MetroCluster構成では、Volume Compliance Clock（VCC；ボリュームコンプライアンスクロック）とSystem Compliance Clock（SCC；システムコンプライアンスクロック）の2つのコンプライアンスクロックメカニズムを使用します。VCCおよびSCCは、すべてのSnapLock構成で使用できます。ノードに新しいボリュームを作成すると、そのVCCはそのノードの現在のSCCの値で初期化されます。ボリュームの作成後は、ボリュームとファイルの保持期限が常にVCCで追跡されます。

ボリュームを別のサイトにレプリケートすると、そのVCCもレプリケートされます。たとえば、サイトAからサイトBへのボリュームのスイッチオーバーが発生した場合、VCCの更新はサイトBで継続され、サイトAのSCCはサイトAがオフラインになると停止します。

サイトAがオンラインに戻ってボリュームのスイッチバックが実行されると、サイトAのSCCクロックが再開されますが、ボリュームのVCCは引き続き更新されます。VCCは継続的に更新されるため、スイッチオーバーやスイッチバックの処理に関係なく、ファイルの保持期間はSCCのクロックに依存せず、長くなりません。

Multi-Admin Verification（MAV）のサポート

ONTAP 9 .13.1以降では、クラスタ管理者が明示的にマルチ管理者検証を有効にして、一部のSnapLock処理を実行する前にクォーラムの承認が必要になるようにすることができます。MAVが有効な場合は、default-retention-time、minimum-retention-time、maximum-retention-time、volume-append-mode、自動コミット期間、privileged-deleteなどのSnapLockボリュームプロパティでクォーラムの承認が必要になります。詳細については、をご覧ください "MAV"。

Storage Efficiency

ONTAP 9 .9.1以降では、SnapLockでSnapLockおよびアグリゲートのデータコンパクション、ボリューム間重複排除、適応圧縮などのStorage Efficiency機能がサポートされます。Storage Efficiencyの詳細については、を参照してください"ONTAPのStorage Efficiencyの概要"。

暗号化

ONTAPは、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないように、ソフトウェアベースとハードウェアベースの暗号化テクノロジを提供します。

- 免責事項： * 認証キーが紛失した場合や、認証に失敗した回数が指定した制限を超えたためにドライブが永続的にロックされた場合、自己暗号化ドライブまたはボリューム上の SnapLock で保護された WORM ファイルを取得できるかどうかは、ネットアップでは保証できません。認証エラーが発生しないようにする責任はユーザにあります。

暗号化されたボリュームはSnapLockアグリゲートでサポートされます。

7-Modeからの移行

7-Mode Transition ToolのCopy-Based Transition（CBT）機能を使用して、SnapLockボリュームを7-ModeからONTAPにマイグレートできます。デスティネーションボリュームのSnapLockモード（ComplianceまたはEnterprise）がソースボリュームのSnapLockモードと一致している必要があります。コピーフリーの移行（CFT）を使用してSnapLockボリュームを移行することはできません。

SnapLockの設定

ONTAP SnapLockの設定について学ぶ

SnapLockを使用する前に、SnapLockを設定する必要があります。たとえば、"SnapLockライセンスをインストールする"SnapLockボリュームを含むアグリゲートをホストするノードごとに、を初期化し"コンプライアンスクロック"、ONTAP 9 10.1より前のリリースのONTAPを実行するクラスタ用にSnapLockアグリゲートを作成します。"SnapLockボリュームの作成とマウント"

ONTAPコンプライアンスクロックを初期化する

SnapLockでは、_volumeコンプライアンスクロック_を使用して、改ざんによるWORMファイルの保持期間の変更を防止します。最初に、SnapLockアグリゲートをホストする各ノードで_system ComplianceClock_を初期化する必要があります。

ONTAP 9.14.1以降では、SnapLockボリュームがない場合やSnapshotロックが有効になっているボリュームがない場合に、システムコンプライアンスクロックを初期化または再初期化できます。再初期化機能を使用すると、システム管理者は、システムコンプライアンスクロックが誤って初期化されたり、システムのクロックドリフトが修正されたりした場合に、システムコンプライアンスクロックをリセットできます。ONTAP 9.13.1以前のリリースでは、一度ノードでコンプライアンスクロックを初期化すると、再度初期化することはできません。

開始する前に

コンプライアンスクロックを再初期化する手順は、次のとおりです。

- クラスタ内のすべてのノードが正常な状態である必要があります。
- すべてのボリュームがオンラインである必要があります。
- どのボリュームもリカバリキューに含めることができません。
- SnapLockボリュームが存在できません。
- Snapshotロックが有効になっているボリュームが存在できません。

コンプライアンスクロックを初期化するための一般的な要件：

- このタスクを実行するには、クラスタ管理者である必要があります。
- "ノードにSnapLockライセンスがインストールされている必要があります。"です。

タスクの内容

システムのコンプライアンスクロックの時間は_volumeコンプライアンスクロック_に継承され、ボリューム上のWORMファイルの保持期間はボリューム側で制御されます。ボリュームコンプライアンスクロックは、新しいSnapLockを作成すると自動的に初期化されます。

> システムコンプライアンスクロックの初期設定は、現在のハードウェアシステムクロックに基づいています。そのため、各ノードでシステムコンプライアンスクロックを初期化する前に、システム時間とタイムゾーンが正しいことを確認する必要があります。ノードでシステムコンプライアンスクロックを初期化すると、ロックが有効なSnapLockボリュームまたはボリュームが存在する場合、再度初期化することはできません。

手順

ONTAP CLIを使用してコンプライアンスクロックを初期化できます。ONTAP 9 12.1以降では、System Managerを使用してコンプライアンスクロックを初期化できます。

System Manager

1. [Cluster]>[Overview]に移動します。
2. [ノード]セクションで、[Initialize SnapLock Compliance Clock*]をクリックします。
3. コンプライアンスクロック*列を表示してコンプライアンスクロックが初期化されたことを確認するには、**[クラスタ]>[概要]>[ノード]***セクションで[表示/非表示]をクリックし、[SnapLockコンプライアンスクロック]*を選択します。

CLI

1. システムコンプライアンスクロックを初期化します。

   `snaplock compliance-clock initialize -node node_name`

   次のコマンドは、のシステムコンプライアンスクロックを初期化し `node1`ます。

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

   の詳細については `snaplock compliance-clock initialize`、を"ONTAPコマンド リファレンス"参照してください。

2. プロンプトが表示されたら、システムクロックが正しいこと、およびコンプライアンスクロックを初期化することを確認します。

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. SnapLockアグリゲートをホストするノードごとに、この手順を繰り返します。

NTPが設定されたシステムでコンプライアンスクロックの再同期を有効にする

NTP サーバーが構成されている場合、 SnapLock Complianceクロック同期機能を有効にすることができます。

開始する前に

- この機能は、advanced権限レベルでのみ使用できます。

- このタスクを実行するには、クラスタ管理者である必要があります。
- "ノードにSnapLockライセンスがインストールされている必要があります。"です。
- この機能は、Cloud Volumes ONTAP、ONTAP Select、vsimの各プラットフォームでのみ使用できます。

タスクの内容

SnapLockセキュアクロックデーモンがしきい値を超えたスキューを検出すると、ONTAPはシステム時間を使用してシステムクロックとボリュームコンプライアンスクロックの両方をリセットします。スキューしきい値として24時間の期間が設定されています。つまり、スキューが1日以上経過した場合にのみ、システムコンプライアンスクロックがシステムクロックに同期されます。

SnapLockセキュアクロックデーモンはスキューを検出し、コンプライアンスクロックをシステム時間に変更します。コンプライアンスクロックはシステム時間がNTP時間と同期されている場合にのみシステム時間と同期されるため、コンプライアンスクロックを強制的にシステム時間に変更しようとすると失敗します。

手順

1. NTP サーバーが構成されている場合は、 SnapLock Complianceクロック同期機能を有効にします。

   `snaplock compliance-clock ntp`

   次のコマンドは、システムのコンプライアンス クロック同期機能を有効にします。

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

   の詳細については `snaplock compliance-clock ntp modify`、を"ONTAPコマンド リファレンス"参照してください。

2. プロンプトが表示されたら、設定したNTPサーバが信頼できること、および通信チャネルがセキュアであることを確認して機能を有効にします。
3. 機能が有効になっていることを確認します。

   `snaplock compliance-clock ntp show`

   次のコマンドは、システムのコンプライアンス クロック同期機能が有効になっているかどうかを確認します。

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

   の詳細については `snaplock compliance-clock ntp show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapLockアグリゲートを作成する

volumeオプションを使用 `-snaplock-type`して、ComplianceまたはEnterprise SnapLockボリュームのタイプを指定します。ONTAP 9 .10.1より前のリリースでは、独立し

たSnapLockアグリゲートを作成する必要があります。ONTAP 9 .10.1以降では、SnapLockボリュームとSnapLock以外のボリュームを同じアグリゲート上に配置できます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はありません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- "ライセンスをインストールする必要があります"ノードのSnapLock。このライセンスはに含まれてい"ONTAP One"ます。
- "ノードのコンプライアンスクロックを初期化する必要があります"です。
- ディスクを「 root 」、「 data1 」、および「 `d ata2` 」としてパーティショニングした場合、スペアディスクが利用可能であることを確認する必要があります。

アップグレード時の考慮事項

ONTAP 9 .10.1にアップグレードすると、既存のSnapLockアグリゲートとSnapLock以外のアグリゲートは、SnapLockボリュームとSnapLock以外のボリュームの両方をサポートするようにアップグレードされますが、既存のSnapLockボリュームの属性は自動的には更新されません。たとえば、data-compaction、cross-volume-dedupe、cross-volume-background-dedupeの各フィールドは変更されません。既存のアグリゲートに作成される新しいSnapLockボリュームのデフォルト値は、SnapLock以外のボリュームと同じです。また、新しいボリュームおよびアグリゲートのデフォルト値はプラットフォームによって異なります。

リバートに関する考慮事項

ONTAP 9.10.1より前のバージョンにリバートする必要がある場合は、SnapLock Compliance、SnapLock Enterprise、およびSnapLockのすべてのボリュームをそれぞれ専用のSnapLockアグリゲートに移動する必要があります。

タスクの内容

- SyncMirrorオプションを使用してComplianceアグリゲートを作成することはできません。
- ミラーされたComplianceアグリゲートをMetroCluster構成で作成できるのは、そのアグリゲートをSnapLock監査ログボリュームのホストとして使用する場合だけです。

> MetroCluster構成では、SnapLock Enterpriseはミラーされたアグリゲートとミラーされていないアグリゲートでサポートされます。SnapLock Complianceは、ミラーされていないアグリゲートでのみサポートされます。

手順

1. SnapLockアグリゲートを作成します。

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

次のコマンドでは、3本のディスクを含む `node1`という名前のSnapLockアグリゲートが `aggr1`作成され`Compliance`ます。

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

の詳細については `storage aggregate create`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SnapLockボリュームの作成とマウント

WORM状態にコミットするファイルまたはSnapshot用にSnapLockボリュームを作成する必要があります。ONTAP 9.10.1以降では、アグリゲートタイプに関係なく、作成するすべてのボリュームがデフォルトでSnapLock以外のボリュームとして作成されます。SnapLockタイプとしてComplianceまたはEnterpriseを指定してSnapLockボリュームを明示的に作成するには、オプションを使用する必要があります `-snaplock-type`。デフォルトでは、SnapLockタイプはに設定されてい `non-snaplock`ます。

開始する前に

- SnapLockアグリゲートがオンラインになっている必要があります。
- そうするべきだ"SnapLockライセンスがインストールされていることの確認"ノードにSnapLockライセンスがインストールされていない場合は"インストール"、ライセンスが必要です。このライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneよりも前のリリースでは、SnapLockライセンスはSecurity and Compliance Bundleに含まれていました。Security and Compliance Bundleの提供は終了しましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は選択できます"ONTAP Oneへのアップグレード"。
- "ノードのコンプライアンスクロックを初期化する必要があります"です。

タスクの内容

適切なSnapLock権限があれば、エンタープライズボリュームの削除や名前変更はいつでも実行できます。Complianceボリュームは保持期間が経過するまで削除できません。Complianceボリュームの名前は変更できません。

SnapLockボリュームはクローニングできますが、SnapLockボリューム上のファイルはクローニングできません。クローンボリュームのSnapLockタイプは親ボリュームと同じになります。

SnapLockボリュームではLUNはサポートされません。SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、Snapshotの改ざんはSnapMirrorソースボリュームとLUNを含むデスティネーションボリュームの両方でサポートされます。

このタスクは、ONTAPシステムマネージャまたはONTAP CLIを使用して実行します。

System Manager

ONTAP 9 12.1以降では、System Managerを使用してSnapLockボリュームを作成できます。

手順

1. [*Storage]>[Volumes]に移動し、[*Add]をクリックします。
2. [ボリュームの追加*]ウィンドウで、[その他のオプション]をクリックします。
3. ボリュームの名前とサイズなど、新しいボリューム情報を入力します。
4. 「* SnapLock を有効にする*」を選択し、SnapLock タイプとして「Compliance」または「Enterprise」を選択します。
5. [ファイルの自動コミット*]セクションで、[変更済み]を選択し、ファイルが自動的にコミットされるまでに変更されないようにする時間を入力します。最小値は5分、最大値は10年です。
6. [*データ保持期間]セクションで、最小保持期間と最大保持期間を選択します。
7. デフォルトの保持期間を選択します。
8. [保存（ Save ）] をクリックします。
9. [* Volumes]ページで新しいボリュームを選択し、SnapLock 設定を確認します。

CLI

1. SnapLockボリュームを作成します。

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。SnapLockボリュームには、、 `-atime-update` `-is-autobalance-eligible`、、 `-space-mgmt-try-first`およびは `vmalign`使用できません `-nvfail`。

次のコマンドは、 `aggr1`on `vs1`という名前のSnapLockボリュームを `vol1`作成し `Compliance`ます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

SnapLockボリュームのマウント

NASクライアントからアクセスできるように、SnapLockボリュームをSVMネームスペースのジャンクションパスにマウントできます。

開始する前に

SnapLockボリュームはオンラインである必要があります。

タスクの内容

- SnapLockボリュームはSVMのルートにのみマウントできます。
- 通常のボリュームをSnapLockボリュームの下にマウントすることはできません。

手順

1. SnapLockボリュームをマウントします。

   `volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*`

   の詳細については `volume mount`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、という名前のSnapLockをネームスペースの `vs1`ジャンクションパスに `/sales`マウントし `vol1`ます。

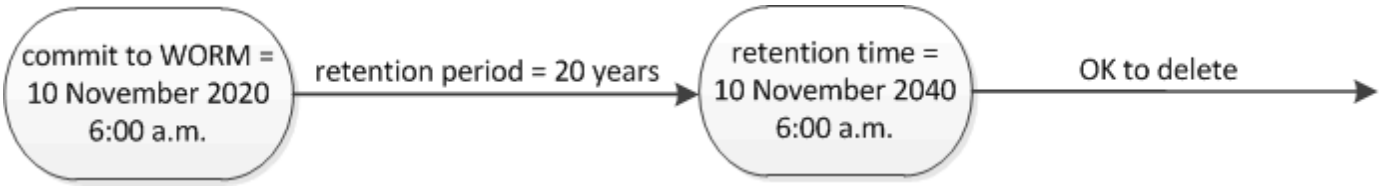
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

ONTAP SnapLockの保持期間を設定する

保持期限の設定については、ファイルに対して明示的に設定する方法と、ボリュームのデフォルトの保持期間から自動的に設定する方法があります。保持期限を明示的に設定しないかぎり、SnapLockではデフォルトの保持期間を使用して保持期限が計算されます。イベント発生後にファイルの保持期間を設定することもできます。

ホシキカントホシキケンニツイテ

WORM ファイルの *retention period* は、 WORM 状態にコミットされたファイルを保持する必要がある期間を指定します。WORM ファイルの _ retention time_ は、その時点までファイルを保持する必要がなくなった時間です。たとえば、2020年11月10日の午前6時にWORM状態にコミットされたファイルの保持期間を20年とすると、保持期限は2040年11月10日の午前6時になります。



ONTAP 9 .10.1以降では、保持期限を3058年10月26日まで、保持期間を100年まで設定できます。保持期限を延長すると、古いポリシーが自動的に変換されます。ONTAP 9 .9.1以前のリリースでは、デフォルトの保持期間をinfiniteに設定しないかぎり、サポートされる最大保持期間は2071年1月19日（GMT）です。

レプリケーションに関する重要な考慮事項

2071年1月19日（GMT）よりもあとの保持期限を使用してSnapLockソースボリュームとのSnapMirror関係を確立する場合は、デスティネーションクラスタでONTAP 9 .10.1以降が実行されている必要があります。SnapMirror転送が失敗します。

リバートに関する重要な考慮事項

ONTAP、保持期間が「2071 年 1 月 19 日午前 8 時 44 分 7 秒」以降のファイルがある場合、クラスターをONTAP 9.10.1 から以前のONTAPバージョンに戻すことはできません。

保持期間について

SnapLock ComplianceまたはEnterpriseボリュームには、次の4つの保持期間があります。

- 最小保持期間(`min`）（デフォルトは0）
- 最大保持期間(`max`）（デフォルトは30年）
- デフォルトの保持期間。ONTAP 9 10.1以降では、コンプライアンスモードとエンタープライズモードの両方でデフォルトがとなります。 `min`ONTAP 9 10.1より前のONTAPリリースでは、デフォルトの保持期間はモードによって異なります。
  - コンプライアンスモードの場合、デフォルトはと同じです `max`。
  - エンタープライズモードの場合、デフォルトはと同じです `min`。
- 未指定の保持期間。

  ONTAP 9 .8以降では、ボリューム内のファイルの保持期間をに設定して、絶対的な保持期限を設定するまでファイルが保持されるようにすることができ `unspecified`ます。絶対保持期間が設定されたファイルの保持期間を未指定に設定し、再度絶対保持期間に設定することができます。ただし、新しい保持期間が以前に設定した絶対保持期間よりもあとである必要があります。

  ONTAP 9 12.1以降では、保持期間がに設定されたWORMファイルの `unspecified`保持期間は、SnapLockボリュームに設定された最小保持期間に設定されます。ファイルの保持期間をから絶対的な保持期間に変更する場合 `unspecified`は、ファイルにすでに設定されている最小保持期間よりも長い新しい保持期間を指定する必要があります。

そのため、ComplianceモードのファイルをWORM状態にコミットする前に保持期限を明示的に設定していない場合、デフォルトを変更しないとファイルが30年間保持されます。同様に、EnterpriseモードのファイルをWORM状態にコミットする前に保持期限を明示的に設定していない場合、デフォルトを変更しないとファイルの保持期間は0年になります。つまり、ファイルは保持されなくなります。

デフォルトの保持期間を設定する

コマンドを使用して、SnapLockボリューム上のファイルにデフォルトの保持期間を設定できます `volume snaplock modify`。

開始する前に

SnapLockボリュームはオンラインである必要があります。

タスクの内容

次の表に、デフォルトの保持期間に指定できる値を示します。

デフォルトの保持期間は、最小保持期間以上、最大保持期間以下にする必要があります。

値	単位	脚注
0 ~ 65535	秒	
0 ~ 24	時間	

値	単位	脚注
0 ~ 365	日	
0 ~ 12	月	
0 ~ 100	年	ONTAP 9 .10.1以降。以前のONTAPリリースでは、値は0~70です。
最大	-	最大保持期間を使用します。
最小	-	最小保持期間を使用します。
インフィニット	-	ファイルを無期限に保持します。
未指定	-	絶対的な保持期間が設定されるまでファイルを保持します。

最大保持期間と最小保持期間の値と範囲は同じですが、と `min`は `max`該当しません。このタスクの詳細については、を参照してください"保持期間の概要の設定"。

コマンドを使用して、ボリュームの保持期間の設定を表示できます `volume snaplock show`。の詳細については `volume snaplock show`、を"ONTAPコマンド リファレンス"参照してください。

ファイルがWORM状態にコミットされたあとは、保持期間を延長することはできますが短縮することはできません。

手順

1. SnapLockボリューム上のファイルにデフォルトの保持期間を設定します。

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -default -retention-period *default_retention_period* -minimum-retention-period *min_retention_period* -maximum-retention-period *max_retention_period*

   の詳細については `volume snaplock modify`、を"ONTAPコマンド リファレンス"参照してください。

   次の例は、最小保持期間と最大保持期間が以前に変更されていないことを前提としています。

   次のコマンドは、ComplianceボリュームまたはEnterpriseボリュームのデフォルトの保持期間を20日に設定します。

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

次のコマンドは、Complianceボリュームのデフォルトの保持期間を70年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

次のコマンドは、Enterpriseボリュームのデフォルトの保持期間を10年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

次のコマンドは、Enterpriseボリュームのデフォルトの保持期間を10日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

次のコマンドは、Complianceボリュームのデフォルトの保持期間を無期限に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

ファイルの保持期限を明示的に設定する

ファイルに対して保持期限を明示的に設定するには、最終アクセス時刻を変更します。最終アクセス日時は、NFSまたはCIFS経由で適切なコマンドやプログラムを使用して変更できます。

タスクの内容

ファイルがWORM状態にコミットされたあとは、保持期限を延長することはできますが短縮することはできません。保持期限は、ファイルのフィールドに保存され `atime`ます。

ファイルの保持期限をに明示的に設定することはできません `infinite`。この値は、デフォルトの保持期間を使用して保持期間を計算する場合にのみ使用できます。

手順

1. 適切なコマンドまたはプログラムを使用して、保持期限を設定するファイルの最終アクセス日時を変更します。

   UNIXシェルで、次のコマンドを使用して、という名前のファイルの保持期限を2020年11月21日午前6時に設定し `document.txt`ます。

   ```
   touch -a -t 202011210600 document.txt
   ```

Windowsでは、任意の適切なコマンドまたはプログラムを使用して最終アクセス時間を変更できます。

イベント発生後のファイル保持期間の設定

ONTAP 9.3以降では、SnapLock のイベントベースの保持（EBR）機能を使用して、イベントの発生後にファイルを保持する期間を定義できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

  "SnapLock管理者アカウントの作成"

- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

タスクの内容

イベント保持ポリシー _ は、イベント発生後のファイルの保持期間を定義します。このポリシーは、単一のファイルに適用することも、ディレクトリ内のすべてのファイルに適用することもできます。

- WORMファイルでないファイルは、ポリシーで定義された保持期間にわたってWORM状態にコミットされます。
- WORMファイルまたは追記可能WORMファイルの場合、保持期間がポリシーで定義された保持期間まで延長されます。

ComplianceモードまたはEnterpriseモードのボリュームを使用できます。

EBRポリシーは、リーガルホールドの対象となるファイルには適用できません。

高度な使用方法については、を参照してください"NetApp SnapLock を使用して WORM ストレージに準拠"。

EBR を使用して既存の **WORM** ファイルの保持期間を延長する _
EBRは、既存のWORMファイルの保持期間を延長する場合に便利です。たとえば、従業員が源泉徴収票を変更した後、3年間、従業員のW-4レコードを変更されていない形式で保持することが会社のポリシーである可能性があります。別の企業ポリシーでは、従業員が解雇された後、W-4レコードを5年間保持することが義務付けられている場合があります。 その場合は、保持期間を5年に設定したEBRポリシーを作成できます。従業員が退職した後（「イベント」）、 EBR ポリシーを従業員の W-4 レコードに適用すると、保持期間が延長されます。これは通常、保持期間を手動で延長するよりも簡単です。特に、多数のファイルが含まれている場合に便利です。

手順

1. EBRポリシーを作成します。

   ```
   snaplock event-retention policy create -vserver SVM_name -name policy_name
   -retention-period retention_period
   ```

   次のコマンドは、保持期間が10年のEBRポリシーをに `vs1`作成し `employee_exit`ます。

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name
employee_exit -retention-period 10years
```

2. EBRポリシーを適用します。

   `snaplock event-retention apply -vserver SVM_name -name policy_name -volume volume_name -path path_name`

   次のコマンドは `vs1`、ディレクトリ内のすべてのファイルに `d1`EBRポリシーを適用し `employee_exit` ます。

```
cluster1::>snaplock event-retention apply -vserver vs1 -name
employee_exit -volume vol1 -path /d1
```

関連情報

- "SnapLock イベント保持ポリシーを作成"
- "SnapLock のイベント保持ポリシーが適用されます"

ONTAP SnapLockで保護された監査ログを作成する

ONTAP 9 .9.1以前を使用している場合は、SnapLockアグリゲートを作成してから、privileged deleteまたはSnapLockボリュームの移動を実行する前にSnapLockで保護された監査ログを作成する必要があります。この監査ログには、SnapLock管理者アカウントの作成と削除、ログボリュームに対する変更、privileged deleteが有効になっているかどうか、privileged delete処理、およびSnapLockボリューム移動処理が記録されます。

ONTAP 9 .10.1以降では、SnapLockアグリゲートの作成は廃止されました。SnapLock "SnapLockボリュームの明示的な作成" SnapLockタイプとしてComplianceまたはEnterpriseのいずれかを指定して、に-replace-typeオプションを使用する必要があります。

開始する前に

ONTAP 9 .9.1以前を使用している場合は、クラスタ管理者でSnapLockアグリゲートを作成する必要があります。

タスクの内容

監査ログは、ログファイルの保持期間が経過するまで削除できません。保持期間が経過したあとも監査ログを変更することはできません。これは、SnapLock ComplianceモードとEnterpriseモードの両方に当てはまります。

> ONTAP 9 .4以前では、SnapLock Enterpriseボリュームを監査ログに使用できません。SnapLock Complianceボリュームを使用する必要があります。ONTAP 9 .5以降では、監査ログにSnapLock EnterpriseボリュームまたはSnapLock Complianceボリュームのいずれかを使用できます。いずれの場合も、監査ログボリュームはジャンクションパスにマウントする必要があります `/snaplock_audit_log`。他のボリュームはこのジャンクションパスを使用できません。

SnapLock監査ログは、監査ログボリュームのルートの下のディレクトリのサブディレクトリ（privileged delete処理）および `system_log`（それ以外のすべて）に `privdel_log`あり `/snaplock_log`ます。監査ログのファイル名には最初にログに記録された処理のタイムスタンプが含まれているため、処理が実行されたおおよその時間で簡単にレコードを検索できます。

- コマンドを使用すると、監査ログボリューム上のログファイルを表示できます `snaplock log file show`。
- コマンドを使用すると、現在のログファイルをアーカイブして新しいログファイルを作成できます `snaplock log file archive`。これは、監査ログ情報を別のファイルに記録する必要がある場合に便利です。

および `snaplock log file archive`の詳細については `snaplock log file show`、を"ONTAPコマンド リファレンス"参照してください。

データ保護ボリュームをSnapLock監査ログボリュームとして使用することはできません。

手順

1. SnapLockアグリゲートを作成します。

   SnapLockアグリゲートを作成する

2. 監査ログを設定するSVMで、SnapLockボリュームを作成します。

   SnapLockボリュームを作成する

3. SVMの監査ログを設定します。

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   -size size -retention-period default_retention_period
   ```

   監査ログファイルのデフォルトの最小保持期間は6カ月です。該当するファイルの保持期間が監査ログの保持期間よりも長い場合、ログの保持期間はファイルの保持期間を継承します。したがって、privileged deleteを使用して削除されたファイルの保持期間が10カ月で、監査ログの保持期間が8カ月の場合、ログの保持期間は10カ月に延長されます。保持期間とデフォルトの保持期間の詳細については、を参照してください"保持期限を設定する"。

   次のコマンドは、SnapLockボリュームを使用して監査ログを `logVol`設定し `SVM1`ます。監査ログの最大サイズは20GBで、8カ月間保持されます。

   ```
   SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
   20GB -retention-period 8months
   ```

   の詳細については `snaplock log create`、を"ONTAPコマンド リファレンス"参照してください。

4. 監査ログを設定したSVMで、ジャンクションパスにSnapLockボリュームをマウントします `/snaplock_audit_log`。

   SnapLockボリュームのマウント

コマンドと `volume file fingerprint dump`コマンドを使用すると、ファイルの種類（通常、WORM、追記可能WORM）、ボリュームの有効期限など、ファイルとボリュームに関する重要な情報を表示できます `volume file fingerprint start。

手順

1. ファイルフィンガープリントを生成します。

   ```
   volume file fingerprint start -vserver <SVM_name> -file <file_path>
   ```

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   コマンドを実行すると、コマンドの入力として使用できるSession IDが生成され `volume file fingerprint dump`ます。

   > コマンドでSession IDを指定すると、フィンガープリント処理の進捗状況を監視できます `volume file fingerprint show`。フィンガープリントを表示する前に、処理が完了していることを確認してください。

2. ファイルのフィンガープリントを表示します。

   ```
   volume file fingerprint dump -session-id <session_ID>
   ```

   ```
   svm1::> volume file fingerprint dump -session-id 33619976
           Vserver:svm1
           Session-ID:33619976
           Volume:slc_vol
           Path:/vol/slc_vol/f1
           Data
   Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

   Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
   Algorithm:SHA256
           Fingerprint Scope:data-and-metadata
           Fingerprint Start Time:1460612586
           Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
           Fingerprint Version:3
           **SnapLock License:available**
           Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
           Volume MSID:2152884007
           Volume DSID:1028
           Hostname:my_host
   ```

```
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

WORMファイルを管理します。

ONTAP SnapLockでWORMファイルを管理する

WORMファイルは次の方法で管理できます。

- "ファイルをWORM状態にコミット"
- "SnapVaultデスティネーションでのSnapshotのWORM状態へのコミット"
- "ディザスタリカバリ用にWORMファイルをミラーリング"
- "訴訟時にWORMファイルを保持"

- "WORMファイルの削除"

ONTAP SnapLockを使用してファイルを**WORM**にコミットする

ファイルをWORM（Write Once、Read Many）にコミットするには、手動でコミットするか、自動的にコミットします。追記可能WORMファイルを作成することもできます。

ファイルを**WORM**状態に手動でコミット

ファイルを手動でWORM状態にコミットするには、ファイルを読み取り専用にします。ファイルの読み取り/書き込み属性は、NFSまたはCIFSで適切なコマンドやプログラムを使用して読み取り専用に変更できます。ファイルの書き込みが完了してファイルが途中でコミットされないようにする場合や、ボリューム数が多いために自動コミットスキャナの拡張に問題がある場合は、ファイルを手動でコミットすることを選択できます。

開始する前に

- コミットするファイルがSnapLockボリューム上にある必要があります。
- ファイルは書き込み可能である必要があります。

タスクの内容

ボリュームComplianceClock時間は、コマンドまたはプログラムの実行時にファイルのフィールドに書き込まれ `ctime`ます。ComplianceClock時間に基づいて、ファイルの保持期限に達したかどうかが決まります。

手順

1. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

   UNIXシェルで、次のコマンドを使用して、という名前のファイルを読み取り専用にし `document.txt`ます。

   ```
   chmod -w document.txt
   ```

   Windowsシェルで、次のコマンドを使用して、という名前のファイルを読み取り専用にし `document.txt`ます。

   ```
   attrib +r document.txt
   ```

ファイルを**WORM**状態に自動的にコミット

SnapLockの自動コミット機能を使用すると、ファイルをWORMに自動的にコミットできます。自動コミット機能では、自動コミット期間中に変更されなかったファイルがSnapLock ボリュームのWORM状態にコミットされます。自動コミット機能は、デフォルトでは無効になっています。

開始する前に

- 自動コミットするファイルがSnapLockボリューム上に存在している必要があります。
- SnapLockボリュームはオンラインである必要があります。
- SnapLockボリュームは読み書き可能ボリュームである必要があります。

SnapLockの自動コミット機能は、ボリューム内のすべてのファイルをスキャンし、自動コミットの要件を満たしている場合はファイルをコミットします。ファイルが自動コミットできる状態になってから、SnapLock自動コミットスキャナによって実際にコミットされるまでに、時間がかかることがあります。ただし、ファイルは自動コミットの対象になった時点からファイルシステムによる削除や変更から保護されます。

タスクの内容

_autocommit_period _ は、ファイルが自動コミットされるまでに、ファイルに変更がないようにする期間を指定します。この期間が経過する前にファイルが変更された場合、自動コミット期間はもう一度最初からカウントされます。

自動コミット期間に指定できる値は次のとおりです。

値	単位	脚注
なし	-	デフォルトです。
5-5256000	分	-
1-87600	時間	-
1～3650	日	-
1 ~ 120	月	-
1 ~ 10	年	-

最小値は5分、最大値は10年です。

手順

1. SnapLockボリューム上のファイルをWORM状態に自動コミットします。

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -autocommit -period *autocommit_period*

   の詳細については `volume snaplock modify`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、5時間変更がないかぎり、SVM vs1のボリューム上のファイルを自動コミットし `vol1`ます。

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

追記可能**WORM**ファイルの作成

追記可能WORMファイルには、ログエントリと同様に段階的に書き込まれたデータが保持されます。追記可能 WORM ファイルは、適切なコマンドやプログラムを使用して作成するか、 SnapLock のボリュームアペンドモード機能を使用してデフォルトで作成できます。

コマンドまたはプログラムを使用して追記可能**WORM**ファイルを作成する

追記可能WORMファイルは、NFSまたはCIFSで適切なコマンドやプログラムを使用して作成できます。追記可能WORMファイルには、ログエントリと同様に段階的に書き込まれたデータが保持されます。データは256KBのチャンク単位でファイルに追加されます。各チャンクが書き込まれると、前のチャンクがWORM方式で保護されます。このファイルは保持期間が経過するまで削除できません。

開始する前に

追記可能WORMファイルはSnapLockボリュームに格納する必要があります。

タスクの内容

データは、アクティブな256KBチャンクに順番に書き込まれる必要はありません。ファイルの n * 256KB+1 バイトにデータが書き込まれると、 1 つ前の 256KB セグメントが WORM 方式で保護されます。

現在アクティブな256KBチャンクを超える順序付けされていない書き込みは、アクティブな256KBチャンクが最新のオフセットにリセットされ、古いオフセットへの書き込みが「読み取り専用ファイルシステム（ROFS）」エラーで失敗します。書き込みオフセットは、クライアントアプリケーションによって異なります。追記可能WORMファイル書き込みセマンティクスに準拠していないクライアントが原因で、書き込み内容が誤って終了する可能性があります。したがって、順序付けされていない書き込みのオフセット制限に従うか、ファイルシステムを同期モードでマウントして同期書き込みを確保することを推奨します。

手順

1. 適切なコマンドまたはプログラムを使用して、必要な保持期限を指定した空のファイルを作成します。

   UNIXシェルで、次のコマンドを使用して、という名前のゼロ長ファイルに保持期限を2020年11月21日午前6時に設定し `document.txt`ます。

   ```
   touch -a -t 202011210600 document.txt
   ```

2. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

   UNIXシェルで、次のコマンドを使用して、という名前のファイルを読み取り専用にし `document.txt`ます。

   ```
   chmod 444 document.txt
   ```

3. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を書き込み可能に戻します。

   ファイルにデータがないため、この手順はコンプライアンスリスクとはみなされません。

   UNIXシェルで、次のコマンドを使用して、という名前のファイルを書き込み可能にし `document.txt`ます。

```
chmod 777 document.txt
```

4. 適切なコマンドまたはプログラムを使用して、ファイルへのデータの書き込みを開始します。

   UNIXシェルで、次のコマンドを使用してにデータを書き込み `document.txt`ます。

```
echo test data >> document.txt
```

   ファイルにデータを追加する必要がなくなったら、ファイル権限を読み取り専用に戻してください。

ボリュームアペンドモードを使用して追記可能**WORM**ファイルを作成する

ONTAP 9.3 以降では、 SnapLock のボリュームアペンドモード（ VAM ）機能を使用して、追記可能 WORM ファイルをデフォルトで作成できます。追記可能WORMファイルには、ログエントリと同様に段階的に書き込まれたデータが保持されます。データは256KBのチャンク単位でファイルに追加されます。各チャンクが書き込まれると、前のチャンクがWORM方式で保護されます。このファイルは保持期間が経過するまで削除できません。

開始する前に

- 追記可能WORMファイルはSnapLockボリュームに格納する必要があります。
- SnapLockボリュームはアンマウントされていて、Snapshotとユーザが作成したファイルが含まれていない必要があります。

タスクの内容

データは、アクティブな256KBチャンクに順番に書き込まれる必要はありません。ファイルの n * 256KB+1 バイトにデータが書き込まれると、 1 つ前の 256KB セグメントが WORM 方式で保護されます。

ボリュームに自動コミット期間を指定した場合、追記可能WORMファイルに変更がなかった期間が自動コミット期間を超えると、そのファイルはWORM状態にコミットされます。

VAMはSnapLock監査ログボリュームではサポートされません。

手順

1. VAMを有効にします。

   `volume snaplock modify -vserver *SVM_name* -volume *volume_name* -is-volume-append -mode-enabled true|false`

   の詳細については `volume snaplock modify`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、SVM`vs1`のボリュームでVAMを有効にし `vol1`ます。

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. 適切なコマンドまたはプログラムを使用して、書き込み権限を持つファイルを作成します。

   ファイルはデフォルトで追記可能WORMです。

ONTAPヴォールト宛先でスナップショットを WORM にコミットする

SnapLock for SnapVaultを使用すると、セカンダリストレージ上のSnapshotをWORM方式で保護できます。SnapLockの基本タスクはすべてSnapVaultデスティネーションで実行します。デスティネーションボリュームは自動的に読み取り専用でマウントされるため、SnapshotをWORM状態に明示的にコミットする必要はありません。

開始する前に

- System Managerを使用して関係を設定する場合は、ソースとデスティネーションの両方のクラスタでONTAP 9.15.1以降が実行されている必要があります。
- デスティネーション クラスタ：
  - "SnapLock ライセンスをインストール"です。
  - "コンプライアンスクロックの初期化"です。
  - 9.10.1より前のONTAPリリースでCLIを使用している場合は、"SnapLockアグリゲートを作成する"
- 保護ポリシーのタイプは「vault」である必要があります。
- ソースアグリゲートとデスティネーションアグリゲートは64ビットである必要があります。
- ソースボリュームをSnapLockボリュームにすることはできません。
- ONTAP CLIを使用している場合は、およびにソースボリュームとデスティネーションボリュームを作成する必要があります"ヒアリンククラスタ""SVM"。

タスクの内容

ソース ボリュームで使用するストレージは、NetAppのストレージでもNetApp以外のストレージでもかまいません。

> WORM状態にコミットされたSnapshotの名前は変更できません。

SnapLockボリュームはクローニングできますが、SnapLockボリューム上のファイルはクローニングできません。

> SnapLockボリュームではLUNはサポートされません。SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、改ざん防止Snapshotは、SnapMirrorのソースボリュームと、LUNを含むデスティネーションボリュームの両方でサポートされます。

ONTAP 9 .10.1以降では、SnapLockボリュームとSnapLock以外のボリュームを同じアグリゲート上に配置できます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はあ

りません。Compliance SnapLockまたはEnterprise SnapLockのボリュームタイプを指定するには、ボリューム「-Enterprise-type」オプションを使用します。ONTAP 9 10.1より前のONTAPリリースでは、SnapLockモード（ComplianceまたはEnterprise）がアグリゲートから継承されます。バージョンに依存しないデスティネーションボリュームはサポートされません。デスティネーションボリュームの言語設定は、ソースボリュームの言語設定と一致している必要があります。

バックアップデスティネーションであるSnapLockには、デフォルトの保持期間が割り当てられています。この期間の最初の値は、SnapLock Enterpriseボリュームの場合は最小0年、SnapLock Complianceボリュームの場合は最大30年です。各NetApp Snapshotは、最初はこのデフォルトの保持期間でコミットされます。保持期間は、必要に応じてあとから延長できます。詳細については、を参照してください "保持期限の設定の概要を確認します"。

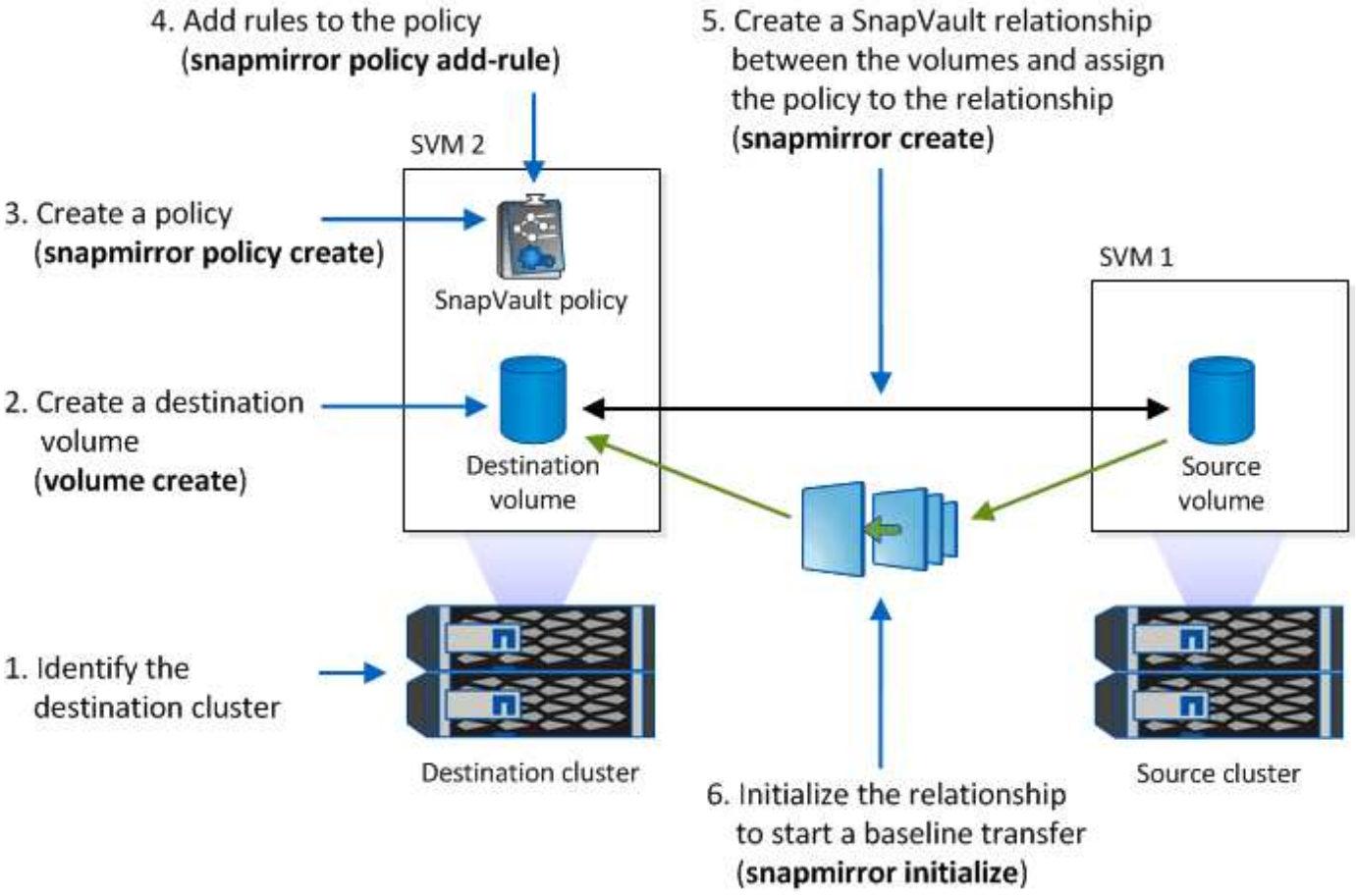
ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーに特定のSnapMirrorラベルの保持期間を指定できます。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたSnapshotが、ルールで指定された保持期間に保持されます。保持期間を指定しない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

ONTAP 9.13.1以降では、ボリュームクローン作成処理の実行時にオプションをに設定し `non-snaplock` てFlexCloneを作成し、そのSnapshotを「parent-snapshot」として指定することで、SnapLockバックアップ関係のデスティネーションSnapLockボリュームでロックされたSnapshotを瞬時にリストアできます。 `snaplock-type`詳細については、をご覧ください "SnapLock タイプのFlexCloneボリュームを作成します"。

MetroCluster構成の場合は、次の点に注意してください。

- SnapVault関係は同期元のSVM間でのみ作成でき、同期元のSVMと同期先のSVM間では作成できません。
- 同期元のSVMのボリュームからデータ提供用のSVMへのSnapVault関係を作成できます。
- データ提供用のSVMから同期元のSVMのDPボリュームへのSnapVault関係を作成できます。

次の図は、SnapLockバックアップ関係を初期化する手順を示しています。



手順

CLIを使用してSnapLockバックアップ関係を作成することも、.15.1以降ではONTAP ONTAP 9を使用してSnapLockバックアップ関係を作成することもできます。

System Manager

1. ソースクラスタで*[ストレージ]>[ボリューム]に移動し、[追加]*を選択します。
2. ウィンドウで、[その他のオプション]*を選択します。
3. ボリューム名、サイズ、エクスポートポリシー、および共有名を入力します。
4. 変更を保存します。
5. デスティネーションクラスタで、*[保護]>[関係]*に移動します。
6. [ソース]列の上にある*を選択し、メニューから[ボリューム]*を選択します。
7. ウィンドウで、保護ポリシーとして[バックアップ]*を選択します。
8. [ソース]*セクションで、保護するクラスタ、Storage VM、およびボリュームを選択します。
9. [デスティネーション]セクションの*で、[デスティネーションのSnapshotをロックする]を選択し、*ロック方法として SnapLock for SnapVault *を選択します。*ロック方法*は、選択したポリシータイプがタイプでない場合、SnapLockライセンスがインストールされていない場合、またはコンプライアンスクロックが初期化されていない場合は表示されません `vault`。
10. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、*[Initialize Compliance Clock]*を選択します。
11. 変更を保存します。

CLI

1. デスティネーションクラスタで、ソースボリュームと同じサイズ以上のタイプのSnapLockデスティネーションボリュームを作成し `DP`ます。

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise> -type DP
   -size <size>
   ```

   次のコマンドは、という名前の2GBのSnapLock Complianceボリュームを `dstvolB` `SVM2`アグリゲート上に作成し `node01_aggr`ます。

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

2. デスティネーションクラスタで、"デフォルトの保持期間を設定する"を実行します。
3. "新しいレプリケーション関係を作成"SnapLock以外のソースと作成した新しいSnapLockデスティネーション間。

   この例では、ポリシーを使用して、dailyおよびweeklyというラベルのSnapshotを毎時スケジュールでバックアップするように、 `XDPDefault`デスティネーションSnapLockボリュームとの新しいSnapMirror関係を作成し `dstvolB`ます。

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

"カスタムレプリケーションポリシーを作成します。"または"カスタムスケジュール"、使用可能なデフォルト値が適切でない場合に使用します。

4. デスティネーションSVMで、作成したSnapVault関係を初期化します。

```
snapmirror initialize -destination-path <destination_path>
```

次のコマンドは、の `SVM1`ソースボリュームとの `SVM2`デスティネーションボリューム `dstvolB`間の関係を初期化し `srcvolA`ます。

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 関係が初期化されアイドル状態になったら、デスティネーションでコマンドを使用して `snapshot show`、レプリケートされたSnapshotに適用されているSnapLock有効期限を確認します。

この例では、SnapMirrorラベルとSnapLockの有効期限が設定されたボリューム上のSnapshotを表示して `dstvolB`います。

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

関連情報

- "クラスタとSVMのピアリング"
- "SnapVaultによるボリュームのバックアップ"
- "スナップミラーの初期化"

災害復旧のために**ONTAP SnapMirror**を使用して **WORM** ファイルをミラーリングする

SnapMirrorを使用すると、ディザスタリカバリなどの目的で、地理的に離れた別の場所にWORMファイルをレプリケートできます。ソースボリュームとデスティネーションボリュームの両方がSnapLock用に設定されていて、両方のボリュームのSnapLockモード（ComplianceまたはEnterprise）が同じである必要があります。ボリュームとファイルの主要なSnapLockプロパティがすべてレプリケートされます。

前提条件

ピアSVMを含むピア クラスタにソース ボリュームとデスティネーション ボリュームを作成する必要があります。詳細については、を参照してください "クラスタとSVMのピアリング"。

タスクの内容

- .5以降では、ONTAP 9（データ保護）タイプの関係ではなくXDP（拡張データ保護）タイプのSnapMirror関係を使用してWORMファイルをレプリケートできます。XDPモードはONTAPのバージョンに依存せず、同じブロックに格納されているファイルを区別できるため、レプリケートされたComplianceモードのボリュームの再同期がはるかに簡単になります。既存のDPタイプの関係をXDPタイプの関係に変換する方法については、を参照してください"データ保護"。
- ComplianceモードのボリュームでDPタイプのSnapMirror関係を再同期する場合、再同期によってデータが失われるとSnapLockで判断されると処理は失敗します。再同期処理に失敗した場合は、コマンドを使用してデスティネーションボリュームのクローンを作成でき `volume clone create`ます。その後、ソースボリュームとクローンを再同期できます。
- SnapLockボリュームのSnapMirror関係は、 `MirrorAllSnapshots` async-mirror タイプのポリシー。SnapLockボリュームの保持期間は、保持されるすべての WORM ファイルの最大保持期間によって決まります。宛先はソースの DR コピーであるため、宛先SnapLockボリュームの保持期間はソースと同じになります。
- SnapLock準拠ボリューム間のXDPタイプのSnapMirror関係では、解除後の再同期がサポートされます。これは、解除後にデスティネーションのデータがソースから分岐していた場合でも同様です。

  再同期では、共通のSnapshotを超えてソースとデスティネーションの間でデータの相違が検出されると、この相違をキャプチャするためにデスティネーションで新しいSnapshotがカットされます。新しいSnapshotと共通のSnapshotの両方が次の保持期間でロックされます。

  - デスティネーションのボリューム有効期限
  - ボリューム有効期限が過ぎているか設定されていない場合、Snapshotは30日間ロックされます。
  - デスティネーションにリーガルホールドが設定されている場合、実際のボリューム有効期限はマスクされて「無期限」と表示されますが、Snapshotは実際のボリューム有効期限内はロックされます。

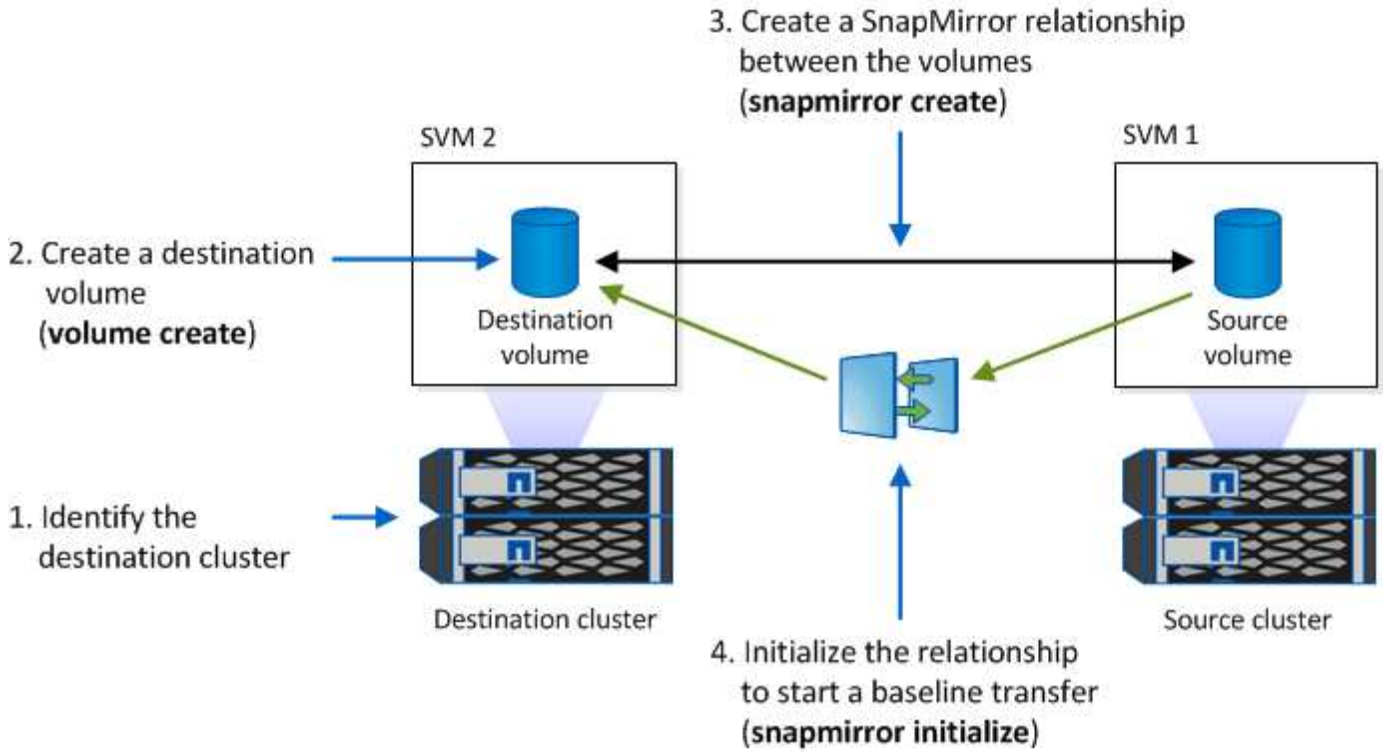
デスティネーションボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が保持され、再同期後にソースボリュームの有効期限で上書きされることはありません。

デスティネーションにソースとは異なるリーガルホールドが設定されている場合、再同期は許可されません。再同期を試行する前に、ソースとデスティネーションのリーガルホールドが同一であるか、デスティネーションのリーガルホールドがすべて解除されている必要があります。

異なるデータをキャプチャするためにデスティネーションボリュームで作成されたロックされたSnapshotは、CLIでコマンドを実行してソースにコピーできます。 `snapmirror update -s snapshot`コピーされたSnapshotは、ソースでも引き続きロックされます。

- SVMデータ保護関係はサポートされません。
- 負荷共有データ保護関係はサポートされません。

次の図は、SnapMirror関係を初期化する手順を示しています。


3. Create a SnapMirror relationship between the volumes (snapmirror create)
SVM 2
SVM 1
2. Create a destination volume (volume create)
Destination volume
Source volume
1. Identify the destination cluster
Destination cluster
Source cluster
4. Initialize the relationship to start a baseline transfer (snapmirror initialize)

System Manager

ONTAP 9 .12.1以降では、System Managerを使用してWORMファイルのSnapMirrorレプリケーションを設定できます。

手順

1. [ストレージ]>[ボリューム]に移動します。
2. 表示/非表示*をクリックし、 SnapLock タイプ*を選択して、*ボリューム*ウィンドウに列を表示します。
3. SnapLockボリュームを探します。
4. をクリックし ⋮ 、*[保護]*を選択します。
5. デスティネーションクラスタとデスティネーションStorage VMを選択
6. [* その他のオプション *] をクリックします。
7. [Show legacy policies*]を選択し、[**DPDefault (legacy)**]を選択します。
8. 「接続先設定の詳細」セクションで「転送スケジュールの上書き」を選択し、「*時間単位」を選択します。
9. [保存（ Save ）] をクリックします。
10. ソースボリューム名の左側にある矢印をクリックしてボリュームの詳細を展開し、ページの右側でリモートSnapMirror保護の詳細を確認します。
11. リモートクラスタで、「保護関係」に移動します。
12. 関係を検索し、デスティネーションボリューム名をクリックして関係の詳細を表示します。
13. デスティネーションボリュームのSnapLockタイプやその他のSnapLock情報を確認します。

CLI

1. デスティネーションクラスタを特定
2. デスティネーションクラスタ、"SnapLockライセンスをインストールする"、"コンプライアンスクロックの初期化"、および9.10.1より前のONTAPリリースを使用している場合は、"SnapLockアグリゲートを作成する"。
3. デスティネーションクラスタで、ソースボリュームと同じサイズ以上のSnapLockデスティネーションボリュームを作成し `DP`ます。

```
volume create -vserver SVM_name -volume volume_name -aggregate
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```

> ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームを同じアグリゲートに配置できるため、ONTAP 9.10.1を使用している場合はSnapLockアグリゲートを別々に作成する必要はありません。ボリュームの-snaplock-typeオプションを使用して、SnapLockボリューム タイプ（ComplianceまたはEnterprise）を指定します。ONTAP 9.10.1より前のリリースでは、SnapLockモード（ComplianceまたはEnterprise）はアグリゲートから継承されます。デスティネーション ボリュームの言語設定とソース ボリュームの言語設定が一致している必要があります。

次のコマンドは、という名前の2GBのSnapLockボリュームを `dstvolB` `SVM2`アグリゲート上に `node01_aggr`作成し `Compliance`ます。

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. デスティネーションSVMで、SnapMirrorポリシーを作成します。

   `snapmirror policy create -vserver *SVM_name* -policy *policy_name*`

   次のコマンドは、SVM全体のポリシーを作成し `SVM1-mirror`ます。

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. デスティネーションSVMで、SnapMirrorスケジュールを作成します。

   `job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*`

   次のコマンドは、という名前のSnapMirrorスケジュールを作成し `weekendcron`ます。

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. デスティネーションSVMで、SnapMirror関係を作成します。

   `snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*`

   次のコマンドでは、の `SVM1`ソースボリュームとの `SVM2`デスティネーションボリューム `dstvolB`の間にSnapMirror関係を作成し `srcvolA`、ポリシーとスケジュールを `weekendcron`割り当て `SVM1-mirror`ます。

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   XDPタイプはONTAP 9 .5以降で使用できます。ONTAP 9 .4以前ではDPタイプを使用する必要があります。

7. デスティネーションSVMで、SnapMirror関係を初期化します。

   `snapmirror initialize -destination-path *destination_path*`

   初期化プロセスでは、デスティネーションボリュームへの _ ベースライン転送 _ が実行されます。SnapMirrorはソースボリュームのSnapshotを作成して、そのコピーおよびコピーが参照するすべてのデータブロックをデスティネーションボリュームに転送します。また、ソースボリューム上のその他のSnapshotもデスティネーションボリュームに転送します。

次のコマンドは、の `SVM1`ソースボリュームとの `SVM2`デスティネーションボリューム `dstvolB` 間の関係を初期化し `srcvolA`ます。

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

関連情報

- "クラスタとSVMのピアリング"
- "ボリュームのディザスタリカバリの準備"
- "データ保護"
- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror policy create"

ONTAP SnapLock Legal Hold を使用して訴訟中に **WORM** ファイルを保持

ONTAP 9.3以降では、_Legal Hold_featureを使用して、ComplianceモードのWORMファイルを訴訟の期間にわたって保持できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

  "SnapLock管理者アカウントの作成"

- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

タスクの内容

リーガルホールドの対象となるファイルは、保持期間が無期限のWORMファイルのように動作します。リーガルホールド期間の終了日を指定するのは、お客様の責任です。

リーガルホールドの対象となるファイル数は、ボリュームで使用可能なスペースによって異なります。

手順

1. リーガルホールドを開始します。

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   次のコマンドは、のすべてのファイルに対してリーガルホールドを開始し `vol1`ます。

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. リーガルホールドの終了：

```
snaplock legal-hold end -litigation-name <litigation_name> -volume
<volume_name> -path <path_name>
```

次のコマンドは、のすべてのファイルのリーガルホールドを終了し `vol1`ます。

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

関連情報

- "SnapLock リーガルホールドの開始"
- "SnapLock リーガルホールドの終了"

ONTAP SnapLockでWORMファイルを削除する

privileged delete機能を使用して、保持期間中にEnterpriseモードのWORMファイルを削除できます。この機能を使用するには、SnapLock管理者アカウントを作成し、そのアカウントを使用して機能を有効にする必要があります。

SnapLock管理者アカウントの作成

privileged deleteを実行するには、SnapLock管理者Privilegesが必要です。これらのPrivilegesは、SnapLockロールで定義されます。このロールが割り当てられていない場合は、クラスタ管理者に依頼して、 SnapLock 管理者ロールを持つ SVM 管理者アカウントを作成してもらいます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

手順

1. SnapLock管理者ロールを持つSVM管理者アカウントを作成します。

   security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment

   次のコマンドは、事前定義されたロールが割り当てられた `vsadmin-snaplock`SVM管理者アカウントにパスワードを使用したアクセスを `SVM1`許可し `SnapLockAdmin`ます。

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

privileged delete機能を有効にする

privileged delete機能は、削除するWORMファイルが格納されているEnterpriseボリュームで明示的に有効にする必要があります。

タスクの内容

オプションの値 `-privileged-delete`によって、`privileged delete`が有効かどうかが決まります。指定できる値は `enabled`、 `disabled`、および `permanently-disabled`です。

> `permanently-disabled`は、終了状態です。ボリュームで状態をに設定したあとに`privileged delete`を有効にすることはできません `permanently-disabled`。

手順

1. SnapLock Enterpriseボリュームに対してprivileged deleteを有効にします。

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   次のコマンドは、の `SVM1`Enterpriseボリュームに対してprivileged delete機能を有効にし `dataVol`ます。

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

EnterpriseモードのWORMファイルの削除

privileged delete機能を使用すると、保持期間中にEnterpriseモードのWORMファイルを削除できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。
- EnterpriseボリュームでSnapLock監査ログを作成し、privileged delete機能を有効にしておく必要があります。

タスクの内容

privileged delete処理を使用して、期限切れのWORMファイルを削除することはできません。コマンドを使用して、削除するWORMファイルの保持期限を表示できます `volume file retention show`。の詳細については `volume file retention show`、を"ONTAPコマンド リファレンス"参照してください。

ステップ

1. EnterpriseボリュームのWORMファイルを削除します。

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   次のコマンドは、SVM上の`SVM1`ファイルを削除し `/vol/dataVol/f1`ます。

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

ONTAP SnapLockボリュームを移動する

ONTAP 9 .8以降では、SnapLockボリュームを同じタイプのデスティネーションアグリゲート（エンタープライズからエンタープライズ、コンプライアンスからコンプライアンス）に移動できます。SnapLockボリュームを移動するには、SnapLockのセキュリティロールが割り当てられている必要があります。

SnapLockセキュリティ管理者アカウントを作成する

SnapLockボリュームの移動を実行するには、SnapLockセキュリティ管理者Privilegesが必要です。この権限は、 ONTAP 9.8 で導入された _ SnapLock _ ロールで付与されます。このロールが割り当てられていない場合は、クラスタ管理者に依頼して、このSnapLockセキュリティロールを持つSnapLockセキュリティユーザの作成を依頼できます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

タスクの内容

SnapLockロールは管理SVMに関連付けられますが、vsadmin-SVM SnapLockロールはデータSVMに関連付けられます。

ステップ

1. SnapLock管理者ロールを持つSVM管理者アカウントを作成します。

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   次のコマンドは、事前定義のロールが割り当てられた `snaplock`SVM管理者アカウントが、パスワードを使用した管理SVMへのアクセスを `cluster1`許可し `SnapLockAdmin`ます。

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

   の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

SnapLockボリュームを移動する

コマンドを使用すると、SnapLockボリュームをデスティネーションアグリゲートに移動できます `volume move`。

開始する前に

- SnapLockボリュームの移動を実行する前に、SnapLockで保護された監査ログを作成しておく必要があります。

  "監査ログを作成する"です。

- ONTAP 9 10.1より前のバージョンのONTAPを使用している場合は、デスティネーションアグリゲートのSnapLockタイプが移動するSnapLockと同じである必要があります（ComplianceからComplianceへ、またはEnterpriseからEnterpriseへ）。ONTAP 9 .10.1以降では、この制限が解除され、アグリゲートにComplianceボリュームとEnterprise SnapLockボリュームの両方を含めることができるようになりました。また、SnapLock以外のボリュームも含めることができます。
- SnapLockのセキュリティロールを持つユーザである必要があります。

手順

1. セキュアな接続を使用して、ONTAPクラスタ管理LIFにログインします。

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. SnapLockボリュームを移動します。

   ```
   volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
   -aggregate destination_aggregate_name
   ```

3. ボリューム移動処理のステータスを確認します。

   ```
   volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
   volume,phase,vserver
   ```

ランサムウェア攻撃から保護するために**ONTAP**スナップショットをロックする

ONTAP 9.12.1以降では、SnapLock以外のボリュームでSnapshotをロックして、ランサムウェア攻撃から保護できます。スナップショットをロックすると、誤ってまたは悪意を持って削除されることがなくなります。

SnapLock Complianceクロック機能を使用すると、Snapshotを指定した期間ロックして、有効期限に達するまで削除できないようにすることができます。Snapshotをロックすることで改ざんを防止し、ランサムウェアの脅威から保護できます。ロックされたSnapshotを使用して、ランサムウェア攻撃によってボリュームが侵害された場合にデータをリカバリできます。

ONTAP 9.14.1以降では、SnapLockヴォールトデスティネーションおよびSnapLock SnapMirror以外のデスティネーションボリュームでの長期保持Snapshotがサポートされます。Snapshotロックを有効にするには、に関連付けられたSnapMirrorポリシールールを使用して保持期間を設定し既存のポリシーラベルます。このルールは、ボリュームに設定されているデフォルトの保持期間よりも優先されます。SnapMirrorラベルに保持期間が関連付けられていない場合は、ボリュームのデフォルトの保持期間が使用されます。

改ざん防止スナップショットの要件と考慮事項

- ONTAP CLIを使用する場合は、クラスタ内のすべてのノードでONTAP 9.12.1以降が実行されている必要があります。System Managerを使用する場合は、すべてのノードでONTAP 9.13.1以降が実行されている必要があります。
- "SnapLockライセンスがクラスタにインストールされている必要があります。"です。このライセンスはに含まれてい"ONTAP One"ます。

- "クラスタのコンプライアンスクロックを初期化する必要があります。"です。
- ボリュームでSnapshotロックが有効になっている場合は、クラスタをONTAP 9.12.1より新しいバージョンのONTAPにアップグレードできます。ただし、ロックされたSnapshotがすべて有効期限に達して削除され、Snapshotロックが無効になるまで、ONTAPを以前のバージョンに戻すことはできません。
- Snapshotがロックされている場合、ボリューム有効期限はSnapshotの有効期限に設定されます。複数のSnapshotがロックされている場合は、すべてのSnapshotの中で最も長い有効時間がボリューム有効時間に反映されます。
- ロックされたSnapshotの保持期間はSnapshot保持数よりも優先されます。つまり、ロックされたSnapshotのSnapshot保持期間が満了していない場合、保持数の制限は適用されません。
- SnapMirror関係では、ミラーバックアップポリシールールに保持期間を設定できます。デスティネーションボリュームでSnapshotロックが有効になっている場合は、デスティネーションにレプリケートされたSnapshotに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、有効期限を過ぎていないSnapshotは、保持数を超えても保持されます。
- SnapLock以外のボリューム上のSnapshotの名前を変更できます。SnapMirror関係のプライマリボリュームでのSnapshot名変更処理は、ポリシーがMirrorAllSnapshotsの場合にのみセカンダリボリュームに反映されます。それ以外のポリシータイプの場合、名前を変更したSnapshotは更新時に伝播されません。
- ONTAP CLIを使用している場合は、ロックされたSnapshotが最新のものである場合にのみ、コマンドを使用してロックされたSnapshotをリストアでき `volume snapshot restore`ます。リストア対象のスナップショットよりもあとに期限切れになっていないスナップショットがある場合、スナップショットのリストア処理は失敗します。

改ざん防止スナップショットでサポートされる機能

- "Cloud Volumes ONTAP"
- FlexGroupボリユウム

  FlexGroupボリュームではSnapshotロックがサポートされます。Snapshotのロックは、ルートコンスティチュエントのSnapshotに対してのみ実行されます。FlexGroupボリュームを削除できるのは、ルートコンスティチュエントの有効期限が過ぎている場合のみです。

- FlexVolからFlexGroupへの変換

  ロックされたSnapshotを含むFlexVol volumeをFlexGroupボリュームに変換できます。変換後もスナップショットはロックされたままになります。

- SnapMirror非同期

  コンプライアンスクロックは、ソースとデスティネーションの両方で初期化する必要があります。

- SVMデータの移動（ソースクラスタからデスティネーションクラスタにSVMを移行または再配置する場合に使用）

  ONTAP 9.14.1以降でサポートされます。

- パラメータを使用したSnapMirrorポリシールール `-schedule`
- SVM DR

  コンプライアンスクロックは、ソースとデスティネーションの両方で初期化する必要があります。

- ボリューム クローンとファイル クローン

ロックされたSnapshotからボリュームクローンとファイルクローンを作成できます。

- FlexCacheホリユウム

  ONTAP 9.16.1以降でサポート。

サポートされない機能

改ざん防止スナップショットでは、現在次の機能はサポートされていません。

- 整合グループ
- "FabricPool"

  改ざん防止スナップショットは、削除できない改ざん防止機能を提供します。FabricPoolではデータを削除する機能が必要なため、同じボリュームでFabricPoolロックとSnapshotロックを有効にすることはできません。

- SMTape
- SnapMirrorアクティブ同期
- SnapMirror同期

ボリューム作成時に**Snapshot**ロックを有効にする

ONTAP 9.12.1以降では、新しいボリュームを作成するとき、またはCLIのコマンドと `volume modify`コマンドでオプションを `volume create`使用して既存のボリュームを変更するときに、Snapshotロックを有効にでき `-snapshot-locking-enabled`ます。ONTAP 9.13.1以降では、System Managerを使用してSnapshotロックを有効にできます。

System Manager

1. [ストレージ]>[ボリューム]に移動し、[追加]*を選択します。
2. ウィンドウで、[その他のオプション]*を選択します。
3. ボリューム名、サイズ、エクスポートポリシー、および共有名を入力します。
4. [Enable Snapshot locking]*を選択します。SnapLockライセンスがインストールされていない場合、この選択は表示されません。
5. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、*[Initialize Compliance Clock]*を選択します。
6. 変更を保存します。
7. ウィンドウで、更新したボリュームを選択し、[概要]*を選択します。
8. SnapLockスナップショットロック*が*有効*と表示されていることを確認します。

CLI

1. 新しいボリュームを作成してSnapshotロックを有効にするには、次のコマンドを入力します。

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   次のコマンドは、vol1という名前の新しいボリュームでSnapshotロックを有効にします。

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

既存のボリュームで**Snapshot**ロックを有効にする

ONTAP 9.12.1以降では、ONTAP CLIを使用して既存のボリュームでSnapshotロックを有効にできます。ONTAP 9.13.1以降では、System Managerを使用して既存のボリュームに対してSnapshotロックを有効にすることができます。

System Manager

1. [ストレージ]>[ボリューム]に移動します。
2. を選択 ⋮ し、*[編集]>[ボリューム]*を選択します。
3. ウィンドウで、**[Snapshot**（ローカル）設定**]**セクションを探し、[Snapshotのロックを有効にする]*を選択します。

   SnapLockライセンスがインストールされていない場合、この選択は表示されません。
4. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、*[Initialize Compliance Clock]*を選択します。
5. 変更を保存します。
6. ウィンドウで、更新したボリュームを選択し、[概要]*を選択します。
7. * SnapLockスナップショット ロック* が 有効 として表示されていることを確認します。

CLI

1. 既存のボリュームを変更してSnapshotロックを有効にするには、次のコマンドを入力します。

   ```
   volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

ロックされた**Snapshot**ポリシーを作成して保持を適用する

ONTAP 9.12.1以降では、Snapshotポリシーを作成してSnapshot保持期間を適用し、そのポリシーをボリュームに適用して、指定した期間Snapshotをロックできます。保持期間を手動で設定してSnapshotをロックすることもできます。ONTAP 9.13.1以降では、System Managerを使用してSnapshotロックポリシーを作成し、ボリュームに適用できます。

スナップショットロックポリシーを作成します。

System Manager

1. [ストレージ]>[Storage VM]*に移動し、Storage VMを選択します。
2. [設定]*を選択します。
3. [Snapshot Policies]*に移動し、を選択します →。
4. [Snapshotポリシーの追加]*ウィンドウで、ポリシー名を入力します。
5. を選択します + Add 。
6. Snapshotスケジュールの詳細（スケジュール名、保持するSnapshotの最大数、SnapLock保持期間など）を指定します。
7. SnapLockの保持期間*列に、Snapshotを保持する時間数、日数、月数、または年数を入力します。たとえば、保持期間が5日のSnapshotポリシーでは、Snapshotが作成されてから5日間ロックされ、その間は削除できません。サポートされる保持期間は次のとおりです。
   - 年：0～100
   - 月：0～1200
   - 日数：0～36500
   - 営業時間：0～24
8. 変更を保存します。

CLI

1. Snapshotポリシーを作成するには、次のコマンドを入力します。

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   次のコマンドは、Snapshotロックポリシーを作成します。

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   アクティブな保持期間にあるSnapshotは置き換えられません。つまり、期限切れになっていないロックされたSnapshotがある場合、保持数は考慮されません。

ボリュームへのロックポリシーの適用

System Manager

1. [ストレージ]>[ボリューム]に移動します。
2. を選択 ⋮ し、*[編集]>[ボリューム]*を選択します。
3. ウィンドウで、[Snapshotのスケジュール設定]*を選択します。
4. リストからロックSnapshotポリシーを選択します。
5. スナップショットのロックがまだ有効になっていない場合は、*スナップショットのロックを有効にする*を選択します。
6. 変更を保存します。

CLI

1. 既存のボリュームにSnapshotロックポリシーを適用するには、次のコマンドを入力します。

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
-policy <policy_name>
```

Snapshotの手動作成時に保持期間を適用

Snapshotの保持期間は、手動でSnapshotを作成するときに適用できます。ボリュームでSnapshotロックが有効になっている必要があります。有効になっていない場合、保持期間の設定は無視されます。

System Manager

1. [ストレージ]>[ボリューム]*に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、*[Snapshots]*タブを選択します。
3. を選択します ＋ Add 。
4. Snapshot名とSnapLockの有効期限を入力します。カレンダーを選択して、保持期限の日付と時刻を選択できます。
5. 変更を保存します。
6. [ボリューム]>[Snapshots]ページで、[表示/非表示]を選択し、[SnapLock Expiration Time]を選択してSnapLock Expiration Time *列を表示し、保持期限が設定されていることを確認します。

CLI

1. スナップショットを手動で作成し、ロック保持期間を適用するには、次のコマンドを入力します。

```
volume snapshot create -volume <volume_name> -snapshot <snapshot name>
-snaplock-expiry-time <expiration_date_time>
```

次のコマンドでは、新しいSnapshotを作成して保持期間を設定します。

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

System Manager

1. [ストレージ]>[ボリューム]*に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、*[Snapshots]*タブを選択します。
3. Snapshotを選択し、を選択して*[Modify SnapLock Expiration Time]*を選択します。カレンダーを選択して、保持期限の日付と時刻を選択できます。
4. 変更を保存します。
5. [ボリューム]>[Snapshots]ページで、[表示/非表示]を選択し、[SnapLock Expiration Time]を選択してSnapLock Expiration Time *列を表示し、保持期限が設定されていることを確認します。

CLI

1. 既存のSnapshotに保持期間を手動で適用するには、次のコマンドを入力します。

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   次の例は、既存のSnapshotに保持期間を適用します。

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

既存のポリシーの変更による長期保持の適用

SnapMirror関係では、ミラーバックアップポリシールールに保持期間を設定できます。デスティネーションボリュームでSnapshotロックが有効になっている場合は、デスティネーションにレプリケートされたSnapshotに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、有効期限を過ぎていないSnapshotは、保持数を超えても保持されます。

ONTAP 9.14.1以降では、Snapshotの長期保持を設定するルールを追加することで、既存のSnapMirrorポリシーを変更できます。このルールは、SnapLockヴォールトデスティネーションとSnapLock SnapMirror以外のデスティネーションボリュームのデフォルトのボリューム保持期間を上書きするために使用されます。

1. 既存のSnapMirrorポリシーにルールを追加します。

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   次の例では、「lockvault」という既存のポリシーに6カ月の保持期間を適用するルールを作成します。

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

   の詳細については `snapmirror policy add-rule`、を"ONTAPコマンド リファレンス"参照してくださ

い。

整合グループ

ONTAPコンシステンシーグループについて学ぶ

整合グループは、1つのユニットとして管理されるボリュームの集まりです。ONTAPでは、整合グループを使用することで、複数のボリュームにまたがるアプリケーションワークロードの管理が容易になり、保護が保証されます。

整合グループを使用すると、ストレージ管理を簡易化できます。20個のLUNにまたがる重要なデータベースがあるとします。LUNを個別に管理することも、LUNを単一のデータセットとして扱い、単一の整合グループに編成することもできます。

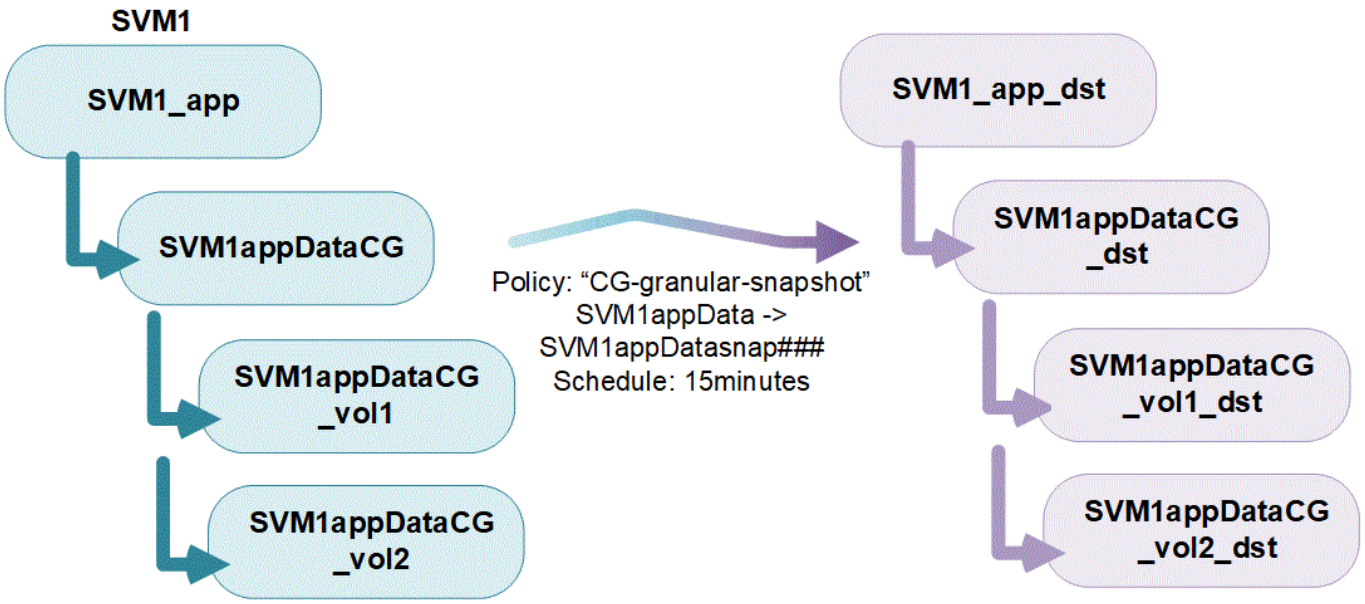
コンシステンシグループを使用すると、アプリケーションワークロードの管理が容易になり、ローカルおよびリモートの保護ポリシーを簡単に設定できます。また、ボリュームのコレクションのある時点における、クラッシュコンシステントまたはアプリケーションコンシステントなスナップショットを同時に作成できます。整合グループのSnapshotを使用すると、アプリケーションワークロード全体をリストアできます。

整合グループの詳細

整合グループは、プロトコル（NAS、SAN、NVMe）に関係なく任意のFlexVol をサポートし、ONTAP REST APIまたは* Storage > Consistency Groups *メニュー項目でSystem Managerから管理できます。ONTAP 9 14.1以降では、ONTAP CLIを使用して整合グループを管理できます。

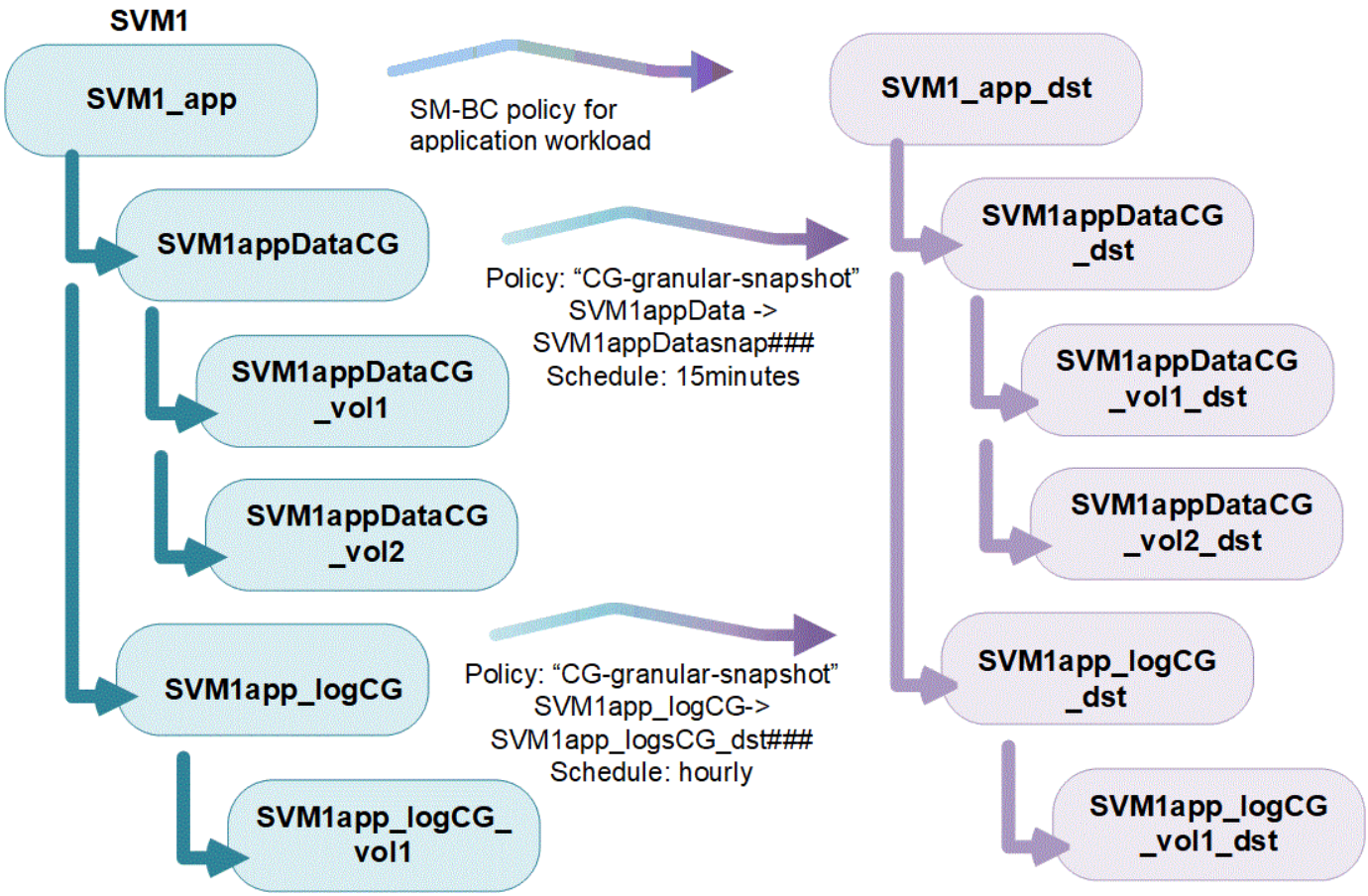
整合グループは、個 々 のエンティティ（ボリュームの集まり）として作成することも、他の整合グループで構成される階層関係として作成することもできます。個 々 のボリュームには、独自のボリューム単位のSnapshotポリシーを設定できます。また、整合性グループ全体のSnapshotポリシーを作成することもできます。整合性グループに設定できるSnapMirrorのアクティブな同期関係と共有SnapMirrorポリシーは1つだけで、整合性グループ全体をリカバリできます。

次の図は、個 々 の整合グループの使用方法を示しています。でホストされているアプリケーションのデータは `SVM1`、との `vol2`2つのボリュームにまたがっています `vol1`。整合性グループのSnapshotポリシーは、データのSnapshotを15分ごとにキャプチャします。



アプリケーションワークロードが大きいほど、複数の整合グループが必要になる場合がありますこのような場合は、階層型整合グループを作成して、1つの整合グループが親整合グループの子コンポーネントになります。親整合グループには、最大5つの子整合グループを含めることができます。個 々 の整合グループと同様に、リモートのSnapMirrorアクティブ同期保護ポリシーを整合グループの構成全体（親と子）に適用して、アプリケーションワークロードをリカバリできます。

次の例では、アプリケーションがでホストされてい `SVM1` ます。管理者が親整合グループを作成しました `SVM1_app`。このグループには、データ用と `SVM1app_logCG`ログ用の2つの子整合グループが含まれてい `SVM1appDataCG`ます。各子整合性グループには、独自のSnapshotポリシーがあります。のボリュームのSnapshotは `SVM1appDataCG`15分ごとに作成されます。のSnapshot `SVM1app_logCG`は1時間ごとに作成されます。親整合性グループ `SVM1_app`にはSnapMirrorのアクティブな同期ポリシーが設定されています。このポリシーは、災害発生時にサービスを継続できるようにデータをレプリケートします。



System.12.1以降では、ONTAP 9 ManagerとONTAP REST APIの両方で、整合グループが整合グループのメンバーをサポートクローニングおよび変更しますボリュームを追加または削除する。ONTAP 9 .12.1以降では、ONTAP REST APIは次の機能もサポートしています。

- 新しいNFS / SMBボリューム、またはNVMeネームスペースを使用して整合グループを作成する。
- 新規または既存のNFS / SMBボリュームまたはNVMeネームスペースを既存の整合性グループに追加する。

ONTAP REST APIの詳細については、を参照してください "ONTAP REST APIのリファレンスドキュメント"。

整合グループの監視

ONTAP 9 .13.1以降では、整合グループで容量とパフォーマンスをリアルタイムおよび履歴で監視し、アプリケーションと個 々 の整合グループのパフォーマンスに関する分析情報を提供します。

監視データは5分ごとに更新され、最長1年間保持されます。次の指標を追跡できます。

- パフォーマンス：IOPS、レイテンシ、スループット
- 容量：サイズ、使用済み論理容量、使用可能

監視データは、System Managerの整合グループメニューの[***Overview**]タブで表示するか、REST APIで要求することで表示できます。ONTAP 9 .14.1以降では、コマンドを使用して、CLIで整合グループの指標を表示できます `consistency-group metrics show`。の詳細については `consistency-group metrics show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP 9.13.1では、REST APIを使用してのみ過去の指標を取得できます。ONTAP 9.14.1以降では、System Managerでも過去の指標を使用できます。

整合グループの保護

整合グループを使用すると、アプリケーションと整合性のある保護が実現し、複数のボリュームやLIF間でデータの整合性が確保されます。整合性グループのSnapshotを作成する場合は、整合性グループに「フェンシング」が確立されます。フェンシングは、Snapshot処理が完了するまでI/Oキューを開始し、整合グループ内のすべてのエンティティでデータのポイントインタイム整合性を確保します。フェンシングによって、スケジュールされたSnapshotポリシーやSystem ManagerでのSnapshotの作成など、Snapshotの作成処理中に一時的にレイテンシが急上昇する可能性があります。REST APIとCLIのコンテキストの詳細については"ONTAP REST APIのドキュメント"、およびを"ONTAPコマンド リファレンス"参照してください。

コンシステンシ・グループでは'

- Snapshotポリシー
- SnapMirrorアクティブ同期
- [mcc] （ONTAP 9.11.1以降）
- SnapMirror非同期 （ONTAP 9.13.1以降）
- "SVMディザスタリカバリ" （ONTAP 9.14.1以降）

整合グループを作成しても、保護は自動的に有効になりません。ローカルとリモートの保護ポリシーは、整合グループの作成時または作成後に設定できます。

コンシステンシグループに保護を設定するには、を参照してください"整合グループの保護"。

リモート保護を使用するには、の要件を満たしている必要がありますSnapMirrorアクティブ同期。

NASアクセス用にマウントされたボリュームでは、SnapMirrorのアクティブな同期関係を確立できません。

整合グループに対する複数管理者の検証のサポート

ONTAP 9 .16.1以降では、整合グループでマルチ管理者検証（MAV）を使用して、整合グループの作成、変更、削除などの特定の処理を、指定した管理者からの承認後にのみ実行できるようにすることができます。これにより、侵害された管理者、悪意のある管理者、または経験の浅い管理者が既存の設定に望ましくない変更を加えることを防止できます。

"詳細"

MetroCluster構成の整合グループ

ONTAP 9 .11.1以降では、MetroCluster構成内のクラスタに新しいボリュームを使用して整合グループをプロビジョニングできます。これらのボリュームはミラーされたアグリゲートでプロビジョニングされます。

プロビジョニングが完了したら、整合グループに関連付けられているボリュームを、ミラーされたアグリゲートとミラーされていないアグリゲートの間で移動できます。そのため、整合性グループに関連付けられたボリュームは、ミラーされたアグリゲート、ミラーされていないアグリゲート、またはその両方に配置できます。整合性グループに関連付けられているボリュームを含むミラーされたアグリゲートを、ミラーされていないア

グリゲートに変更できます。同様に、整合グループに関連付けられているボリュームを含むミラーされていないアグリゲートを変更して、ミラーリングを有効にすることができます。

ミラーされたアグリゲートに配置された整合性グループに関連付けられているボリュームとSnapshotがリモートサイト（サイトB）にレプリケートされます。サイトBのボリュームの内容によって整合グループの書き込み順序が保証されるため、災害発生時にサイトBからリカバリできます。ONTAP 9.11.1以降を実行しているクラスタでは、REST APIおよびSystem Managerを使用して整合グループのSnapshotにアクセスできます。ONTAP 9.14.1以降では、ONTAP CLIを使用してスナップショットにアクセスすることもできます。

整合性グループに関連付けられているボリュームの一部またはすべてがミラーされていないアグリゲートに配置されていて、そのアグリゲートに現在アクセスできない場合、整合性グループに対するGETまたはDELETE処理はローカル ボリュームまたはホスティング アグリゲートがオフラインであるかのように動作します。

レプリケーション用の整合性グループ設定

サイトBでONTAP 9.10.1以前が実行されている場合は、整合性グループに関連付けられているボリュームのうち、ミラーされたアグリゲートにあるボリュームだけがサイトBにレプリケートされます。整合性グループの設定がレプリケートされるのは、両方のサイトでONTAP 9.11.1以降が実行されている場合のみです。サイトBをONTAP 9.11.1にアップグレードすると、サイトAの整合性グループのうち、関連付けられているボリュームがすべてミラーされたアグリゲートに配置されている整合性グループのデータが、サイトBにレプリケートされます。

> ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。

アップグレード時の考慮事項

10.1以降にアップグレードすると、**ONTAP 9 .8**および**9.9.1**で**SnapMirror**アクティブ同期（以前の**SnapMirror**ビジネス継続性）で作成された整合グループが自動的にアップグレードされ、**System Manager**の**[**ストレージ**]>[**整合グループ**]**または**ONTAP ONTAP 9 API**で管理できるようになり**"SnapMirror**アクティブ同期のアップグレードとリバートに関する考慮事項**"**ます。**ONTAP 9 .8**または**9.9.1**からのアップグレードの詳細については、を参照してください。

REST APIで作成された整合グループSnapshotは、System Managerの整合グループインターフェイスおよび整合グループREST APIエンドポイントを使用して管理できます。ONTAP 9.14.1以降では、ONTAP CLIでも整合グループSnapshotを管理できます。

> ONTAPIコマンドで作成されたSnapshot `cg-start`で、 `cg-commit`整合性グループのSnapshotとしては認識されないため、System Managerの整合性グループインターフェイスまたはONTAP REST APIの整合性グループエンドポイントから管理することはできません。ONTAP 9.14.1以降では、SnapMirror非同期ポリシーを使用している場合、これらのSnapshotをデスティネーションボリュームにミラーリングできます。詳細については、を参照してください SnapMirror非同期の設定。

リリースごとにサポートされる機能

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9 12.1	ONTAP 9.11.1	ONTAP 9 10.1
カイソウセイクルウフ	✓	✓	✓	✓	✓	✓	✓
Snapshotによるローカル保護	✓	✓	✓	✓	✓	✓	✓
SnapMirrorアクティブ同期	✓	✓	✓	✓	✓	✓	✓
MetroClusterのサポート	✓	✓	✓	✓	✓	✓	
2フェーズコミット（REST APIのみ）	✓	✓	✓	✓	✓	✓	
アプリケーションタグとコンポーネントタグ	✓	✓	✓	✓	✓		
クローン整合グループ	✓	✓	✓	✓	✓		
ボリュームの追加と削除	✓	✓	✓	✓	✓		
新しいNASボリュームでCGを作成する	✓	✓	✓	✓	REST APIのみ		
新しいNVMeネームスペースでCGを作成	✓	✓	✓	✓	REST APIのみ		
子整合性グループ間でのボリュームの移動	✓	✓	✓	✓			
コンシステンシグループジオメトリの変更	✓	✓	✓	✓			
監視	✓	✓	✓	✓			
マルチ管理者認証	✓						
SnapMirror非同期（単一の整合グループのみ）	✓	✓	✓	✓			
SVMディザスタリカバリ（単一の整合グループのみ）	✓	✓	✓				
CLIのサポート	✓	✓	✓				

整合グループに関する詳細情報

関連情報

- "ONTAP自動化に関するドキュメント"
- SnapMirrorアクティブ同期
- SnapMirror非同期ディザスタリカバリの基本
- "MetroClusterのドキュメント"
- "マルチ管理者認証"
- "ONTAPコマンド リファレンス"

ONTAP整合性グループの制限について学ぶ

整合グループを計画および管理する場合は、クラスタと親整合グループまたは子整合グループの両方の範囲でオブジェクトの制限を考慮してください。

テキヨウセイケン

次の表に、整合グループの制限を示します。SnapMirrorのアクティブな同期を使用する整合グループには別々 の制限が適用されます。詳細については、を参照してください "SnapMirrorアクティブ同期の制限"。

制限	適用範囲	最小	最大
整合性グループの数	クラスタ	0	クラスタ内の最大ボリューム数と同じ*
親整合性グループの数	クラスタ	0	クラスタの最大ボリューム数と同じ

個々の整合性グループと親整合性グループの数	クラスタ	0	クラスタの最大ボリューム数と同じ
整合性グループ内のボリューム数	単一の整合グループ	1個のボリューム	80ボリューム
非同期SnapMirrorを使用する整合性グループ内のボリューム数	単一の整合グループ	1個のボリューム	• ONTAP 9.15.1以降：ボリューム×80 • ONTAP 9.13.1および9.14.1：16個のボリューム
親整合性グループの子内のボリューム数	親整合グループ	1個のボリューム	80ボリューム
子整合性グループ内のボリューム数	子整合グループ	1個のボリューム	80ボリューム
親整合グループ内の子整合グループの数	親整合グループ	1個の整合グループ	5つの整合グループ
整合性グループが存在するSVMディザスタリカバリ関係の数（ONTAP 9 14.1以降で使用可能）	クラスタ	0	32

｛asterisk｝ SnapMirror非同期が有効になっている最大50個の整合グループをクラスタでホストできます。

強制されていない制限

整合性グループでサポートされる最小Snapshotスケジュールは30分です。これは"FlexGroupボリユウムテノテスト"、が整合グループと同じSnapshotインフラを共有するに基づいています。

単一の**ONTAP**コンシステンシーグループを構成する

整合グループは、既存のボリューム、または新しいLUNまたはボリュームを使用して作成できます（ONTAPのバージョンによって異なります）。ボリュームまたはLUNを関連付けることができる整合グループは一度に1つだけです。

タスクの内容

- ONTAP 9 .10.1~9.11.1では、整合グループのメンバーボリュームを作成後に変更することはできません。

  ONTAP 9 12.1以降では、整合グループのメンバーボリュームを変更できます。このプロセスの詳細については、を参照してください整合グループの変更。

- ONTAP 9.17.1 以降では、NVMe プロトコルを選択して、 SnapMirrorアクティブ同期構成で VMware ワークロードの NVMe サブシステムにホストをマッピングできます。

新しい**LUN**またはボリュームを含む整合グループを作成する

LUN.10.1~9.12.1では、新しいONTAP 9を使用して整合グループを作成できます。ONTAP 9 .13.1以降では、新しいNVMeネームスペースまたは新しいNASボリュームを使用した整合グループの作成もサポートされま

す。（これは、ONTAP 9.12.1以降のONTAP REST APIでもサポートされています）。

システムマネージャ（**ONTAP 9.16.1**以前）

手順

1. Storage > Consistency groups * を選択します。
2. [+ Add]*を選択し、ストレージオブジェクトのプロトコルを選択します。

   ONTAP 9.10.1~9.12.1では、新しいストレージオブジェクトの唯一のオプションは新しい**LUN**を使用するです。.13.1以降では、新しいONTAP 9ネームスペースと新しいNASボリュームを使用した整合グループの作成がサポートされます。

3. 整合グループに名前を付けます。ボリュームまたはLUNの数と各ボリュームまたはLUNの容量を指定します。
   a. アプリケーションタイプ: ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられますの一貫性のタグ付けの詳細については、をアプリケーションタグとコンポーネントタグ参照してください。リモート保護ポリシーを使用して整合グループを作成する場合は、* other *を使用する必要があります。
   b. [**New LUNs**]の場合：ホストオペレーティングシステムとLUN形式を選択します。ホストイニシエータ情報を入力します。
   c. [**New NAS volumes**]の場合：SVMのNAS構成に基づいて、適切なエクスポートオプション（NFSまたはSMB/CIFS）を選択します。
   d. [**New NVMe Namespaces**]の場合：ホストオペレーティングシステムとNVMeサブシステムを選択します。
4. 保護ポリシーを設定したり、子コンシステンシグループを追加したり、アクセス権限を追加したりするには、*[その他のオプション]*を選択します。
5. [保存（ Save ）] を選択します。
6. メインの整合グループメニューに戻って整合グループが作成されたことを確認します。このメニューは、ジョブの完了後に表示されます。保護ポリシーを設定した場合は、該当するポリシー（リモートまたはローカル）の下に緑の盾が表示され、その保護ポリシーが適用されていることがわかります。

システムマネージャ（**ONTAP 9.17.1**以降）

手順

1. *保護 > 一貫性グループ*を選択します。
2. [+ Add]*を選択し、ストレージオブジェクトのプロトコルを選択します。
3. 整合性グループに名前を付けます。ボリュームまたはLUNの数とボリュームまたはLUNあたりの容量を指定します。アプリケーションの種類: アプリケーションの種類を選択します。値が選択されていない場合、整合性グループにはデフォルトでその他が割り当てられます。整合タグの一貫性についての詳細は以下をご覧くださいアプリケーションタグとコンポーネントタグ。 リモート保護ポリシーを使用して整合性グループを作成する場合は、「その他」を使用する必要があります
   a. [**New LUNs**]の場合：ホストオペレーティングシステムとLUN形式を選択します。ホストイニシエータ情報を入力します。
   b. [**New NAS volumes**]の場合：SVMのNAS構成に基づいて、適切なエクスポートオプション（NFSまたはSMB/CIFS）を選択します。
   c. [**New NVMe Namespaces**]の場合：ホストオペレーティングシステムとNVMeサブシステムを選択します。

4. 保護ポリシーを設定したり、子コンシステンシグループを追加したり、アクセス権限を追加したりするには、*[その他のオプション]*を選択します。
5. [保存（ Save ）] を選択します。
6. メインの整合グループメニューに戻って整合グループが作成されたことを確認します。このメニューは、ジョブの完了後に表示されます。保護ポリシーを設定した場合は、該当するポリシー（リモートまたはローカル）の下に緑の盾が表示され、その保護ポリシーが適用されていることがわかります。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して、新しいボリュームを含む新しい整合グループを作成できます。パラメータは、ボリュームがSAN、NVMe、NFSのいずれであるかによって異なります。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

NFSボリュームを使用した整合性グループの作成

1. 整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

SANボリュームを使用した整合性グループの作成

1. 整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

NVMeネームスペースを含む整合性グループを作成する

1. 整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

の詳細については `consistency-group create`、を"ONTAPコマンド リファレンス"参照してください。

終わったら

1. コマンドを使用して、整合グループが作成されたことを確認します `consistency-group show`。

の詳細については `consistency-group show`、を"ONTAPコマンド リファレンス"参照してください。

既存のボリュームを含む整合グループを作成する

既存のボリュームを使用して整合グループを作成できます。

システムマネージャ（**ONTAP 9.16.1**以前）

手順

1. Storage > Consistency groups * を選択します。
2. 「+追加」を選択し、既存のボリュームを使用する*を選択します。
3. 整合グループに名前を付け、Storage VMを選択します。
   a. アプリケーションタイプ: ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられますの一貫性のタグ付けの詳細については、をアプリケーションタグとコンポーネントタグ参照してください。整合性グループにSnapMirrorアクティブな同期関係がある場合は、* other *を使用する必要があります。

   ⓘ ONTAP 9.15.1より前のバージョンのONTAPでは、SnapMirrorアクティブ同期をSnapMirrorビジネス継続性と呼びます。

4. 対象に含める既存のボリュームを選択します。整合グループにまだ含まれていないボリュームのみが選択可能になります。

   ⓘ 既存のボリュームを含む整合グループを作成する場合、整合グループではFlexVolボリュームがサポートされます。SnapMirror同期関係またはSnapMirror非同期関係が設定されたボリュームは、整合グループに追加できますが、整合グループに対応していません。整合グループでは、S3バケットまたはSVMDR関係を使用するStorage VMはサポートされません。

5. [保存（ Save ）] を選択します。
6. ONTAPジョブの完了後に表示されるメインの整合グループメニューに戻って、整合グループが作成されたことを確認します。保護ポリシーを選択した場合は、メニューから整合グループを選択して、保護ポリシーが適切に設定されていることを確認します。保護ポリシーを設定した場合は、該当するポリシー（リモートまたはローカル）の下に緑の盾が表示されているときに適用されていることがわかります。

CLI

ONTAP 9 14.1以降では、ONTAP CLIを使用して、既存のボリュームを含む整合グループを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. コマンドを実行し `consistency-group create`ます。 `-volumes`パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume <volumes>
```

の詳細については `consistency-group create`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用して、整合グループを表示し `consistency-group show`ます。

   の詳細については `consistency-group show`、を"ONTAPコマンド リファレンス"参照してください。

次のステップ

- 整合グループの保護
- 整合グループの変更
- 整合グループのクローニング

階層型ONTAPコンシステンシーグループを構成する

階層整合グループを使用すると、複数のボリュームにまたがる大規模なワークロードを管理できます。作成した親整合グループは、子整合グループの傘として機能します。

階層整合グループの親には、最大5つの個別の整合グループを含めることができます。階層型整合性グループは、整合性グループまたは個 々 のボリューム間で異なるローカルSnapshotポリシーをサポートできます。リモート保護ポリシーを使用する場合は、階層整合グループ全体（親と子）に適用されます。

ONTAP 9 .13.1以降では、およびを子整合グループ間でボリュームを移動します使用できますコンシステンシグループの形状を変更します。

整合グループのオブジェクト制限については、を参照してください整合性グループのオブジェクトの制限。

新しいLUNまたはボリュームを含む階層整合グループを作成する

階層整合グループを作成する場合は、新しいLUNを追加できます。ONTAP 9 .13.1以降では、新しいNVMeネームスペースとNASボリュームも使用できます。

System Manager

手順

1. Storage > Consistency groups * を選択します。
2. [+ Add]*を選択し、ストレージオブジェクトのプロトコルを選択します。

   ONTAP 9.10.1~9.12.1では、新しいストレージオブジェクトの唯一のオプションは新しい**LUN**を使用するです。.13.1以降では、新しいONTAP 9ネームスペースと新しいNASボリュームを使用した整合グループの作成がサポートされます。

3. 整合グループに名前を付けます。ボリュームまたはLUNの数と各ボリュームまたはLUNの容量を指定します。
   a. アプリケーションタイプ: ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられますの一貫性のタグ付けの詳細については、をアプリケーションタグとコンポーネントタグ参照してください。リモート保護ポリシーを使用する場合は、*[その他]*を選択する必要があります。
4. ホストオペレーティングシステムとLUNの形式を選択します。ホストイニシエータ情報を入力します。
   a. [**New LUNs]**の場合：ホストオペレーティングシステムとLUN形式を選択します。ホストイニシエータ情報を入力します。
   b. [**New NAS volumes]**の場合：SVMのNAS構成に基づいて、適切なエクスポートオプション（NFSまたはSMB/CIFS）を選択します。
   c. [**New NVMe Namespaces]**の場合：ホストオペレーティングシステムとNVMeサブシステムを選択します。
5. 子整合グループを追加するには、**[**その他のオプション**]***を選択し、+子整合グループを追加*を選択します。
6. パフォーマンスレベル、LUNまたはボリュームの数、およびLUNまたはボリュームあたりの容量を選択します。使用しているプロトコルに基づいて、適切なエクスポート設定またはオペレーティングシステム情報を指定します。
7. 必要に応じて、ローカルSnapshotポリシーを選択し、アクセス権限を設定します。
8. 最大5つの子整合性グループについて、同じ手順を繰り返します。
9. [保存（ Save ）] を選択します。
10. ONTAPジョブが完了すると表示されるメインの整合グループメニューに戻って、整合グループが作成されたことを確認します。保護ポリシーを設定する場合は、該当するポリシー（remoteまたはlocal）の下にチェックマークの付いた緑色の盾が表示されていることを確認します。

CLI

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

CLIで新しいボリュームを含む階層整合グループを作成する場合は、子整合グループをそれぞれ個別に作

成する必要があります。

ステップ

1. コマンドを使用して、新しい整合グループを作成し `consistency-group create`ます。

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
   -count <number_of_volumes> -size <size>
   ```

2. CLIのプロンプトが表示されたら、新しい親整合グループの作成を確認します。と入力し `y`ます。
3. 必要に応じて、手順1を繰り返して子整合グループをさらに作成します。

   の詳細については `consistency-group create`、を"ONTAPコマンド リファレンス"参照してください。

既存のボリュームを含む階層整合性グループを作成する

既存のボリュームを階層整合グループにまとめることができます。

System Manager

手順

1. Storage > Consistency groups * を選択します。
2. 「+追加」を選択し、既存のボリュームを使用する*を選択します。
3. Storage VMを選択します。
4. 対象に含める既存のボリュームを選択します。整合グループにまだ含まれていないボリュームのみが選択可能になります。
5. 子コンシステンシグループを追加するには、 * + 子コンシステンシグループの追加 * を選択します。必要な整合グループを作成します。この整合グループには、自動的にという名前が付けられます。
   a. コンポーネントタイプ: ONTAP 9.12.1以降を使用している場合は、「データ」、「ログ」、または「その他」のコンポーネントタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられますの一貫性のタグ付けの詳細については、をアプリケーションタグとコンポーネントタグ参照してください。リモート保護ポリシーを使用する場合は、* other *を使用する必要があります。
6. 既存のボリュームを各整合グループに割り当てます。
7. 必要に応じて、ローカルSnapshotポリシーを選択します。
8. 最大5つの子整合性グループについて、同じ手順を繰り返します。
9. [保存（ Save ）] を選択します。
10. ONTAPジョブが完了すると表示されるメインの整合グループメニューに戻って、整合グループが作成されたことを確認します。保護ポリシーを選択した場合は、メニューから整合グループを選択して、保護ポリシーが適切に設定されていることを確認します。適切なポリシータイプの下にチェックマークが付いた緑色の盾が表示されます。

CLI

ONTAP 9 14.1以降では、CLIを使用して階層整合グループを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. 新しい親整合グループをプロビジョニングし、新しい子整合グループにボリュームを割り当てます。

   ```
   consistency-group create -vserver <svm_name> -consistency-group
   <child_consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volumes <volume_names>
   ```

2. と入力して `y`、新しい親整合グループと子整合グループの作成を確定します。

   の詳細については `consistency-group create`、を"ONTAPコマンド リファレンス"参照してください。

次のステップ

- 整合グループのジオメトリの変更
- 整合グループの変更
- 整合グループの保護

ONTAPコンシステンシグループを保護する

整合グループを使用すると、複数のボリュームにまたがるSAN、NAS、NVMeアプリケーションに対して、ローカルとリモートの保護を簡単に管理できます。

整合グループを作成しても、保護は自動的に有効になりません。保護ポリシーは、コンシステンシグループの作成時または作成後に設定できます。次のコマンドを使用して整合グループを保護できます。

- ローカルSnapshot
- SnapMirrorアクティブ同期（9.15.1より前のバージョンのONTAPではSnapMirrorビジネス継続性と呼ばれます）
- MetroCluster（9.11.1以降）
- SnapMirror非同期（9.13.1以降）
- 非同期SVMディザスタ リカバリ（9.14.1以降）

ネストされた整合性グループを使用している場合は、親整合性グループと子整合性グループに別々の保護ポリシーを設定できます。

ONTAP 9 .11.1以降では、整合グループが提供されます2フェーズの整合性グループSnapshotの作成。2フェーズのスナップショット操作は事前チェックを実行し、スナップショットが正常にキャプチャされることを確認します。

リカバリは、整合グループ全体、階層構成の単一の整合グループ、または整合グループ内の個 々 のボリュームに対して実行できます。リカバリを実行するには、リカバリする整合性グループを選択し、Snapshotタイプを選択してから、リストアのベースとなるSnapshotを特定します。このプロセスの詳細については、を参照してください"以前のSnapshotからボリュームをリストアする"。

ローカル**Snapshot**ポリシーを設定する

ローカルSnapshot保護ポリシーを設定すると、整合性グループ内のすべてのボリュームにまたがるポリシーを作成できます。

タスクの内容

整合性グループでサポートされる最小Snapshotスケジュールは30分です。これは"FlexGroupホリユウムテノテスト"、が整合グループと同じSnapshotインフラを共有するに基づいています。

System Manager

手順

1. Storage > Consistency groups * を選択します。
2. [整合グループ]メニューから、作成した整合グループを選択します。
3. コンシステンシ・グループの概要ページの右上にある * 編集 * を選択します
4. スナップショットのスケジュール **(**ローカル**)** の横にあるボックスをオンにします。
5. Snapshot ポリシーを選択します。新しいカスタムポリシーを設定するには、を参照してください"カスタムのデータ保護ポリシーを作成する"。
6. [保存（ Save ）] を選択します。
7. 整合性グループの概要メニューに戻ります。[Snapshots（Local）]*の左側の列で、の横に「protected」と表示されます。

CLI

ONTAP 9 14.1以降では、CLIを使用してコンシステンシグループの保護ポリシーを変更できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

ステップ

1. 次のコマンドを実行して、保護ポリシーを設定または変更します。

   子整合性の保護ポリシーを変更する場合は、パラメータを使用して親整合性グループを指定する必要があります `-parent-consistency-group` *`parent_consistency_group_name`*。

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

オンデマンドスナップショットを作成します

通常のスケジュールされたポリシー以外で整合性グループのSnapshotを作成する必要がある場合は、オンデマンドでSnapshotを作成できます。

System Manager

手順

1. **>**[整合グループ]*に移動します。
2. オンデマンドSnapshotを作成する整合性グループを選択します。
3. タブに切り替えて、+追加*を選択します。
4. 名前*とSnapMirrorラベル*を指定してください。[整合性]のドロップダウンメニューで、**[**アプリケーション整合性**]***または[クラッシュ整合性]*を選択します。
5. [保存（ Save ）] を選択します。

CLI

ONTAP 9.14.1以降では、CLIを使用して整合性グループのオンデマンドSnapshotを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

ステップ

1. Snapshotを作成します。

   デフォルトでは、Snapshotタイプはcrash-consistentです。オプションのパラメータを使用すると、Snapshotタイプを変更できます `-type`。

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

2フェーズのコンシステンシ・グループ・スナップショットの作成

ONTAP 9.11.1以降では、整合グループ（CG）Snapshot作成の2段階のコミットがサポートされます。この2段階では、Snapshotをコミットする前に事前確認が実行されます。この機能は、ONTAP REST APIでのみ使用できます。

2フェーズCG Snapshotの作成はSnapshotの作成にのみ使用でき、整合性グループのプロビジョニングや整合性グループのリストアには使用できません。

2フェーズのCG Snapshotでは、Snapshot作成プロセスが2つのフェーズに分割されます。

1. 最初のフェーズでは、APIが事前確認を実行し、スナップショットの作成をトリガーします。最初のフェーズには、スナップショットが正常にコミットされるまでの時間を指定するタイムアウトパラメータが含まれています。
2. フェーズ1の要求が正常に完了した場合は、最初のフェーズから指定した間隔内に第2フェーズを呼び出して、適切なエンドポイントにスナップショットをコミットできます。

開始する前に

- 2フェーズCG Snapshot作成を使用するには、クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- 整合性グループインスタンスで一度にサポートされる整合性グループのSnapshot処理のアクティブな呼び出しは、1フェーズでも2フェーズでも1回だけです。別の処理の実行中にSnapshot処理を開始しようとすると、エラーになります。
- Snapshotの作成を実行するときに、オプションのタイムアウト値として5~120秒を設定できます。タイムアウト値を指定しない場合、処理はデフォルトの7秒でタイムアウトします。APIで、パラメータを使用してタイムアウト値を設定し `action_timeout`ます。CLIでは、フラグを使用し `-timeout`ます。

手順

REST APIまたはONTAP 9.14.1以降のONTAP CLIを使用して、2フェーズのスナップショットを作成できます。この処理はSystem Managerではサポートされていません。

> APIを使用してスナップショットの作成を呼び出す場合は、APIを使用してスナップショットをコミットする必要があります。CLIを使用してスナップショットの作成を呼び出す場合は、CLIを使用してスナップショットをコミットする必要があります。混在方式はサポートされていません。

CLI

ONTAP 9.14.1以降では、CLIを使用して2フェーズスナップショットを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. Snapshotを開始します。

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Snapshotが作成されたことを確認します。

   ```
   consistency-group snapshot show
   ```

3. Snapshotをコミットします。

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. スナップショットの作成を呼び出します。パラメータを使用して、整合性グループエンドポイントにPOST要求を送信します `action=start`。

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. POST要求が成功すると、出力にSnapshot UUIDが表示されます。そのUUIDを使用して、スナップショットをコミットするPATCH要求を送信します。

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

整合グループのリモート保護の設定

整合グループは、SnapMirrorのアクティブな同期機能と、ONTAP 9 .13.1以降のSnapMirror非同期機能を使用してリモート保護を提供します。

SnapMirror Active Syncによる保護の設定

SnapMirrorアクティブ同期を使用すると、整合グループに作成された整合グループのSnapshotを確実にデスティネーションにコピーできます。SnapMirrorアクティブ同期の詳細、またはCLIを使用したSnapMirrorアクティブ同期の設定方法については、を参照してくださいビジネス継続性のための保護の設定。

開始する前に

- NASアクセス用にマウントされたボリュームでは、SnapMirrorのアクティブな同期関係を確立できません。
- ソースクラスタとデスティネーションクラスタのポリシーラベルが一致している必要があります。
- SnapMirror Active Syncでは、デフォルトでSnapshotはレプリケートされません。ただし、事前定義されたポリシーにSnapMirrorラベルのルールを追加し、そのラベルでSnapshotを `AutomatedFailOver`作成する必要があります。

  このプロセスの詳細については、を参照してください"SnapMirrorのアクティブな同期で保護"。
- カスケード構成SnapMirrorアクティブ同期ではサポートされていません。
- ONTAP 9 .13.1以降では、アクティブなSnapMirrorのアクティブな同期関係を無停止で使用できます整合グループにボリュームを追加します。整合性グループにその他の変更を加える場合は、SnapMirrorのアクティブな同期関係を解除し、整合性グループを変更してから関係を再確立して再同期する必要があります。

SnapMirrorアクティブ同期をCLIで設定するには、を参照してくださいSnapMirrorのアクティブな同期で保護。

System Managerでの手順

1. が完了していることを確認し"SnapMirrorアクティブ同期を使用するための前提条件"ます。
2. Storage > Consistency groups * を選択します。
3. [整合グループ]メニューから、作成した整合グループを選択します。

4. 概要ページの右上で、 [* その他 *] 、 [* 保護 *] の順に選択します。
5. ソース側の情報はSystem Managerで自動的に入力されます。デスティネーションに適したクラスタとStorage VMを選択します。保護ポリシーを選択します。「関係の初期化」がオンになっていることを確認します。
6. [保存（ Save ）] を選択します。
7. 整合グループを初期化して同期する必要があります。メニューに戻って、同期が正常に完了したことを確認します。の横に SnapMirror（リモート）*ステータスが表示されます `Protected` 。

SnapMirror非同期の設定

ONTAP 9.13.1以降では、単一の整合グループにSnapMirror非同期保護を設定できます。ONTAP 9.14.1以降では、SnapMirror非同期を使用して、整合性グループ関係を使用してボリューム単位のSnapshotをデスティネーションクラスタにレプリケートできます。

タスクの内容

ボリューム単位のSnapshotをレプリケートするには、ONTAP 9.14.1以降を実行している必要があります。MirrorAndVaultポリシーとVaultポリシーの場合、ボリューム単位のSnapshotポリシーのSnapMirrorラベルが整合性グループのSnapMirrorポリシールールと一致している必要があります。ボリューム単位のSnapshotには、整合グループのSnapMirrorポリシーのkeep値が適用されます。keep値は、整合グループのSnapshotとは別に計算されます。たとえば、デスティネーションに2つのSnapshotを保持するポリシーがある場合、ボリューム単位のSnapshotを2つと整合グループのSnapshotを2つ作成できます。

ボリューム単位のSnapshotを使用してSnapMirror関係を再同期する場合は、フラグを指定してボリューム単位のSnapshotを保持できます `-preserve`。整合グループSnapshotよりも新しいボリューム単位のSnapshotが保持されます。整合性グループSnapshotがない場合、再同期処理でボリューム単位のSnapshotを転送することはできません。

開始する前に

- SnapMirror非同期保護は、単一の整合グループでのみ使用できます。階層型整合グループではサポートされません。階層整合グループを単一の整合グループに変換するには、を参照してください整合グループのアーキテクチャを変更。
- ソースクラスタとデスティネーションクラスタのポリシーラベルが一致している必要があります。
- アクティブなSnapMirror非同期関係では、システムを停止することはできません整合グループにボリュームを追加します。整合性グループにその他の変更を加える場合は、SnapMirror関係を解除し、整合性グループを変更してから関係を再確立して再同期する必要があります。
- SnapMirror非同期による保護が有効になっている整合グループには制限が異なります。詳細については、を参照してください 整合グループの制限。
- 複数の個 々 のボリュームに対してSnapMirror非同期保護関係を設定している場合は、既存のSnapshotを保持しながら、それらのボリュームを整合グループに変換できます。ボリュームを正常に変換するには：
  - ボリュームの共通のSnapshotが必要です。
  - 既存のSnapMirror関係を解除し、ボリュームを単一の整合グループに追加します次のワークフローを使用して関係を再同期する必要があります。

手順

1. デスティネーションクラスタで、*[ストレージ]>[整合グループ]*を選択します。
2. [整合グループ]メニューから、作成した整合グループを選択します。

3. 概要ページの右上で、 [* その他 *] 、 [* 保護 *] の順に選択します。
4. ソース側の情報はSystem Managerで自動的に入力されます。デスティネーションに適したクラスタとStorage VMを選択します。保護ポリシーを選択します。「関係の初期化」がオンになっていることを確認します。

   非同期ポリシーを選択するときは、転送スケジュールを上書きするオプションがあります。

   SnapMirror非同期整合グループでサポートされる最小スケジュール（目標復旧時点（RPO）は30分です。

5. [保存（ Save ）] を選択します。
6. 整合グループを初期化して同期する必要があります。メニューに戻って、同期が正常に完了したことを確認します。の横に SnapMirror（リモート）*ステータスが表示されます `Protected` 。

SVMディザスタリカバリの設定

ONTAP 9.14.1以降SVMディザスタリカバリでは整合グループがサポートされ、ソースクラスタからデスティネーションクラスタに整合グループ情報をミラーリングできます。

すでに整合グループが含まれているSVMでSVMディザスタリカバリを有効にする場合は、またはのSVM設定ワークフローに従ってONTAP CLIください。System Manager

アクティブで正常な状態のSVMディザスタリカバリ関係が確立されたSVMに整合性グループを追加する場合は、デスティネーションクラスタからSVMディザスタリカバリ関係を更新する必要があります。詳細については、を参照してください レプリケーション関係を手動で更新する。関係は、整合グループを拡張するたびに更新する必要があります。

制限事項

- SVMディザスタリカバリでは、階層型整合グループはサポートされません。
- SVMディザスタリカバリでは、SnapMirror非同期で保護された整合グループはサポートされません。SVMディザスタリカバリを設定する前に、SnapMirror関係を解除する必要があります。
- 両方のクラスタでONTAP 9 14.1以降が実行されている必要があります。
- 整合グループを含むSVMディザスタリカバリ構成では、ファンアウト関係はサポートされません。
- その他の制限については、を参照してください整合グループの制限。

関係を視覚化

System Managerの*[保護]>[関係]*メニューにLUNマップが表示されます。ソース関係を選択すると、ソース関係が可視化されて表示されます。ボリュームを選択すると、それらの関係をさらに掘り下げて、含まれているLUNおよびイニシエータグループ関係のリストを確認できます。この情報は、個 々 のボリュームビューからExcelブックとしてダウンロードできます。ダウンロード処理はバックグラウンドで実行されます。

関連情報

- "整合グループのクローニング"
- "スナップショットの設定"
- "カスタムのデータ保護ポリシーを作成する"

- "スナップショットからのリカバリ"
- "以前のSnapshotからボリュームをリストアする"
- "SnapMirrorアクティブ同期の概要"
- "ONTAP自動化に関するドキュメント"
- SnapMirror非同期ディザスタリカバリの基本

ONTAPコンシステンシグループのメンバーボリュームを変更する

ONTAP 9 12.1以降では、ボリュームを削除するか、ボリュームを追加（コンシステンシグループを拡張）することで、コンシステンシグループを変更できます。ONTAP 9 .13.1以降では、子整合グループが共通の親を共有している場合は、子整合グループ間でボリュームを移動できます。

整合性グループへのボリュームの追加

ONTAP 9 12.1以降では、無停止で整合グループにボリュームを追加できます。

タスクの内容

- 別の整合性グループに関連付けられているボリュームを追加することはできません。
- 整合グループでは、NAS、SAN、NVMeの各プロトコルがサポートされます。
- 調整が全体の範囲内であれば、整合グループに一度に最大16個のボリュームを追加できます。整合グループの制限
- ONTAP 9 .13.1以降では、アクティブなSnapMirrorアクティブ同期またはSnapMirror非同期保護ポリシーを使用して整合性グループに無停止でボリュームを追加できます。
- SnapMirrorアクティブな同期で保護されている整合グループにボリュームを追加すると、新しいボリュームに対してミラーリングと保護が設定されるまで、SnapMirrorアクティブな同期関係のステータスは「拡張中」に変わります。このプロセスの完了前にプライマリクラスタで災害が発生すると、整合グループはフェイルオーバー処理の一環として元の構成に戻ります。
- ONTAP 9.12.1以前では、SnapMirrorアクティブな同期関係の整合性グループにボリュームを追加できません。まず、SnapMirrorのアクティブな同期関係を削除し、整合グループを変更してから、SnapMirrorのアクティブな同期による保護をリストアする必要があります。
- ONTAP 9.12.1以降では、ONTAP REST APIで_new_または既存のボリュームを整合グループに追加できます。ONTAP REST APIの詳細については、を参照してください"ONTAP REST APIのリファレンスドキュメント"。

  ONTAP 9.13.1以降では、この機能がSystem Managerでサポートされます。

- コンシステンシグループを拡張する場合、変更前にキャプチャされたコンシステンシグループのスナップショットは部分的とみなされます。そのSnapshotに基づくリストア処理には、Snapshotのポイントインタイムの整合性グループが反映されます。
- ONTAP 9.10.1～9.11.1を使用している場合は、整合性グループを変更できません。ONTAP 9.10.1または9.11.1で整合性グループの設定を変更するには、整合性グループを削除し、希望するボリュームで新しく整合性グループを作成する必要があります。
- ONTAP 9.14.1以降では、SnapMirror非同期を使用している場合に、ボリューム単位のSnapshotをデスティネーションクラスタにレプリケートできます。SnapMirror非同期を使用して整合グループを拡張する場

合、ボリューム単位のSnapshotは、SnapMirrorポリシーがMirrorAllまたはMirrorAndVaultの場合に整合グループを拡張したあとにのみレプリケートされます。ベースライン整合性グループSnapshotよりも新しいボリューム単位のSnapshotのみがレプリケートされます。

- SVMディザスタ リカバリ関係（ONTAP 9.14.1以降でサポート）にある整合性グループにボリュームを追加する場合は、整合性グループを拡張したあとに、デスティネーション クラスタからSVMディザスタ リカバリ関係を更新する必要があります。詳細については、 レプリケーション関係を手動で更新する 。
- ONTAP 9.17.1 で NVMe を使用している場合は、整合性グループを変更できません。

例 **31.** 手順

System Manager

ONTAP 9 12.1以降では、この操作をSystem Managerで実行できます。

1. Storage > Consistency groups * を選択します。
2. 変更する整合グループを選択します。
3. 1つの整合グループを変更する場合は、* Volumes メニューの上部で More を選択し、 Expand *を選択してボリュームを追加します。

   子整合グループを変更する場合は、変更する親整合グループを特定します。[>]ボタンを選択して子整合グループを表示し、変更する子整合グループの名前の横にあるを選択します ⋮ 。このメニューから、* Expand *を選択します。
4. 整合グループに追加するボリュームを最大16個選択します。
5. [保存（ Save ）] を選択します。処理が完了したら、整合グループの*[ボリューム]*メニューで新たに追加されたボリュームを確認します。

CLI

ONTAP 9 14.1以降では、ONTAP CLIを使用して整合グループにボリュームを追加できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

既存のボリュームを追加

1. 次のコマンドを実行します。 `-volumes`パラメータには、カンマで区切ったボリュームのリストを指定できます。

   ⓘ パラメータは、整合性グループが階層関係にある場合にのみ `-parent-consistency-group`指定します。

```
consistency-group volume add -vserver svm_name -consistency-group
consistency_group_name -parent-consistency-group parent_consistency_group
-volume volumes
```

新しいボリュームの追加

新しいボリュームを追加する手順は、使用するプロトコルによって異なります。

ⓘ のみを含める `-parent-consistency-group`整合性グループが階層関係にある場合のパラメータ。

- 新しいボリュームをエクスポートせずに追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group existingParentCg -volume
```

```
volume_name -size size
```

- 新しいNFSボリュームを追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- 新しいSANボリュームを追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- 新しいNVMeネームスペースを追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

整合性グループからボリュームを削除する

整合性グループから削除したボリュームは削除されません。クラスタ内でアクティブなままです。

タスクの内容

- SnapMirrorのアクティブな同期関係またはSVMディザスタリカバリ関係の整合性グループからボリュームを削除することはできません。最初にSnapMirrorアクティブな同期関係を削除して整合性グループを変更してから、関係を再確立する必要があります。
- 削除処理後に整合グループにボリュームが含まれていない場合、その整合グループは削除されます。
- ボリュームを整合グループから削除しても、整合グループの既存のSnapshotは維持されますが、無効とみなされます。既存のSnapshotを使用して整合グループの内容をリストアすることはできません。ボリューム単位のSnapshotは引き続き有効です。
- クラスタからボリュームを削除すると、そのボリュームは整合グループから自動的に削除されます。
- ONTAP 9 .10.1または9.11.1で整合グループの設定を変更するには、整合グループを削除してから、必要なメンバーボリュームを含む新しい整合グループを作成する必要があります。
- クラスターからボリュームを削除すると、整合性グループからも自動的に削除されます。

System Manager

ONTAP 9 12.1以降では、この操作をSystem Managerで実行できます。

手順

1. Storage > Consistency groups * を選択します。
2. 変更する単一整合グループまたは子整合グループを選択します。
3. 整合グループから削除する個 々 のボリュームの横にあるチェックボックスをオンにします。
4. 「」「整合グループからボリュームを削除する」を選択します。
5. ボリュームを削除すると整合性グループのすべてのSnapshotが無効になることを理解していることを確認し、*[削除]*を選択します。

CLI

ONTAP 9 14.1以降では、CLIを使用して整合グループからボリュームを削除できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

ステップ

1. ボリュームを削除します。 `-volumes`パラメータには、カンマで区切ったボリュームのリストを指定できます。

   パラメータは、整合性グループが階層関係にある場合にのみ `-parent-consistency-group`指定します。

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

整合グループ間でのボリュームの移動

ONTAP 9 .13.1以降では、親を共有する子整合グループ間でボリュームを移動できます。

タスクの内容

- ボリュームは、同じ親整合グループにネストされた整合グループ間でのみ移動できます。
- 既存の整合性グループSnapshotは無効になり、整合性グループSnapshotとしてアクセスできなくなります。個 々 のボリュームSnapshotは有効なままです。
- 親整合グループのSnapshotは引き続き有効です。
- 子整合グループからすべてのボリュームを移動すると、その整合グループは削除されます。
- 整合グループに対する変更は、に従う必要があり整合グループの制限ます。

System Manager

ONTAP 9 12.1以降では、この操作をSystem Managerで実行できます。

手順

1. Storage > Consistency groups * を選択します。
2. 移動するボリュームを含む親整合性グループを選択します。子コンシステンシグループを検索し、[*ボリューム]メニューを展開します。移動するボリュームを選択します。
3. 移動を選択します。
4. ボリュームを新しい整合グループと既存のグループのどちらに移動するかを選択します。
   a. 既存のコンシステンシグループに移動するには、既存の子コンシステンシグループを選択し、ドロップダウンメニューからコンシステンシグループの名前を選択します。
   b. 新しいコンシステンシグループに移動するには、[*新しい子コンシステンシグループ]を選択します。新しい子整合グループの名前を入力し、コンポーネントタイプを選択します。
5. 移動を選択します。

CLI

ONTAP 9 14.1以降では、ONTAP CLIを使用して整合グループ間でボリュームを移動できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

新しい子整合性グループにボリュームを移動する

1. 次のコマンドは、指定したボリュームを含む新しい子整合グループを作成します。

   新しい整合性グループを作成するときに、新しいSnapshot、QoS、階層化ポリシーを指定できます。

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

既存の子整合性グループにボリュームを移動する

1. ボリュームを再割り当てします。 `-volumes`パラメータには、ボリューム名をカンマで区切って指定できます。

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

関連情報

- 整合グループの制限
- 整合グループのクローニング

ONTAPコンシステンシグループのジオメトリを変更する

ONTAP 9 .13.1以降では、コンシステンシグループのジオメトリを変更できます。整合グループのジオメトリを変更すると、進行中のIO処理を中断することなく、子整合グループまたは親整合グループの構成を変更できます。

コンシステンシグループジオメトリの変更は、コンシステンシグループの既存のスナップショットに影響します。詳細については、実行する形状に対する特定の修正を参照してください。

> リモート保護ポリシーが設定されている整合グループのジオメトリは変更できません。最初に保護関係を解除し、ジオメトリを変更してから、リモート保護をリストアする必要があります。

新しい子整合性グループの追加

ONTAP 9.13.1以降では、既存の親整合性グループに新しい子整合性グループを追加できます。

タスクの内容

- 親整合グループには、最大5つの子整合グループを含めることができます。その他の制限についてはを参照してください整合グループの制限。
- 1つの整合グループに子整合グループを追加することはできません。最初に整合グループを追加してから、子整合グループを追加する必要があり[プロモート]ます。
- 拡張処理の前にキャプチャされたコンシステンシグループの既存のスナップショットは、部分的なものとみなされます。そのSnapshotに基づくリストア処理には、Snapshotのポイントインタイムの整合性グループが反映されます。

例 **32.** 手順

System Manager

System.13.1以降では、ONTAP 9 Managerでこの処理を実行できます。

新しい子整合性グループの追加

1. Storage > Consistency groups * を選択します。
2. 子整合グループを追加する親整合グループを選択します。
3. 親コンシステンシグループの名前の横にある[詳細**]**を選択してから、**[**新しい子コンシステンシグループの追加*]を選択します。
4. 整合グループの名前を入力します。
5. 新しいボリュームと既存のボリュームのどちらを追加するかを選択します。
   a. 既存のボリュームを追加する場合は、既存のボリュームを選択し、ドロップダウンメニューからボリュームを選択します。
   b. 新しいボリュームを追加する場合は、[***New volumes**]を選択し、ボリュームの数とサイズを指定します。
6. 追加を選択します。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して子整合グループを追加できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

新しいボリュームを含む子整合性グループを追加する

1. 新しい整合グループを作成します。整合グループ名、ボリュームプレフィックス、ボリューム数、ボリュームサイズ、ストレージサービス、およびエクスポートポリシー名の値を指定します。

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

既存のボリュームを含む子整合性グループを追加する

1. 新しい整合グループを作成します。 `volumes`パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

子整合グループの接続解除

ONTAP 9 .13.1以降では、子整合グループを親から削除して、個別の整合グループに変換できます。

タスクの内容

- 子整合グループの接続を解除すると、親整合グループのSnapshotが無効になり、アクセスできなくなります。ボリューム単位のSnapshotは引き続き有効です。
- 個 々 の整合グループの既存のSnapshotは有効なままです。
- 接続を解除する子整合グループと同じ名前の既存の整合グループが1つある場合、この処理は失敗します。この状況が発生した場合は、整合グループの接続を解除するときに整合グループの名前を変更する必要があります。

例 **33.** 手順

System Manager

System.13.1以降では、ONTAP 9 Managerでこの処理を実行できます。

子整合グループの接続解除

1. Storage > Consistency groups * を選択します。
2. 接続を解除する子を含む親整合性グループを選択します。
3. 分離する子コンシステンシグループの横にある[詳細**]**を選択してから、**[**親からの分離*]を選択します。
4. 必要に応じて、整合グループの名前を変更し、アプリケーションタイプを選択します。
5. 切り離しを選択します。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して子整合グループの接続を解除できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

子整合グループの接続解除

1. 整合グループの接続を解除します。必要に応じて、パラメータを使用して、接続解除された整合グループの名前を変更し `-new-name`ます。

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

親整合グループの下に既存の単一の整合グループを移動する

ONTAP 9 .13.1以降では、既存の単一の整合グループを子整合グループに変換できます。移動処理中に、既存の親整合グループの下に整合グループを移動するか、新しい親整合グループを作成できます。

タスクの内容

- 親整合グループには子が4つ以下である必要があります。親整合グループには、最大5つの子整合グループを含めることができます。その他の制限についてはを参照してください整合グループの制限。
- この操作の前にキャプチャされた_parent_consistencyグループの既存のスナップショットは部分的とみなされます。これらのSnapshotの1つに基づくリストア処理には、Snapshotのポイントインタイムの整合グループが反映されます。
- 単一の整合グループの既存の整合グループSnapshotは有効なままです。

例 **34.** 手順

System Manager

System.13.1以降では、ONTAP 9 Managerでこの処理を実行できます。

親整合グループの下に既存の単一の整合グループを移動する

1. Storage > Consistency groups * を選択します。
2. 変換する整合グループを選択します。
3. [**More***]を選択してから、**[**Move under different consistency group]**を選択します。
4. 必要に応じて、整合グループの新しい名前を入力し、コンポーネントタイプを選択します。デフォルトでは、コンポーネントタイプはOtherになります。
5. 既存の親整合グループに移行するか、新しい親整合グループを作成するかを選択します。
   a. 既存の親コンシステンシグループに移行するには、既存のコンシステンシグループを選択し、ドロップダウンメニューからコンシステンシグループを選択します。
   b. 新しい親コンシステンシグループを作成するには、[*新しいコンシステンシグループ]を選択し、新しいコンシステンシグループの名前を指定します。
6. 移動を選択します。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して、親整合グループの下に1つの整合グループを移動できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

新しい親整合グループの下に整合グループを移動する

1. 新しい親整合グループを作成します。パラメータを指定する `-consistency-groups`と、既存の整合グループが新しい親に移行されます。

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

既存の整合グループの下に整合グループを移動する

1. 整合グループを移動します。

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

子整合グループを昇格する

ONTAP 9 .13.1以降では、単一の整合グループを親整合グループに昇格できます。単一の整合グループを親に昇格すると、元の単一の整合グループ内のすべてのボリュームを継承する新しい子整合グループも作成されま

す。

タスクの内容

- 子整合グループを親整合グループに変換する場合は、まず子整合グループを作成してから、次の手順を実行する必要があります[detach]。
- 整合グループの既存のSnapshotは、整合グループをプロモートしたあとも有効なままです。

System Manager

System.13.1以降では、ONTAP 9 Managerでこの処理を実行できます。

子整合グループを昇格する

1. Storage > Consistency groups * を選択します。
2. 昇格する整合性グループを選択します。
3. **More**を選択してから、**Promote to parent consistency group** を選択します。
4. 名前を入力し、子コンシステンシグループのコンポーネントタイプを選択します。
5. プロモートを選択します。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して、親整合グループの下に1つの整合グループを移動できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

子整合グループを昇格する

1. 整合グループを昇格します。このコマンドは、1つの親整合グループと1つの子整合グループを作成します。

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

親を単一の整合グループに降格

ONTAP 9 .13.1以降では、親整合グループを単一の整合グループに降格できます。親を降格すると、整合グループの階層がフラット化され、関連付けられている子整合グループがすべて削除されます。整合グループ内のすべてのボリュームは、新しい単一の整合グループに残ります。

タスクの内容

- _parent_consistencyグループの既存のスナップショットは、単一の整合性に降格したあとも有効です。その親のassociated_child_consistencyグループの既存のスナップショットは、降格時に無効になります。子整合性グループ内の個 々 のボリュームSnapshotには、引き続きボリューム単位のSnapshotとしてアクセスできます。

例 **35.** 手順

System Manager

System.13.1以降では、ONTAP 9 Managerでこの処理を実行できます。

整合グループを降格する

1. Storage > Consistency groups * を選択します。
2. 降格する親整合性グループを選択します。
3. **More**を選択してから **Demote to single consistency group** を選択します。
4. 関連付けられているすべての子整合グループが削除され、そのボリュームが新しい単一の整合グループの下に移動されることを示す警告が表示されます。降格を選択して、影響を理解していることを確認します。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して整合グループを降格できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

整合グループを降格する

1. 整合グループを降格します。オプションのパラメータを使用し `-new-name`て、整合グループの名前を変更します。

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

ONTAP整合性グループのアプリケーションとコンポーネントのタグを変更する

ONTAP 9 12.1以降では、コンシステンシグループはコンポーネントとアプリケーションのタグ付けをサポートしています。アプリケーションタグとコンポーネントタグは管理ツールであり、整合グループ内のさまざまなワークロードをフィルタして特定できます。

タスクの内容

整合グループには、次の2種類のタグがあります。

- アプリケーションタグ:個 々 のコンシステンシグループと親コンシステンシグループに適用されます。アプリケーションタグを使用して、MongoDB、Oracle、SQL Serverなどのワークロードをラベル付けできます。整合グループのデフォルトのアプリケーションタグはotherです。
- コンポーネントタグ:階層整合グループの子には、アプリケーションタグではなくコンポーネントタグがあります。コンポーネントタグのオプションは、「data」、「logs」、または「other」です。デフォルト値はOtherです。

タグは、整合グループの作成時または整合グループの作成後に適用できます。

整合性グループにSnapMirrorのアクティブな同期関係がある場合は、アプリケーションタグまたはコンポーネントタグとして* other *を使用する必要があります。

手順

System.12.1以降では、ONTAP 9 Managerを使用してアプリケーションタグとコンポーネントタグを変更できます。ONTAP 9 .14.1以降では、ONTAP CLIを使用してアプリケーションタグとコンポーネントタグを変更できます。

System Manager

1. Storage > Consistency groups * を選択します。
2. タグを変更する整合性グループを選択します。整合性グループの名前の横にあるを選択し、*[編集]* を選択し ⋮ ます。
3. ドロップダウンメニューで、適切なアプリケーションまたはコンポーネントタグを選択します。
4. [保存（ Save ）] を選択します。

CLI

ONTAP 9 .14.1以降では、ONTAP CLIを使用して、既存の整合グループのアプリケーションタグまたはコンポーネントタグを変更できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

アプリケーションタグの変更

1. アプリケーションタグは、限られた数のプリセット文字列を受け入れます。許可された文字列のリストを表示するには、次のコマンドを実行します。
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. 出力から適切な文字列を選択し、整合グループを変更します。
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

構成要素タグを修正します

1. 構成要素タイプを修正します。コンポーネントタイプには、データ、ログ、またはその他があります。SnapMirrorアクティブ同期を使用している場合は、「その他」である必要があります。
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

ONTAPコンシステンシーグループのクローンを作成する

ONTAP 9 12.1以降では、整合グループのクローンを作成して、整合グループとその内容

のコピーを作成できます。整合グループをクローニングすると、整合グループの設定、そのメタデータ（アプリケーションタイプなど）、およびすべてのボリュームとそのコンテンツ（ファイル、ディレクトリ、LUN、NVMeネームスペースなど）のコピーが作成されます。

タスクの内容

整合グループをクローニングするときは、現在の設定を使用してクローニングできますが、ボリュームの内容はそのままにすることも、既存の整合グループSnapshotに基づいてクローニングすることもできます。

整合グループのクローニングは、整合グループ全体でのみサポートされます。階層関係にある子整合グループを個別にクローニングすることはできません。クローニングできるのは、整合グループの設定全体のみです。

整合グループをクローニングしても、次のコンポーネントはクローニングされません。

- igroup
- LUNマツフ
- NVMeサフシステム
- NVMeネームスペースサブシステムマップ

開始する前に

- 整合グループをクローニングする際、ONTAP共有名を指定しないと、クローンボリューム用のSMB共有は作成されません。*ジャンクションパスを指定しないと、クローン整合グループはマウントされません。
- 整合性グループの現在のコンスティチュエントボリュームが反映されていないSnapshotに基づいて整合性グループをクローニングしようとすると、処理は失敗します。
- 整合グループをクローニングしたら、適切なマッピング処理を実行する必要があります。

  詳細については、またはNVMeネームスペースをサブシステムにマッピングするを参照してigroupを複数のLUNにマッピングください。

- 整合性グループのクローニングは、SnapMirrorのアクティブな同期関係にある整合性グループ、または関連付けられているDPボリュームではサポートされません。

System Manager

手順

1. Storage > Consistency groups * を選択します。
2. [* Consistency Group]メニューから'クローンを作成するコンシステンシ・グループを選択します
3. コンシステンシ・グループの概要ページの右上にある*クローン*を選択します
4. クローンされた新しい整合グループの名前を入力するか、デフォルトの名前をそのまま使用します。
   a. 有効にするかどうかを選択し"* シンプロビジョニング *"ます。
   b. ソースから整合グループの関連付けを解除し、そのクローン整合グループに追加のディスクスペースを割り当てる場合は、「* Split Clone *」を選択します。
5. 整合性グループを現在の状態で複製するには、[新しいスナップショットの追加] を選択します。

   Snapshotに基づいて整合グループをクローニングするには、*[既存のSnapshotを使用する]*を選択します。このオプションを選択すると、新しいサブメニューが開きます。クローニング処理のベースとして使用するSnapshotを選択します。
6. 「 * Clone * 」を選択します。
7. 「* Consistency Group *」メニューに戻り、整合グループのクローンが作成されたことを確認します。

CLI

ONTAP 9 14.1以降では、CLIとクラスタ管理者のクレデンシャルを使用して整合グループをクローニングできます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

整合グループのクローニング

1. コマンドは、 `consistency-group clone create`現在のポイントインタイムステータスで整合グループをクローニングします。Snapshotに基づいてクローニング処理を実行するには、パラメータを指定し `-source-snapshot`ます。

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

   の詳細については `consistency-group clone create`、を"ONTAPコマンド リファレンス"参照してください。

次のステップ

- igroupを複数のLUNにマッピング
- NVMeネームスペースをサブシステムにマッピングする

ONTAPコンシステンシーグループを削除する

整合グループが不要になった場合は、その整合グループを削除できます。

タスクの内容

- 整合グループを削除すると、整合グループのインスタンスが削除され、コンスティチュエントボリュームまたはLUNには影響しません。整合グループを削除しても、各ボリュームにあるSnapshotは削除されませんが、整合グループSnapshotとしてはアクセスできなくなります。ただし、Snapshotは通常のボリューム単位のSnapshotとして引き続き管理できます。
- 整合グループ内のボリュームがすべて削除されると、ONTAPは整合グループを自動的に削除します。
- 親整合グループを削除すると、関連付けられている子整合グループがすべて削除されます。
- 9.10.1~9.12.0のONTAPバージョンを使用している場合、ボリューム自体が削除された場合にのみ整合グループからボリュームを削除できます。削除された場合、ボリュームは整合グループから自動的に削除されます。ONTAP 9 12.1以降では、整合グループを削除せずに、整合グループからボリュームを削除できます。このプロセスの詳細については、を参照してください整合グループの変更。

例 **36.** 手順

System Manager

1. Storage > Consistency groups * を選択します。
2. 削除する整合性グループを選択します。
3. 整合グループの名前の横にある*[削除]*を選択します ⋮ 。

CLI

ONTAP 9 14.1以降では、CLIを使用して整合グループを削除できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

整合グループを削除する

1. 整合グループを削除します。

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirrorアクティブ同期

はじめに

ONTAP SnapMirrorアクティブ同期について学ぶ

SnapMirrorアクティブ シンク (SnapMirror Business Continuity (SM-BC) とも呼ばれる)

を使用すると、サイト全体に障害が発生した場合でもビジネス サービスが継続して機能できるようになります。このテクノロジーにより、手動による介入やカスタム スクリプトなしで、アプリケーションをシームレスにセカンダリ コピーにフェイルオーバーできます。

NetApp SnapMirror Active Sync (SM-as) は、自動フェイルオーバーを備えた、よりきめ細かく、低コストで、使いやすいアプリケーション レベルの保護を実現するように設計されています。 SnapMirrorアクティブ同期により、サイト全体の障害が発生した場合でも、ミッションクリティカルなビジネス サービスの運用を継続できます。 SnapMirrorアクティブ同期を使用すると、地理的に分散した場所にあるサイト間で、アプリケーションの複数のボリュームを（整合性グループに追加することで）同期的に複製できるようになりました。プライマリが停止した場合に自動的にセカンダリ コピーにフェイルオーバーできるため、ティア1アプリケーションのビジネス継続性を確保できます。

一部の国では、金融機関に対する規制により、企業はセカンダリ データ センターから定期的にサービスを受けることが義務付けられています。 SnapMirrorアクティブ同期は、高可用性クラスターを備えており、ビジネス継続性のためにこれらのデータセンターの切り替えを可能にします。

ONTAP 9.9.1 以降で利用可能なSnapMirrorアクティブ シンクは、 AFFおよびオールフラッシュ SAN アレイ (ASA) クラスタでサポートされます。プライマリ クラスタとセカンダリ クラスタは同じタイプ（ ASA、 ASA r2、またはAFF）である必要があります。 SnapMirrorアクティブ シンクは、iSCSI または FCP LUN または NVMe 名前空間を持つアプリケーションを保護します。

SnapMirrorアクティブ同期は、対称構成と非対称構成の両方をサポートします。対称アクティブ/アクティブのサポートは、 ONTAP 9.15.1 で導入されました。対称アクティブ/アクティブ構成では、保護された LUN の両方のコピーが双方向同期レプリケーションを使用して読み取りおよび書き込み I/O 操作を実行できるため、各 LUN コピーがローカル I/O 要求に対応できるようになります。

2024年7月以降、これまでPDFとして公開されていたテクニカルレポートの内容がONTAPの製品ドキュメントに統合されました。ONTAP SnapMirrorアクティブ同期のドキュメントに、「TR-4878：SnapMirrorアクティブ同期_」の内容が追加されました。

メリット

SnapMirror Active Syncには次のようなメリットがあります。

- ビジネスクリティカルなアプリケーションの継続的可用性：
- 重要なアプリケーションをプライマリサイトとセカンダリサイトから交互にホストできます。
- 整合グループを使用して従属書き込み順序の整合性を確保し、アプリケーション管理を簡易化
- 各アプリケーションのフェイルオーバーをテストする機能。
- アプリケーションの可用性に影響を与えることなく、ミラークローンを瞬時に作成できます。
- 保護されているワークロードと保護されていないワークロードを同じONTAPクラスタに導入できる。
- LUN、NVMe 名前空間、NVMe サブシステム、またはストレージ ユニット ID は同じままなので、アプリケーションはそれらを共有仮想デバイスとして認識します。
- セカンダリクラスタを柔軟に再利用して、アプリケーションのパフォーマンスや可用性に影響を与えることなく、開発テスト、UAT、レポート作成に使用するクローンを瞬時に作成できます。

SnapMirror Active Syncを使用すると、データLUNまたはNVMeネームスペースを保護し、災害発生時にアプリケーションを透過的にフェイルオーバーしてビジネス継続性を確保できます。詳細については、 "ユースケ

ース" 。

主な概念

SnapMirrorアクティブ同期は、整合性グループを使用して、データが確実に複製されるようにします。SnapMirrorアクティブ シンクは、自動フェイルオーバーにONTAP Mediator を使用するか、 ONTAP 9.17.1 以降では Cloud Mediator を使用し、災害発生時にもデータが確実に提供されるようにします。SnapMirrorアクティブ同期の導入を計画する際は、SnapMirrorアクティブ同期とそのアーキテクチャの基本概念を理解しておくことが重要です。

非対称性と対称性

対称アクティブ/アクティブ構成では、両方のサイトがアクティブI/Oのためにローカルストレージにアクセスできます。対称アクティブ/アクティブは、VMware vMSC、Windows Failover Cluster with SQL、Oracle RACなどのクラスタ化されたアプリケーションに最適化されています。

非対称アクティブ/アクティブ構成では、セカンダリ サイトのデータは LUN、名前空間、またはストレージユニットにプロキシされます。

詳細については、を参照してください SnapMirror Active Syncアーキテクチャ。

整合グループ

AFFおよびASAシステムの場合"整合グループ" FlexVolボリュームの集合であり、ビジネス継続性を確保するために保護する必要があるアプリケーションワークロードの整合性を保証します。ASAASAシステムでは、コンシステンシグループはストレージユニットの集合です。

整合性グループの目的は、ボリュームまたはストレージユニットのコレクションのスナップショットイメージを同時に取得し、ある時点でのコレクションのクラッシュ整合性コピーを確保することです。整合性グループにより、データセットのすべてのボリュームが休止され、同じ時点でのSnapshotが作成されます。これにより、データセットをサポートするボリュームまたはストレージユニット全体にわたって、データの整合性が保たれた復元ポイントが提供されます。整合性グループはこうして従属書き込み順序の整合性を維持します。ビジネス継続性のためにアプリケーションを保護する場合は、そのアプリケーションに対応するボリュームまたはストレージユニットのグループを整合性グループに追加し、ソースとデスティネーションの整合性グループ間にデータ保護関係を確立する必要があります。ソースとデスティネーションの整合性グループには、同じ数とタイプのボリュームを含める必要があります。

コンスティチュエント

SnapMirrorアクティブ同期関係で保護されている整合性グループの一部である個々のボリューム、LUN、または NVMe 名前空間 (ONTAP 9.17.1 以降)。

ONTAP Mediator

その"ONTAP Mediator"ピア接続されたONTAPクラスタとノードのヘルス情報を受信し、両者間のオーケストレーションを行い、各ノード/クラスタが正常で稼働しているかどうかを判断します。ONTAPONTAPは、以下のヘルス情報を提供します。

- ONTAPクラスタのピアリング
- ピアONTAPクラスタノード
- 整合グループ（SnapMirrorのアクティブな同期関係でフェイルオーバーユニットを定義）。整合グループごとに次の情報が表示されます。
  - レプリケーションの状態：Uninitialized、In Sync、またはOut of Sync
  - プライマリコピーをホストするクラスタ

- 操作コンテキスト（計画的フェイルオーバーに使用）

このONTAPメディエーターの健常性情報を使用すると、クラスタで障害のタイプを区別し、自動フェイルオーバーを実行するかどうかを判断できます。ONTAPメディエーターは、両方のONTAPクラスタ（プライマリおよびセカンダリ）とともにSnapMirrorアクティブ同期クォーラムを構成する3つのメンバーの1つです。合意に達するには、クォーラムの少なくとも2つの当事者が特定の処理に同意する必要があります。

ONTAP 9.15.1以降では、どちらかのクラスタのSnapMirrorのアクティブな同期関係のステータスが表示されます。ONTAPメディエーターのステータスは、System Managerのどちらのクラスタからも監視できます。以前のリリースのONTAPでは、ソースクラスタのSnapMirrorのアクティブな同期関係のステータスが表示されていました。

ONTAPクラウドメディエーター

ONTAP Cloud Mediatorは、 ONTAP 9.17.1以降で利用できます。ONTAPONTAP Cloud Mediator は、 NetAppコンソールを使用してクラウドでホストされる点を除いて、 ONTAP Mediator と同じサービスを提供します。

計画的フェイルオーバー

SnapMirrorアクティブ同期関係でのコピーの役割を変更する手動処理。プライマリ サイトがセカンダリ サイトに、セカンダリ サイトがプライマリ サイトになります。

自動計画外フェイルオーバー（**AUFO**）

ミラー コピーへのフェイルオーバーを実行する自動処理。この処理には、プライマリ コピーが使用できないことを検出するためにONTAP Mediatorが必要です。

プライマリファーストとプライマリバイアス

SnapMirrorアクティブ同期では、ネットワークが分割された場合のI/O処理にプライマリ コピーを優先するプライマリファーストの原則が使用されます。

プライマリバイアスとは、SnapMirrorアクティブ同期で保護されたデータセットの可用性を向上させる特別なクォーラムの実装です。どちらのクラスタからもONTAP Mediatorにアクセスできない場合に、プライマリ コピーが使用可能だと、プライマリバイアスが効果を発揮します。

ONTAP 9.15.1以降では、SnapMirrorアクティブ同期でプライマリファーストとプライマリバイアスがサポートされます。プライマリ コピーはSystem Managerで指定され、REST APIおよびCLIを使用して出力されます。

非同期（**OOS**）

アプリケーションI/Oがセカンダリ・ストレージ・システムにレプリケートされていない場合は**'out of sync**と報告されます非同期ステータスは、セカンダリボリュームがプライマリ（ソース）と同期されておらず、SnapMirrorレプリケーションが実行されていないことを示します。

ミラー状態が `Snapmirrored`これは、 SnapMirror関係が確立され、データ転送が完了したことを示します。つまり、宛先ボリュームはソース ボリュームと最新の状態になっています。

SnapMirror Active Syncは自動再同期をサポートしており、コピーをInSync状態に戻すことができます。

ONTAP 9 .15.1以降では、SnapMirrorアクティブ同期がサポートされて"ファンアウト構成での自動再構成"います。

均一な構成と非均一な構成

- 均一なホストアクセスは、両方のサイトのホストが両方のサイトのストレージクラスタへのすべてのパス

に接続されていることを意味します。サイト間パスが複数の距離にわたってストレッチされている。

- **Non-uniform host access** は、各サイトのホストが同じサイトのクラスタにのみ接続されることを意味します。サイト間パスとストレッチパスは接続されません。

> 均一ホストアクセスは、すべてのSnapMirrorアクティブ同期配置でサポートされます。非均一ホストアクセスは、対称アクティブ/アクティブ配置でのみサポートされます。

RPOゼロ

RPOはRecovery Point Objective（目標復旧時点）の略で、所定の期間内に許容可能とみなされるデータ損失量を指します。RPOゼロとは、データ損失が一切許容されないことを意味します。

RTOゼロ

RTOはRecovery Time Objective（目標復旧時間）の略で、システム停止、障害、またはその他のデータ損失イベントが発生してから、アプリケーションが無停止で通常の処理に戻るまでに許容可能とみなされる時間です。RTOゼロとは、ダウンタイムが一切許容されないことを意味します。

ONTAPバージョン別の**SnapMirror**アクティブ同期構成のサポート

SnapMirror Active Sync のサポートは、 ONTAPのバージョンによって異なります。

ONTAPのバージョン	サポートされているクラスター	サポートされるプロトコル	サポートされている構成
9.17.1以降	• AFF • ASA • Cシリーズ • ASA r2	• iSCSI • FC • VMware ワークロード向け NVMe	• 非対称アクティブ/アクティブ > 非対称アクティブ/アクティブはASA r2とNVMeをサポートしていません。NVMeサポートの詳細については、以下を参照してください。"NVMeの設定、サポート、制限事項" 。 • 対称アクティブ/アクティブ

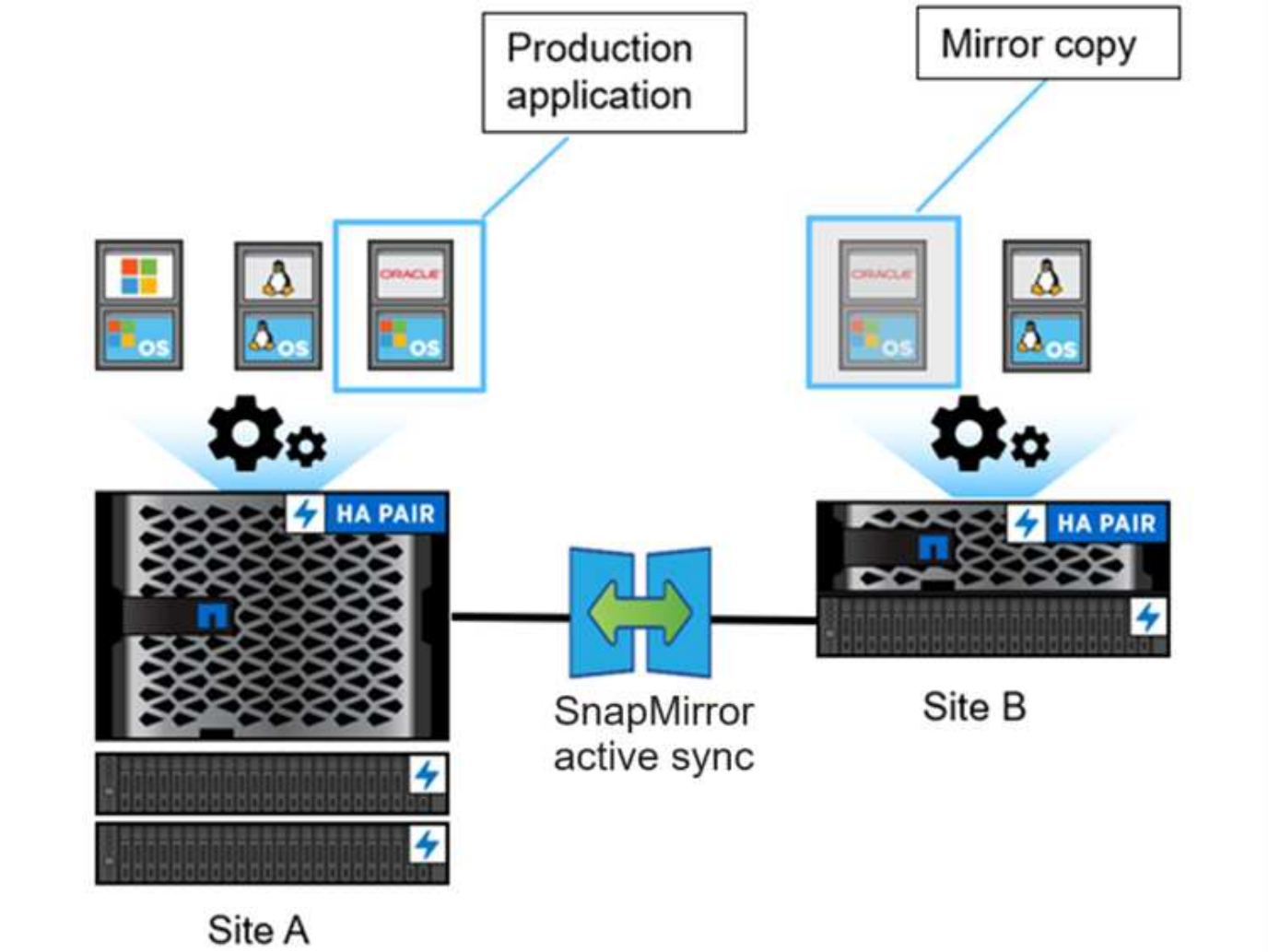
9.16.1以降	• AFF • ASA • Cシリーズ • ASA r2	• iSCSI • FC	• 非対称アクティブ/アクティブ • 対称アクティブ/アクティブ 対称アクティブ/アクティブ構成は、 ONTAP 9.16.1 以降で 4 ノード クラスタをサポートします。 ASA r2 では、2 ノード クラスタのみがサポートされます。
9.15.1以降	• AFF • ASA • Cシリーズ	• iSCSI • FC	• 非対称アクティブ/アクティブ • 対称アクティブ/アクティブ 対称アクティブ/アクティブ構成は、 ONTAP 9.15.1 で 2 ノード クラスタをサポートします。4ノード クラスタはONTAP 9.16.1 以降でサポートされます。
9.9.1以降	• AFF • ASA • Cシリーズ	• iSCSI • FC	非対称アクティブ/アクティブ

プライマリクラスタとセカンダリクラスタは同じタイプである必要があります。 "ASA" 、 "ASA r2" 、またはAFF。

ONTAP SnapMirrorアクティブ同期アーキテクチャ

SnapMirrorアクティブ同期アーキテクチャにより、アクティブなワークロードを両方のクラスタに配置し、両方のクラスタから同時にプライマリ ワークロードを処理できます。一部の国の金融機関の規制では、企業がセカンダリ データ センターからも定期的にサービスを受けられるようにする (「Tick-Tock」展開と呼ばれる) ことが求められており、 SnapMirrorアクティブ同期によってこれが可能になります。

ストレージ仮想マシン (SVM) 内の異なるボリュームからアプリケーション固有の LUN または NVMe 名前空間を整合性グループに追加することにより、ソース ストレージ システムと宛先ストレージ システム間にビジネス継続性を保護するためのデータ保護関係が作成されます。通常の運用時には、エンタープライズ アプリケーションによってプライマリ整合グループに書き込みが行われ、そのI/Oがミラー整合グループに同期的にレプリケートされます。



データ保護関係にはデータの 2 つの個別のコピーが存在するにもかかわらず、 SnapMirrorアクティブ同期は同じ LUN または NVMe 名前空間 ID を維持するため、アプリケーション ホストはこれを複数のパスを持つ共有仮想デバイスとして認識し、一度に書き込まれる LUN または NVMe 名前空間コピーは 1 つだけです。障害が発生してプライマリ ストレージ システムがオフラインになると、ONTAPはこの障害を検出し、Mediatorを使用して再確認します。ONTAPもMediatorもプライマリ サイトにpingを送信できない場合、ONTAPは自動フェイルオーバー処理を実行します。このプロセスにより、以前はフェイルオーバーのために必要だった手動による介入やスクリプトを必要とせずに、特定のアプリケーションのみをフェイルオーバーできるようになります。

その他の考慮事項：

- ビジネス継続性を目的とする保護の対象から外れた、ミラーされていないボリュームがサポートされる
- ビジネス継続性を目的として保護されているボリュームでは、他のSnapMirror非同期関係は1つのみサポートされる
- ビジネス継続性を目的とする保護では、カスケード トポロジはサポートされない

仲介者の役割

SnapMirror Active Syncは、メディエーターを使用して、 SnapMirror Active Syncコピーの受動的な監視役と

して機能します。ネットワークが分断された場合、または一方のコピーが使用できなくなった場合、SnapMirror Active Syncはメディエーターを使用して、どちらのコピーがI/O処理を継続するかを決定し、もう一方のコピーのI/O処理を停止します。オンプレミスのONTAPメディエーターに加えて、 ONTAP 9.17.1以降では、 ONTAP Cloud Mediatorをインストールすることで、クラウド環境で同様の機能を提供できます。ONTAPONTAPとONTAP Cloud Mediatorのどちらかを使用できますが、両方を同時に使用することはできません。

Mediator は、パッシブ クォーラム ウィットネスとしてSnapMirrorアクティブ同期構成で重要な役割を果たし、クォーラムの維持を保証し、障害発生時のデータ アクセスを容易にします。これは、ピア コントローラの活性状態を判断するためのコントローラの ping プロキシとして機能します。Mediatorは、スイッチオーバー処理をアクティブにトリガーしませんが、重要な機能を提供するために、ネットワーク通信の問題が発生したときに稼働しているノードがパートナーのステータスを確認できるようにします。ONTAP Mediatorは、クォーラム監視という役割の中で、ピア クラスタへの代替パスを提供します（実質的にはプロキシとして機能します）。

さらに、クォーラム プロセスの一環として、クラスタがこの情報を取得できるようにします。通信にはノード管理LIFとクラスタ管理LIFを使用します。サイト障害とインタースイッチ リンク（ISL）障害を区別するために、複数のパスを経由する冗長な接続を確立します。イベントによりクラスタがMediatorソフトウェアおよびその全ノードとの接続を失うと、そのクラスタは到達不能とみなされます。これによりアラートがトリガーされ、セカンダリサイトのミラーコンシステンシグループへの自動フェイルオーバーが有効になり、クライアントのI/Oが中断されないようになります。レプリケーション データ パスはハートビート メカニズムに依存しているため、ネットワークの不具合やイベントが一定期間以上続くと、ハートビート障害が発生し、関係が非同期状態になる可能性があります。ただし、LIFの別のポートへのフェイルオーバーなど、冗長パスがあると、ハートビートが維持され、そのような中断を防ぐことができます。

ONTAP Mediator

ONTAP Mediator は、監視対象の 2 つのONTAPクラスタとは別の 3 番目の障害ドメインにインストールされます。この環境には、次の3つの主要コンポーネントがあります。

- SnapMirrorアクティブ同期プライマリ整合性グループをホストしているプライマリONTAPクラスタ
- ミラー整合性グループをホストしているセカンダリONTAPクラスタ
- ONTAP Mediator

ONTAP Mediator は次の目的で使用されます。

- クォーラムを確立する
- 自動フェイルオーバー（AUFO）による継続的可用性
- 計画的フェイルオーバー（PFO）

ONTAP Mediator 1.7 は、ビジネス継続性のために 10 個のクラスタ ペアを管理できます。

ONTAP Mediatorを使用できない場合は、計画的フェイルオーバーや自動フェイルオーバーを実行できません。アプリケーション データは中断されることなく同期的にレプリケートされ続けるため、データ損失はゼロになります。

ONTAPクラウドメディエーター

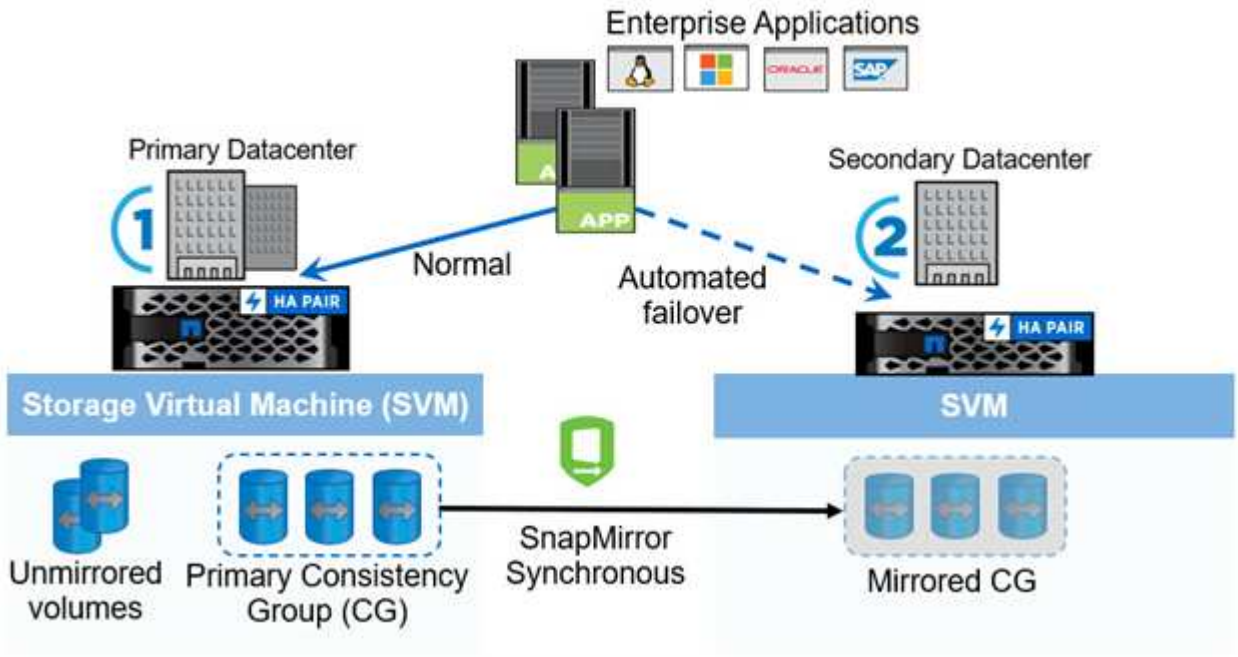
ONTAP 9.17.1 以降では、 ONTAP Cloud Mediator がNetAppコンソールでクラウドベースのサービスとして利用でき、 SnapMirror Active Sync で使用できるようになります。Mediatorと同様に、 ONTAP Cloud MediatorはSnapMirror Active Sync関係において以下の機能を提供します。

- HA またはSnapMirrorアクティブ同期メタデータ用の永続的かつ隔離されたストアを提供します。
- コントローラの稼働を維持するためのpingプロキシとして機能します。
- クォーラムの決定に役立つ同期ノード健全性クエリ機能を提供します。

ONTAP Cloud Mediator は、 NetApp Console クラウド サービスを管理の必要のない第 3 のサイトとして使用することで、 SnapMirror Active Sync の導入を簡素化します。Cloud Mediatorサービスはオンプレミスのの同じ機能を提供しますが、第3サイトの維持に伴う運用上の複雑ONTAP Mediatorと同じONTAPを軽減します。ONTAP、 ONTAP Mediatorはパッケージとして提供されており、独立した電源とネットワークインフラを備えた第3サイトで稼働するLinuxホストにインストールする必要があります。

SnapMirrorアクティブ同期操作ワークフロー

次の図は、SnapMirrorアクティブ同期の設計の概要を表しています。



次の図は、プライマリデータセンターのStorage VM（SVM）でホストされているエンタープライズアプリケーションを示しています。SVMには5つのボリュームがあり、そのうちの3つは整合グループに属しています。整合グループ内の3つのボリュームがセカンダリデータセンターにミラーリングされます。通常、すべての書き込み処理はプライマリデータセンターに対して実行されます。つまり、このデータセンターがI/O処理のソースとして機能し、セカンダリデータセンターがデスティネーションとして機能します。

プライマリ データセンターで災害が発生した場合は、ONTAPがセカンダリ データセンターをプライマリとして機能させて、すべてのI/O処理に対応させます。整合性グループ内のミラーリングされているボリュームのみが対象となります。SVM 上の他の 2 つのボリュームに関連するすべての操作は、災害イベントの影響を受けます。

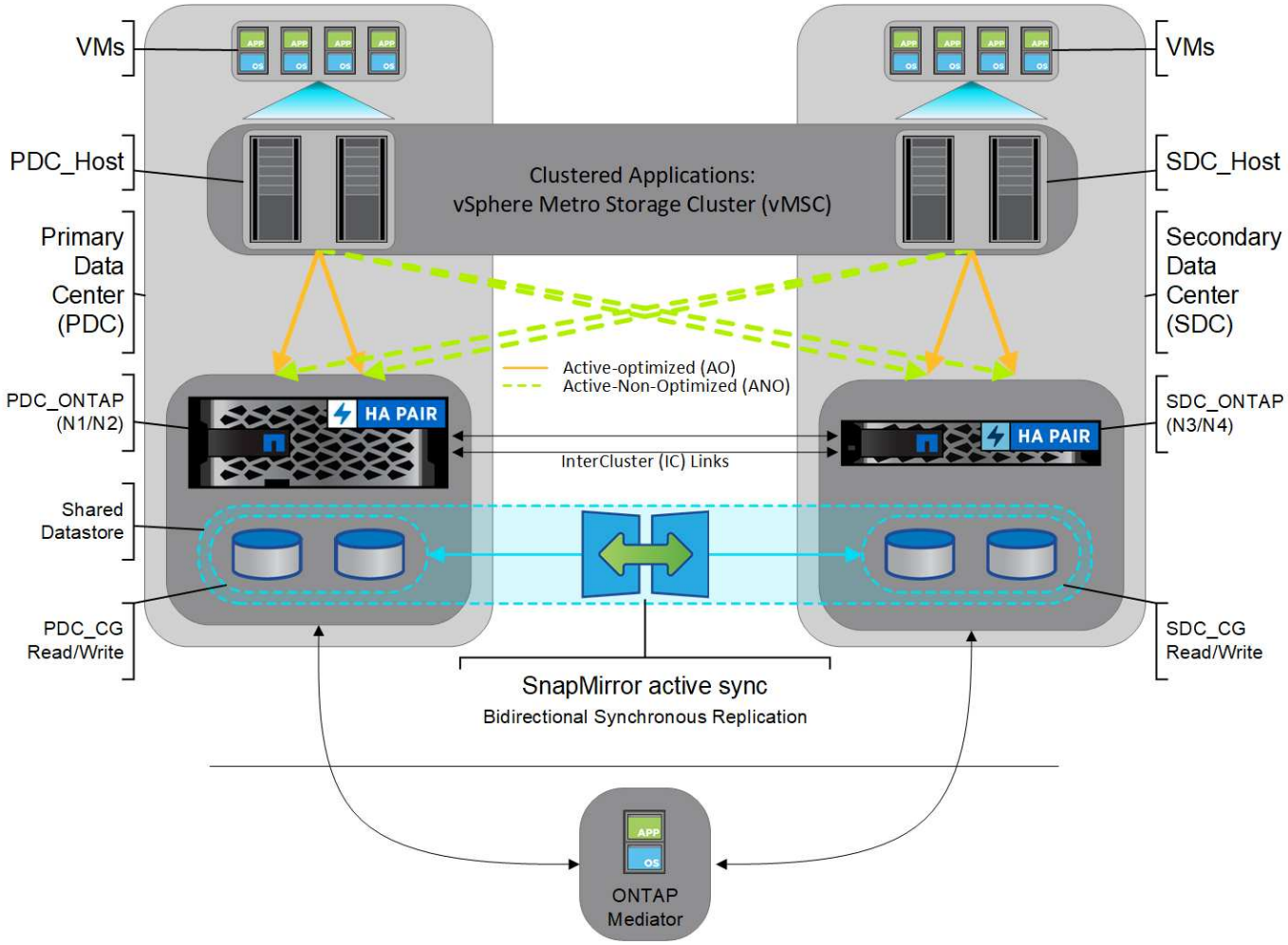
対称アクティブ/アクティブ

SnapMirror Active Syncは、非対称ソリューションと対称ソリューションを提供します。

非対称構成 では、プライマリ ストレージ コピーはアクティブに最適化されたパスを公開し、クライアント I/O をアクティブに提供します。NVMeセカンダリ サイトはI/Oにリモート パスを使用します。セカンダリ サ

イトのストレージ パスはアクティブ / 非最適化とみなされます。書き込みLUNへのアクセスは、セカンダリ サイトからプロキシされます。プロトコルは非対称構成ではサポートされません。

_対称アクティブ/アクティブ構成_では、アクティブ最適化パスが両サイトに公開され、ホスト固有で設定可能です。つまり、どちらの側のホストもアクティブI/Oのためにローカルストレージにアクセスできます。ONTAPONTAP以降、対称アクティブ/アクティブは最大4ノードのクラスタでサポートされます。ONTAP9.17.1以降、対称アクティブ/アクティブ構成は2ノードクラスタでNVMeプロトコルをサポートします。



対称アクティブ/アクティブ構成は、VMware Metro Storage Cluster、Oracle RAC、SQLを使用したWindows フェイルオーバークラスタリングなどのクラスタ化されたアプリケーションを対象としています。

ONTAP SnapMirror Active Syncの使用例

グローバルに接続されたビジネス環境では、サイバー攻撃、停電、自然災害などの障害が発生した場合でも、データ損失なしでビジネスクリティカルなアプリケーション データを迅速に回復することが求められています。こうした要求は、一般データ保護規則（GDPR）といった規制要件を遵守する金融などの業界で高まっています。

SnapMirrorアクティブ同期には、次のようなユースケースがあります。

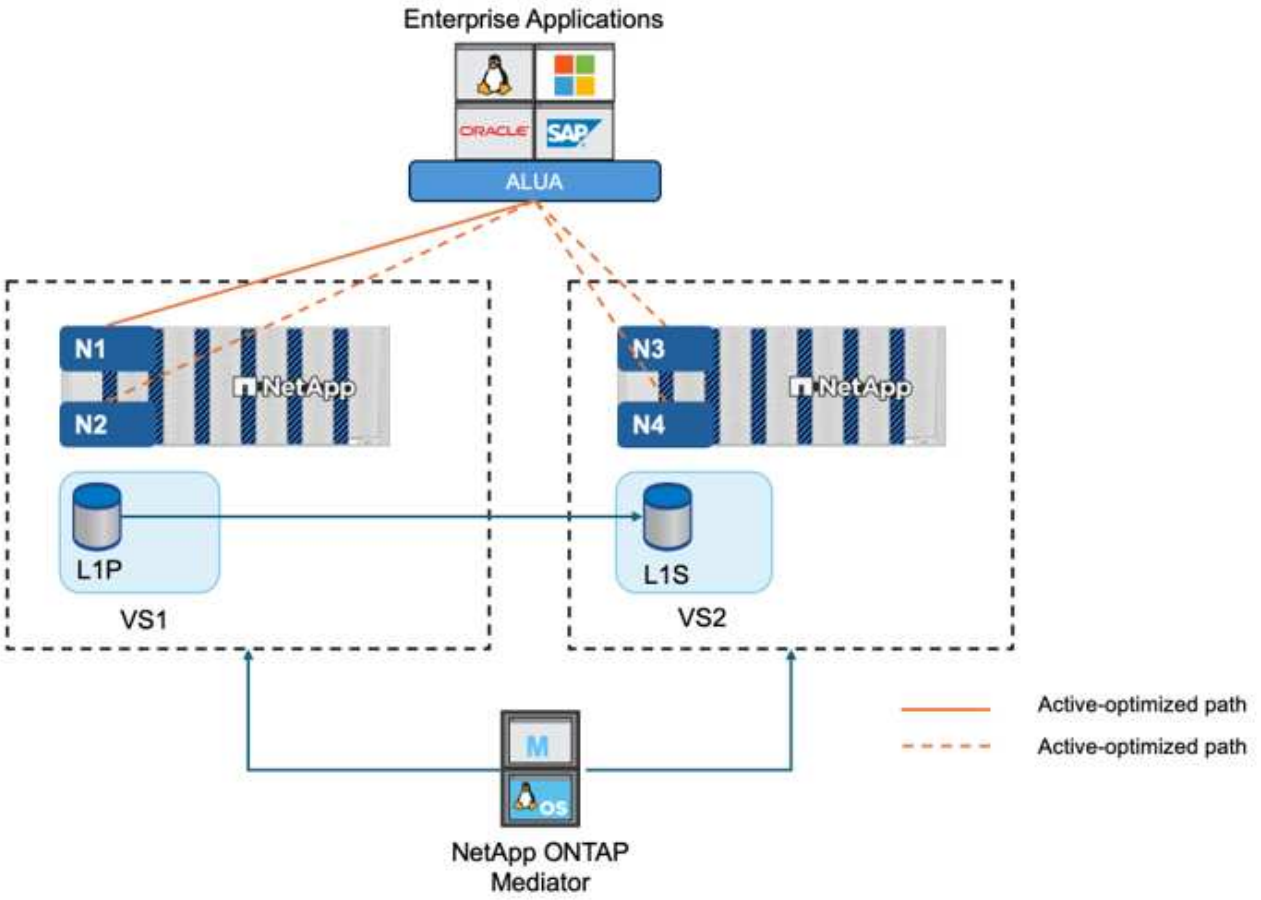
アプリケーションの導入による目標復旧時間（**RTO**）ゼロ

SnapMirrorアクティブ同期環境では、プライマリ クラスタとセカンダリ クラスタを使用します。プライマリ

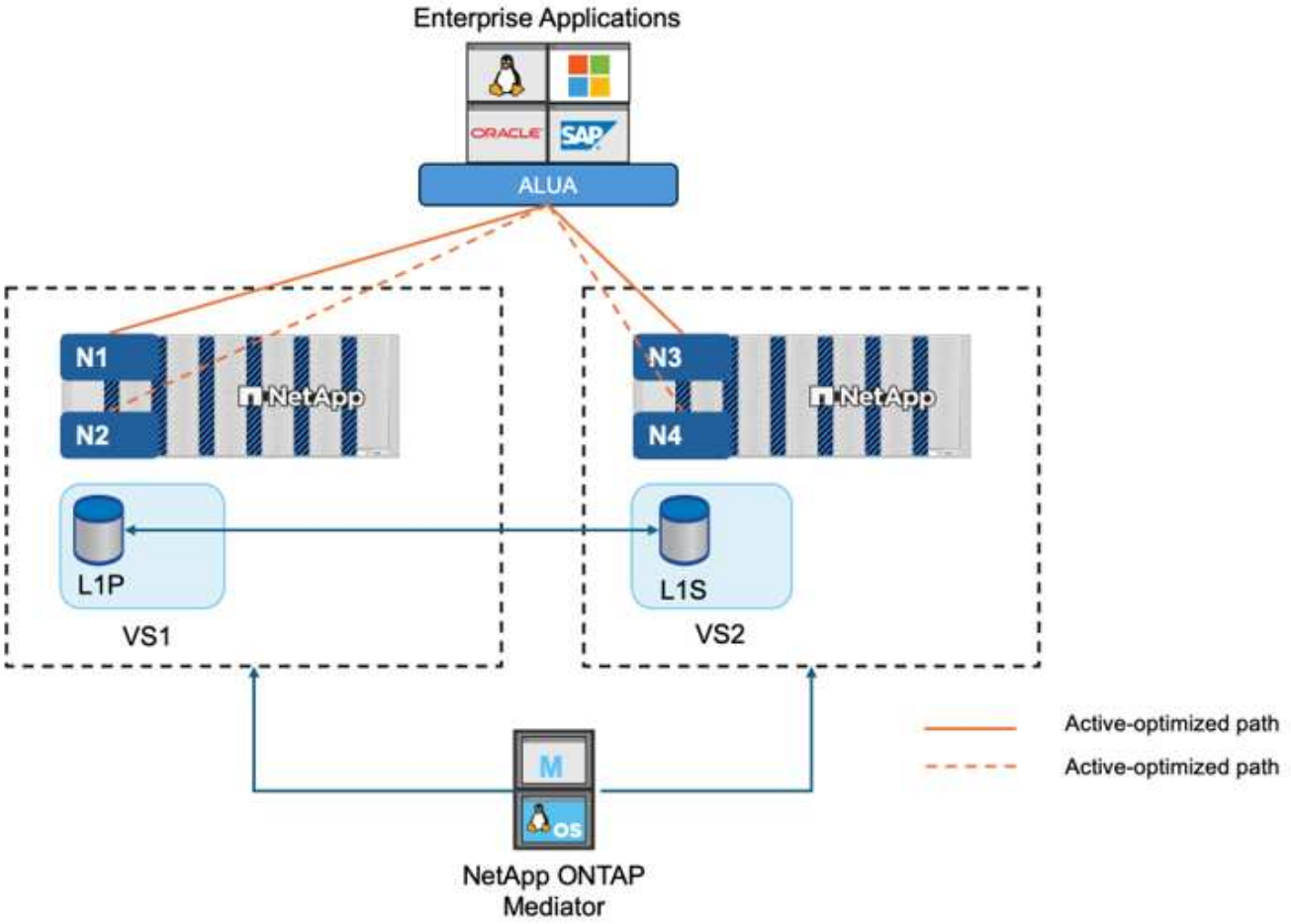
クラスタ内のLUN `L1P` ）には鏡がある `L1S` ）はセカンダリLUNに同じシリアルIDを持ち、ホストには読み書き可能なLUNとして報告されます。しかし、非対称構成では、読み取りと書き込みの操作はプライマリLUNにのみサービスされる、 `L1P`。 `L1S`プロキシによって提供されます。

RTOゼロまたは透過的なアプリケーションフェイルオーバー（**TAF**）のためのアプリケーション導入

TAFは、ホストのMPIOソフトウェアベースのパス フェイルオーバーに基づいて、ストレージへのノンストップ アクセスを実現します。プライマリとミラーの両方のLUNコピー（L1PとL1Sなど）に同じID（シリアル番号）が割り当てられ、両方が読み取り / 書き込み可能としてホストに報告されます。ただし、非対称構成では、読み取りと書き込みはプライマリ ボリュームによってのみ処理されます。ミラー コピーへのI/Oはプライマリ コピーにプロキシされます。ホストからL1への優先パスはVS1:N1で、これは非対称論理ユニット アクセス（ALUA）のアクセス状態「アクティブ / 最適化済み」（A/O）に基づきます。主にプライマリでストレージが停止した場合にフェイルオーバー（計画的または計画外）を実行するため、ONTAP Mediatorを使用する必要があります。



TAFは、自動フェイルオーバーと自動フェイルオーバー・デュプレックスの2つのモードで動作します。自動フェイルオーバーでは、読み取りと書き込みはプライマリボリュームのみで処理されるため、ミラーコピー（ミラーコピー自身は書き込み処理を実行できません）へのIOはプライマリコピーにプロキシされます。自動フェイルオーバー・デュプレックスでは、プライマリコピーとセカンダリコピーの両方でIOを処理できるため、プロキシは不要です。



ONTAP 9.17.1 でホスト アクセスに NVMe を使用している場合は、AutomatedFailoverDuplex ポリシーのみがサポートされます。

SnapMirrorアクティブ同期では、ALUAが使用されます。ALUAは、アプリケーションホストのマルチパスソフトウェアに対して、優先順位およびアクセス可用性を指定してアドバタイズされたパスを使用して、アプリケーションホストとストレージアレイの通信を行うためのメカニズムです。ALUAは、LUNを所有するコントローラへのアクティブな最適パスおよびその他のパスをアクティブな非最適パスとしてマークします。このパスは、プライマリパスで障害が発生した場合にのみ使用されます。

NVMe プロトコルを使用したSnapMirrorアクティブ同期は非対称名前空間アクセス (ANA) を使用します。これにより、アプリケーション ホストは保護されている NVMe 名前空間への最適化されたパスと最適化されていないパスを検出できます。NVMeターゲットは適切なパス状態を公開し、アプリケーションホストが保護対象のNVMeネームスペースへの最適なパスを使用できるようにします。

クラスタアプリケーション

VMware Metro Storage Cluster、Oracle RAC、Windows Failover Clustering with SQL などのクラスタ化されたアプリケーションでは、パフォーマンスのオーバーヘッドなしで VM を他のサイトにフェールオーバーできるように、同時アクセスが必要です。SnapMirrorアクティブ同期の対称アクティブ / アクティブは、双方向レプリケーションによってローカルでIOを処理することで、クラスタ アプリケーションの要件を満たします。ONTAP 9.16.1 以降では、対称アクティブ/アクティブが 4 ノード クラスタの構成でサポートされ、 ONTAP 9.15.1 の 2 ノード クラスタの制限から拡張されました。

災害シナリオ

地理的に分散したサイト間で、アプリケーション用の複数のボリュームを同期的にレプリケートします。プラ

イマリが停止した場合に自動的にセカンダリ コピーにフェイルオーバーできるため、ティア1アプリケーションのビジネス継続性を確保できます。プライマリ クラスタをホストしているサイトで災害が発生すると、ホストのマルチパス ソフトウェアはそのクラスタを経由するすべてのパスを停止とマークし、セカンダリ クラスタからのパスを使用します。その結果、ONTAP Mediatorによる無停止でのミラー コピーへのフェイルオーバーが可能になります。

拡張アプリケーションサポート

SnapMirrorアクティブ同期は柔軟性に優れ、使いやすいアプリケーションレベルのきめ細かい対応と自動フェイルオーバーを実現します。SnapMirrorアクティブ シンクは、IP ネットワーク経由の実績のあるSnapMirror同期レプリケーションを使用して、LAN または WAN 経由で高速にデータをレプリケートし、仮想環境と物理環境の両方で、Oracle、Microsoft SQL Server などのビジネス クリティカルなアプリケーションの高いデータ可用性と高速なデータ レプリケーションを実現します。

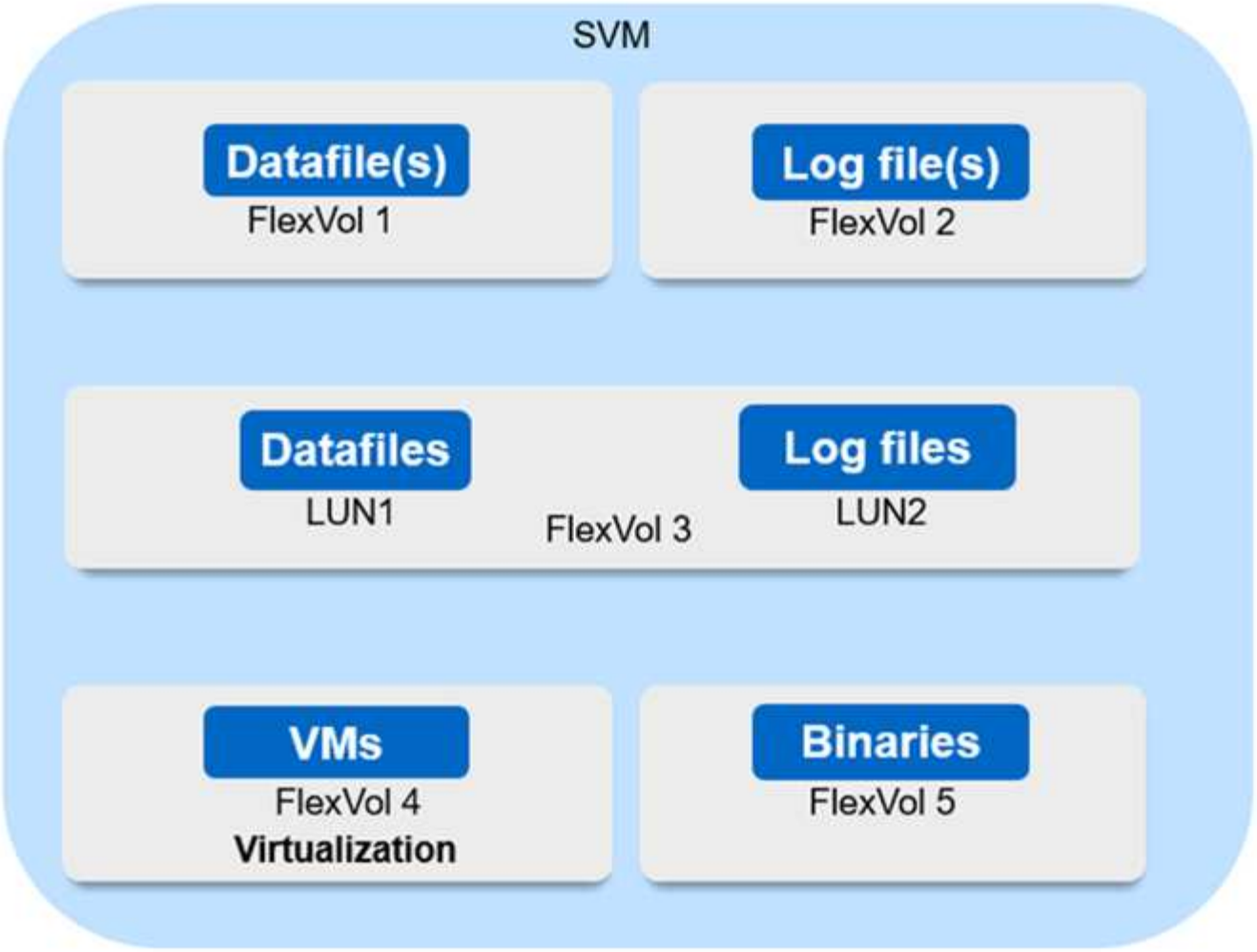
SnapMirrorアクティブ同期を使用すると、セカンダリ コピーへのTAFにより、サイト全体に障害が発生してもミッションクリティカルなビジネス サービスの運用を継続できます。このフェイルオーバーをトリガーするために、手動による介入や追加のスクリプトは必要ありません。

ONTAP SnapMirror Active Sync の導入戦略とベストプラクティス

データ保護戦略では、ビジネス継続性のために保護する必要があるワークロードを明確に特定することが重要です。データ保護戦略で最も重要なステップは、エンタープライズ アプリケーションのデータ レイアウトを明確にして、どのようにボリュームを分散させ、ビジネス継続性を保護するかを決定できるようにすることです。フェイルオーバーはアプリケーションごとに整合性グループ レベルで起こるため、必要なデータ ボリュームを整合性グループに必ず追加するようにします。

SVM構成

次の図は、SnapMirrorのアクティブな同期に推奨されるStorage VM（SVM）設定を示しています。



- データボリュームの場合：
  - ランダムリードのワークロードはシーケンシャルライトとは切り離されているため、データファイルとログファイルは通常、データベースのサイズによっては別 々 のボリュームに配置されます。
    - 重要な大規模データベースの場合、単一のデータファイルがFlexVol 1に、対応するログファイルがFlexVol 2にあります。
    - 統合を効率化するために、小規模から中規模の重要でないデータベースは、すべてのデータファイルがFlexVol 1に配置され、対応するログファイルがFlexVol 2に配置されるようにグループ化されます。ただし、このグループ化によって、アプリケーションレベルの細分性が失われます。
  - 別の方法としては、すべてのファイルを同じFlexVol 3に格納し、データファイルをLUN1に、ログファイルをLUN 2に格納する方法があります。
- 環境が仮想化されている場合は、さまざまなエンタープライズアプリケーションのすべてのVMを1つのデータストアで共有します。通常、VMとアプリケーションバイナリはSnapMirrorを使用して非同期でレプリケートされます。

計画

ONTAP SnapMirrorアクティブ同期の前提条件

SnapMirror Active Syncの導入を計画する際には、ハードウェア、ソフトウェア、および

システム構成のさまざまな要件を満たしていることを確認します。

ハードウェア

次の表に、サポートされるNetAppクラスタ構成を示します。

クラスタの種類	サポートされるモデル	サポートされる機能	サポートされる最大クラスタノード数
AFF	Aシリーズ、Cシリーズ	自動フェールオーバーデュプレックス（対称アクティブ/アクティブ）、自動フェールオーバー（非対称アクティブ/アクティブ）	• 2（ONTAP 9.9.1以降） • 4（対称アクティブ/アクティブ構成のONTAP 9.16.1）
ASA	Aシリーズ、Cシリーズ	自動フェールオーバーデュプレックス（対称アクティブ/アクティブ）、自動フェールオーバー（非対称アクティブ/アクティブ）	• 2 (ONTAP 9.9.1以降 • 4（対称アクティブ/アクティブ構成のONTAP 9.16.1）
ASA r2	すべて	自動フェイルオーバーデュプレックス（対称アクティブ/アクティブ）	2

次の表に、クラスタタイプ間のレプリケーション機能の概要を示します。

クラスタタイプ1	クラスタタイプ2	レプリケーションのサポート
AFF Aシリーズ	AFF Cシリーズ	○
ASA r2 Aシリーズ	ASA r2 Cシリーズ	○
AFF	ASA	いいえ
ASA	ASA r2	いいえ
ASA r2	ASA r2	○

ソフトウェア

- ONTAP 9.9.1以降
- ONTAP Mediator 1.2以降
- 次のいずれかを実行している ONTAP Mediator 用の Linux サーバまたは仮想マシン。

ONTAP メディエーターのバージョン	サポートされるLinuxバージョン
1.10	• Red Hat Enterprise Linux ◦ 互換性: 9.5 [1] ◦ 推奨: 10、9.6、9.4、8.10 • Rocky Linux 10、9.6、および 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 互換性: 9.3、9.1、8.9、8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.9	• Red Hat Enterprise Linux ◦ 互換性: 9.3、9.1、8.9、8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.8	• Red Hat Enterprise Linux： ◦ 互換性: 8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.4、9.3、9.2、9.1、9.0、8.10、8.9、8.8 • Rocky Linux 9.4、8.10
1.7	• Red Hat Enterprise Linux： ◦ 互換性: 8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.3、9.2、9.1、9.0、8.9、8.8 • Rocky Linux 9.3、8.9
1.6	• Red Hat Enterprise Linux： ◦ 互換性: 8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.2、9.1、9.0、8.8 • Rocky Linux 9.2、8.8
1.5	• Red Hat Enterprise Linux: 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6

1.4	• Red Hat Enterprise Linux: 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6
1.3	• Red Hat Enterprise Linux: 8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6
1.2	• Red Hat Enterprise Linux: 8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6

1. 互換性があるとは、Red Hat がこれらの RHEL バージョンをサポートしなくなったものの、 ONTAP Mediator をこれらのバージョンにインストールできることを意味します。

ライセンス

次のSnapMirrorライセンスは、 ONTAP One ライセンス スイートの一部として使用可能であり、両方のクラスタに適用する必要があります。

- SnapMirror同期
- SnapMirror

> 2019年6月より前にONTAPストレージシステムを購入した場合は、を参照して、"NetApp ONTAP のマスターライセンスキー"必要なSnapMirror同期ライセンスを取得してください。

- VMware の場合、vSphere Metro Storage Cluster (vMSC) ライセンスが必要です。

ネットワーク環境

- クラスタ間レイテンシのラウンド トリップ タイム（RTT）が10ミリ秒未満である必要があります。
- ONTAP 9 .14.1以降では、"SCSI-3の永続的予約"SnapMirrorアクティブ同期でサポートされています。

サポートされるプロトコル

SnapMirrorアクティブ同期は SAN プロトコルをサポートします。

- FC および iSCSI プロトコルは、 ONTAP 9.9.1 以降でサポートされます。
- NVMe プロトコルは、 ONTAP 9.17.1 以降の VMware ワークロードでサポートされます。

> VMware での NVMe/TCP は、VMware バグ ID: TR1049746 の解決に依存します。

SnapMirrorアクティブ同期は、NVMe プロトコルでは以下をサポートしません。

  - 4ノード対称アクティブ/アクティブ構成
  - 非対称アクティブ/アクティブ構成

- 一貫性グループのサイズの変更

  SnapMirrorアクティブ同期で NVMe プロトコルを使用する場合、整合性グループを拡張または縮小することはできません。

- 同じ整合性グループ内の LUN と名前空間の共存。

IPspace

SnapMirrorアクティブ同期でクラスタ ピア関係を確立するには、デフォルトのIPspaceが必要です。カスタム IPspace はサポートされていません。

NTFSセキュリティ形式

NTFSセキュリティ形式は、SnapMirrorアクティブな同期ボリュームでは*サポートされていません*。

ONTAP Mediator

- 透過的なアプリケーション フェイルオーバーを実現するには、ONTAP Mediator を外部でプロビジョニングし、ONTAP に接続する必要があります。
- 完全に機能し、計画外の自動フェイルオーバーを有効にするには、外部 ONTAP メディエーターをプロビジョニングし、ONTAP クラスタで設定する必要があります。
- ONTAP Mediator は、2 つの ONTAP クラスタとは別の 3 番目の障害ドメインにインストールする必要があります。
- ONTAP Mediator をインストールするときは、自己署名証明書を、主流の信頼できる CA によって署名された有効な証明書に置き換える必要があります。
- ONTAPメディエーターの詳細については、 "ONTAPメディエーターのインストール準備" 。

その他の前提条件

- ONTAP 9.15.1 より前のリリースでは、読み取り/書き込みデスティネーション ボリューム（非対称アクティブ/アクティブで DP から読み取り/書き込みに変換されたボリューム）ではSnapMirrorアクティブ同期関係はサポートされません。読み取り/書き込みボリュームを使用する前に、ボリューム レベルのSnapMirror関係 (非同期または同期) を作成してからその関係を削除し、読み取り/書き込みボリュームを DP ボリュームに変換する必要があります。詳細については、 "既存のSnapMirror関係をSnapMirrorアクティブな同期に変換する" 。
- SnapMirror Active Sync を使用するストレージ VM は、クライアント コンピュータとして Active Directory に参加できません。

詳細情報

- "Hardware Universe"
- "ONTAPメディエーターの概要"

ONTAP SnapMirrorアクティブ同期の相互運用性

SnapMirrorアクティブ同期は、多数のオペレーティング システム、アプリケーション ホスト、ONTAPのその他の機能と互換性があります。

サポートの可否や相互運用性の詳細については、Interoperability Matrix Toolを参照して ("IMT" ください）。

アプリケーションホスト

SnapMirrorアクティブ シンクは、Hyper-V、ESXi、Red Hat Enterprise Linux (RHEL)、Windows Server などのオペレーティング システム、vSphere Metro Storage Cluster (vMSC) などのクラスタリング ソリューション、およびONTAP 9.14.1 以降では Windows Server フェールオーバー クラスタなどのハイパーバイザをサポートします。

オペレーティングシステム

SnapMirrorアクティブ同期は、次のような多数のオペレーティングシステムでサポートされています。

- PVRを使用したAIX（ONTAP 9.11.1以降）
- HP-UX（ONTAP 9.10.1以降）
- Solaris 11.4（ONTAP 9.10.1以降）

AIX

ONTAP 9.11.1 以降、AIX は、以下の規定を理解した上で、標準エンジニアリング機能ポリシー変動要求 (FPVR) を介してSnapMirrorアクティブ同期でサポートされます。

- SnapMirrorアクティブ同期ではRPOゼロのデータ保護を実現できますが、AIXのフェイルオーバープロセスではパスの変更を認識するために追加の手順が必要になります。ルートボリュームグループに属していないLUNは、コマンドが実行されるまでI/Oの一時停止が発生します `cfgmgr`。これは自動化でき、ほとんどのアプリケーションはそれ以上のシステム停止を伴わずに運用を再開できます。
- ルートボリュームグループに属するLUNは、通常はSnapMirrorのアクティブな同期で保護しないでください。フェイルオーバー後にコマンドを実行することはでき `cfgmgr`ません。つまり、SANパスの変更を認識するにはリブートが必要です。ルートボリュームグループではRPOゼロのデータ保護を実現できますが、フェイルオーバーの際はシステムが停止します。

AIXとのSnapMirrorアクティブ同期の詳細については、NetAppアカウントチームにお問い合わせください。

HP-UX

ONTAP 9.10.1以降では、HP-UX用のSnapMirrorアクティブ同期がサポートされます。

HP-UXでの自動計画外フェイルオーバー

プライマリ クラスタとセカンダリ クラスタ間の接続が失われ、プライマリ クラスタとメディエーター間の接続も失われた場合、分離されたマスター クラスタでの自動計画外フェイルオーバー (AUFO) イベントは、デュアル イベント障害によって発生する可能性があります。他のAUFOイベントと違い、これは滅多に発生しないイベントです。

- このような場合、HP-UXホストでI/Oが再開されるまでに120秒以上かかることがあります。実行中のアプリケーションによっては、I/Oが中断しない場合や、エラー メッセージが表示されない場合があります。
- 問題を修正するには、許容される中断時間が120秒未満のHP-UXホストでアプリケーションを再起動する必要があります。

Solaris

ONTAP 9.10.1以降では、SnapMirrorアクティブ同期でSolaris 11.4がサポートされます。

SnapMirrorアクティブ同期環境で計画外のサイト フェイルオーバー / スイッチオーバーが発生した場合にSolarisクライアント アプリケーションが停止しないようにするには、Solaris OSのデフォルト設定を変更します。Solarisを推奨設定で構成するには、"NetAppナレッジベース: Solaris ホストサポートのSnapMirror Active Sync の推奨設定" 。

ONTAPの相互運用性

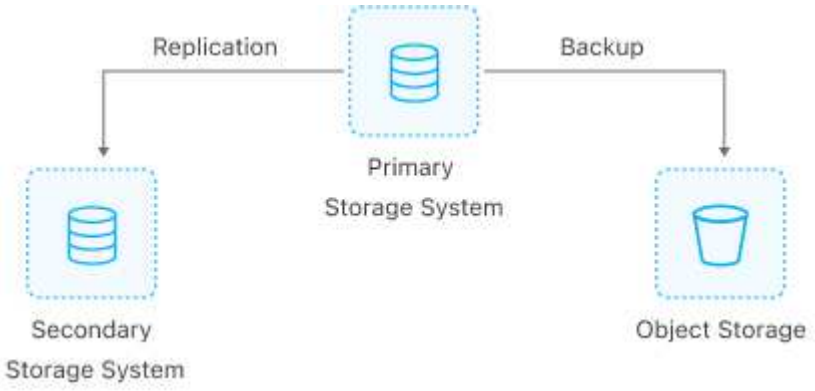
SnapMirrorアクティブ同期は、ONTAPのコンポーネントと統合されて、データ保護機能を拡張します。

FabricPool

SnapMirrorのアクティブな同期では、FabricPoolアグリゲートのソースボリュームとデスティネーションボリュームの階層化ポリシーが「なし」、「Snapshot」、または「自動」に設定されています。SnapMirrorのアクティブな同期では、階層化ポリシーを「すべて」に設定したFabricPoolアグリゲートはサポートされません。

ファンアウト構成

でファンアウト構成、ソース ボリュームをSnapMirrorアクティブ同期の宛先エンドポイントと 1 つのSnapMirror非同期関係にミラーリングできます。



SnapMirror Active Syncでは、 `MirrorAllSnapshots`ポリシー、および`ONTAP 9.11.1`以降 `MirrorAndVault`でポリシーがサポートされますファンアウト構成。ファンアウト構成は、ポリシーとの`SnapMirror`アクティブな同期ではサポートされません `XDPDefault`。

ONTAP 9.15.1以降では、SnapMirrorアクティブ同期でフェイルオーバーイベント後のファンアウトレッグの自動再設定がサポートされます。プライマリサイトからセカンダリサイトへのフェイルオーバーが成功すると、セカンダリサイトをソースとして扱うように、ターシャリサイトが自動的に再設定されます。非同期ファンアウトレッグには、整合性グループ関係または独立したボリューム関係を指定できます。リコンフィグレーションはどちらのケースでも機能します。再設定は、計画的フェイルオーバーまたは計画外フェイルオーバーによってトリガーされます。プライマリ サイトへのフェイルバック時にも実行されます。

以前のリリースのONTAPでのファンアウト構成の管理については、を参照してくださいファンアウト構成で保護を再開します。

NDMPリストア

ONTAP 9.13.1以降では、SnapMirrorアクティブ同期でを使用できNDMPによるデータのコピーとリストアます。NDMPを使用すると、データをSnapMirrorのアクティブな同期ソースに移動して、保護を一時停止することなくリストアを完了できます。これは、ファンアウト構成で特に便利です。

SnapCenter

SnapMirrorアクティブ同期は、以降のSnapCenterでサポートされて"SnapCenter 5.0"います。SnapCenterを使用すると、アプリケーションと仮想マシンの保護とリカバリに使用できるスナップショットを作成できます。これにより、アプリケーションレベルのきめ細かさで、いつでも利用可能なストレージソリューションを実現できます。

SnapRestore

SnapMirrorアクティブ同期では、部分ファイルと単一ファイルのSnapRestoreがサポートされます。

Single File SnapRestore

ONTAP 9 .11.1以降では、単一ファイルのSnapRestoreSnapMirrorのアクティブな同期ボリュームでサポートされます。SnapMirrorのアクティブな同期元からデスティネーションにレプリケートされたSnapshotから単一のファイルをリストアできます。ボリュームには1つ以上のLUNを含めることができるため、この機能を使用すると、中断の少ないリストア処理を実装して、他のLUNを中断せずに1つのLUNをきめ細かくリストアできます。Single File SnapRestoreには、インプレースとアウトオブプレースの2つのオプションがあります。

Partial File SnapRestore

ONTAP 9 .12.1以降では、"部分的なLUNリストア"SnapMirrorアクティブ同期ボリュームでサポートされています。SnapMirrorのアクティブな同期元（ボリューム）ボリュームとデスティネーション（Snapshot）ボリュームの間でレプリケートされた、アプリケーションで作成されたSnapshotからデータをリストアできます。同じLUNに複数のデータベースが格納されているホストでデータベースをリストアする必要がある場合は、LUNまたはファイルの部分リストアが必要になることがあります。この機能を使用するには、データの開始バイトオフセットとバイトカウントを知る必要があります。

大規模なLUNと大規模なボリューム

大規模なLUNと大規模なボリューム（100TBを超えるボリューム）がサポートされるかどうかは、使用しているONTAPのバージョンとプラットフォームによって異なります。

ONTAP 9.12.1P2以降

- ONTAP 9 12.1 P2以降では、SnapMirrorアクティブ同期で、ASAおよびAFF（AシリーズおよびCシリーズ）で大容量のLUNと100TBを超える大容量ボリュームがサポートされます。プライマリクラスタとセカンダリクラスタのタイプが同じである必要があります（ASAまたはAFF）。AFF AシリーズからAFF Cシリーズへ（またはその逆）のレプリケーションがサポートされます。

ONTAPリリース9.12.1P2以降では、プライマリクラスタとセカンダリクラスタの両方がオールフラッシュSANアレイ（ASA）またはオールフラッシュアレイ（AFF）で、両方にONTAP 9 12.1P2以降がインストールされていることを確認する必要があります。セカンダリクラスタでONTAP 9 .12.1P2より前のバージョンが実行されている場合やアレイタイプがプライマリクラスタと異なる場合、プライマリボリュームが100TBを超えると同期関係が同期されなくなることがあります。

ONTAP 9 .9.1 ~ 9.12.1P1

- ONTAP 9 .9.1から9.12.1 P1までのONTAPリリースでは、100TBを超える大容量LUNと大容量ボリュームがオールフラッシュSANアレイでのみサポートされます。AFF AシリーズからAFF Cシリーズへ（またはその逆）のレプリケーションがサポートされます。

ONTAP 9 .9.1から9.12.1 P2の間のONTAPリリースでは、プライマリクラスタとセカンダリクラスタの両方がオールフラッシュSANアレイであり、両方にONTAP 9 .9.1以降がインストールされていることを確認する必要があります。セカンダリクラスタでONTAP 9 .9.1より前のバージョンが実行されている場合やオールフラッシュSANアレイでない場合、プライマリボリュームが100TBを超えると同期関係が同期されなくなることがあります。

詳細情報

- "AIXホストでSnapMirrorアクティブ同期を設定する方法"

ONTAP SnapMirror Active Sync のオブジェクト制限

SnapMirrorアクティブ同期を使用する際は、以下のオブジェクト数の制限に注意してください。

クラスタ内の整合性グループ数

SnapMirrorアクティブ同期を使用するクラスタに対する整合性グループ数の制限は、関係に基づいて計算され、使用するONTAPのバージョンによって異なります。制限はプラットフォームには依存しません。

ONTAPのバージョン	関係の最大数
ONTAP 9.11.1以降	50 *
ONTAP 9 10.1	20
ONTAP 9 .9.1	5

｛asterisk｝ ONTAP 9.16.1以降では、SnapMirrorアクティブ同期で対称アクティブ/アクティブ構成の4ノードクラスタがサポートされます。4ノードクラスタでは、100個の整合グループがサポートされます。

整合性グループあたりのボリューム数

SnapMirrorアクティブ同期を使用する整合性グループあたりの最大ボリューム数は、プラットフォームに依存しません。

ONTAPのバージョン	整合性グループ関係でサポートされる最大ボリューム数
ONTAP 9.15.1以降	80
ONTAP 9 .10.1-9.14.1	16
ONTAP 9 .9.1	12

ボリューム

SnapMirror Active Syncのボリューム制限は、関係の数ではなくエンドポイントの数に基づいて計算されます。12個のボリュームで構成される整合グループは、プライマリクラスタとセカンダリクラスタの両方のエンドポイントを12個提供します。エンドポイントの総数は、SnapMirrorのアクティブな同期関係とSnapMirrorの同期関係の両方で構成されます。

これらの制限はFAS、 AFF、およびASAシステムに適用されます。ASAr2システム（ASA ASA 、 ASA A90、 ASA A70、 ASA A50、 ASA A30、またはASA A20）をご利用の場合は、 "ASA r2のドキュメント" 。

プラットフォームあたりの最大エンドポイント数を次の表に示します。

プラットフォーム	**SnapMirror**アクティブ同期の**HA**あたりのエンドポイント数			**HA**あたりの全体的な同期エンドポイントと**SnapMirror**のアクティブな同期エンドポイント		
	ONTAP 9.11.1以降	ONTAP 9 10.1	ONTAP 9 .9.1	ONTAP 9.11.1以降	ONTAP 9 10.1	ONTAP 9 .9.1
AFF	400 *	200	60	400	200	80
ASA	400 *	200	60	400	200	80

｛asterisk｝ ONTAP 9.16.1以降では、SnapMirrorアクティブ同期で対称アクティブ/アクティブ構成の4ノードクラスタがサポートされます。4ノードクラスタの合計エンドポイント数は800です。

SANオブジェクトの制限

SANオブジェクトの制限を次の表に示します。これらの制限は、プラットフォームに関係なく適用されます。

SnapMirrorアクティブ同期関係のオブジェクト	カウント
ボリュームあたりのLUN数	• 256（ONTAP 9.9.1 - ONTAP 9.15.0） • 512（ONTAP 9.15.1以降）
2 x 2 SnapMirrorアクティブ同期ソリューションあたりの一意の LUN、ネームスペース、またはストレージ ユニットの数	4,096

SnapMirrorアクティブ同期関係のオブジェクト	カウント
4 x 4 SnapMirror Active-Sync ソリューションあたりの一意の LUN、ネームスペース、またはストレージユニットの数 (ONTAP 9.16.1 以降で利用可能)	6,144
SVM あたりの LIF 数（ SnapMirrorアクティブ同期関係に少なくとも 1 つのボリュームがある）	256
ノードあたりのクラスタ間LIF数	4
クラスタあたりのクラスタ間LIF数	8

NVMeオブジェクトの制限

ONTAP 9.17.1以降、 SnapMirror Active SyncはNVMeプロトコルをサポートします。NVMeオブジェクトの制限については、次の表をご覧ください。

SnapMirrorアクティブ同期関係におけるオブジェクトの最大数	カウント
ノードあたりの名前空間マップの数	4K
クラスターサイズ	2ノード
HAペアあたりの整合性グループの数	50
単一のNVMe SnapMirrorアクティブ同期整合性グループ内のボリュームの数	80
HAペアのボリューム数	400
整合性グループあたりのNVMeサブシステム	16
一貫性グループごとの名前空間マップ	256

関連情報

- "Hardware Universe"
- "整合グループの制限"

設定

SnapMirror Active Sync 用に**ONTAP**クラスタを構成する

SnapMirror Active Syncは、フェイルオーバー発生時にピアクラスタを使用してデータを保護します。SnapMirrorActive Sync用にONTAP MediatorまたはONTAP Cloud Mediatorを設定する前に、クラスタが正しく設定されていることを確認する必要があります。

開始する前に

ONTAP Mediator またはONTAP Cloud Mediator を設定する前に、次の点を確認する必要があります。

1. クラスター間にクラスター ピアリング関係が存在します。

クラスタピア関係のSnapMirror Active SyncではデフォルトのIPspaceが必要です。カスタムIPspaceはサポートされません。

"クラスタピア関係の作成"

2. SVM は各クラスター上に作成されます。

   "SVMの作成"

3. 各クラスタの SVM 間にはピア関係が存在します。

   "SVMピア関係の作成"

4. LUN 用のボリュームが存在します。

   "ボリュームの作成"

5. 両方のクラスターの各ノードに、少なくとも 1 つの SAN LIF (該当する場合は FC または iSCSI) が作成されます。

   "クラスタSAN環境でのLIFに関する考慮事項"

   "LIFの作成"

6. 必要な LUN が作成され、igroup にマップされます。igroup は、LUN をアプリケーション ホスト上のイニシエーターにマップするために使用されます。

   "LUNの作成とigroupのマッピング"

7. アプリケーション ホストが再スキャンされ、新しい LUN が検出されます。

SnapMirror Active Sync 用のONTAP Mediator を構成する

SnapMirror Active Syncでは、フェイルオーバーが発生した場合にピアクラスタを使用してデータを保護します。ONTAP Mediatorは、各クラスタの健全性を監視することでビジネス継続性を実現する重要なリソースです。SnapMirrorActive Syncを設定するには、まずONTAP Mediatorをインストールし、プライマリクラスタとセカンダリクラスタが適切に設定されていることを確認する必要があります。

ONTAP Mediatorをインストールしてクラスタを設定したら、 自己署名証明書を使用して、SnapMirror Active Sync 用の ONTAP Mediator を初期化します。 。そうしなければなりませんSnapMirrorアクティブ同期の整合性グループを作成、初期化、マッピングする。

ONTAP Mediator

ONTAP Mediatorは、SnapMirror Active Sync関係にあるONTAPクラスタで使用される高可用性（HA）メタデータのための永続的かつフェンスされたストアを提供します。さらに、ONTAP Mediatorは、クォーラムの決定を支援する同期ノードヘルスクエリ機能を提供し、コントローラの稼働状態検出のためのpingプロキシとして機能します。

各クラスタピア関係は、1つのONTAPメディエーターインスタンスにのみ関連付けることができます。HAメ

ディエーターインスタンスはサポートされません。クラスタが他のクラスタと複数のピア関係にある場合は、次のONTAPメディエーターオプションを使用できます。

- 各関係にSnapMirrorのアクティブな同期が設定されている場合は、各クラスタピア関係に固有のONTAPメディエーターインスタンスを設定できます。
- クラスタでは、すべてのピア関係に同じONTAPメディエーターインスタンスを使用できます。

たとえば、クラスタBがクラスタA、クラスタC、およびクラスタDとピア関係にある場合、各関係にSnapMirrorのアクティブな同期が設定されていれば、3つのクラスタピア関係すべてに一意のONTAPメディエーターインスタンスを関連付けることができます。または、クラスタBは、3つのピア関係すべてに同じONTAPメディエーターインスタンスを使用できます。このシナリオでは、クラスタに対してONTAPメディエーターの同じインスタンスが3回表示されます。

ONTAP 9.17.1以降では、 "ONTAPクラウドメディエーター"ただし、 SnapMirrorアクティブ同期構成でクラスタの健全性を監視するには、両方のメディエーターを同時に使用することはできません。

ONTAP 9.17.1でSnapMirror Active SyncとONTAP MediatorまたはONTAP Cloud Mediatorを使用している場合は、*既知の問題と制限*を確認してください。"ONTAPリリースノート"これらの構成に関する重要な情報については、こちらをご覧ください。

ONTAPメディエーターの前提条件

- ONTAP Mediatorには独自の前提条件が含まれています。ONTAPMediatorをインストールする前に、これらの前提条件を満たす必要があります。

  詳細については、 "ONTAP Mediatorサービスのインストールの準備" 。

- デフォルトでは、ONTAP MediatorはTCPポート31784を使用してサービスを提供します。ONTAPクラスタとONTAPメディエーターの間でポート 31784 が開いていて使用可能であることを確認する必要があります。

ONTAPメディエーターをインストールし、クラスタ構成を確認する

ONTAP Mediatorをインストールし、クラスタ構成を確認するには、以下の各手順を実行してください。各手順で、特定の設定が実行されていることを確認してください。各手順には、実行する必要がある特定の手順へのリンクが含まれています。

手順

1. ソース クラスタと宛先クラスタが正しく設定されていることを確認する前に、ONTAP Mediator をインストールします。

   ONTAP Mediatorのインストールまたはアップグレードの準備

2. クラスタ間にクラスタピア関係が確立されていることを確認します。

   クラスタピア関係のSnapMirror Active SyncではデフォルトのIPspaceが必要です。カスタムIPspaceはサポートされません。

   "SnapMirror Active Sync 用にONTAPクラスタを構成する"

自己署名証明書を使用して、**SnapMirror Active Sync** 用の **ONTAP Mediator** を初期化します。

ONTAP Mediatorをインストールし、クラスタ構成を確認したら、クラスタ監視のためにONTAP Mediatorを初期化する必要があります。ONTAPMediatorの初期化は、System ManagerまたはONTAP CLIを使用して行うことができます。

System Manager

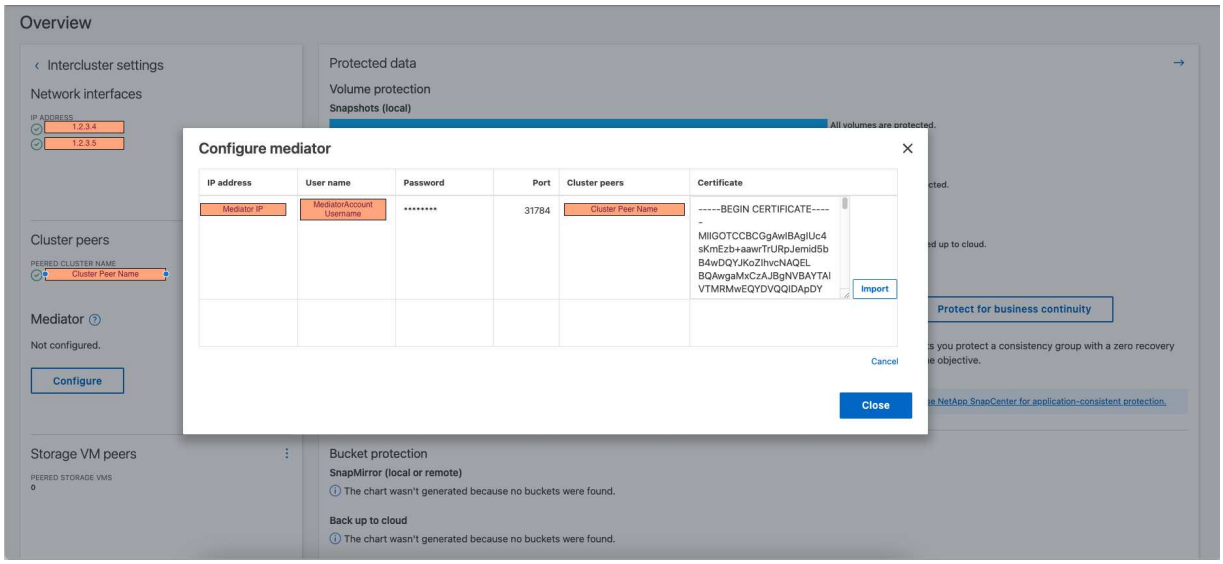
System Managerを使用すると、ONTAPメディエーターを自動フェイルオーバー用に設定できます。また、自己署名SSL証明書とCAを、サードパーティの検証済みSSL証明書とCAに置き換えることもできます（まだ行っていない場合）。

ONTAP 9.14.1 から 9.8 では、 SnapMirror Active Sync はSnapMirror Business Continuity (SM-BC) と呼ばれます。

ONTAP Mediator 1.9以降

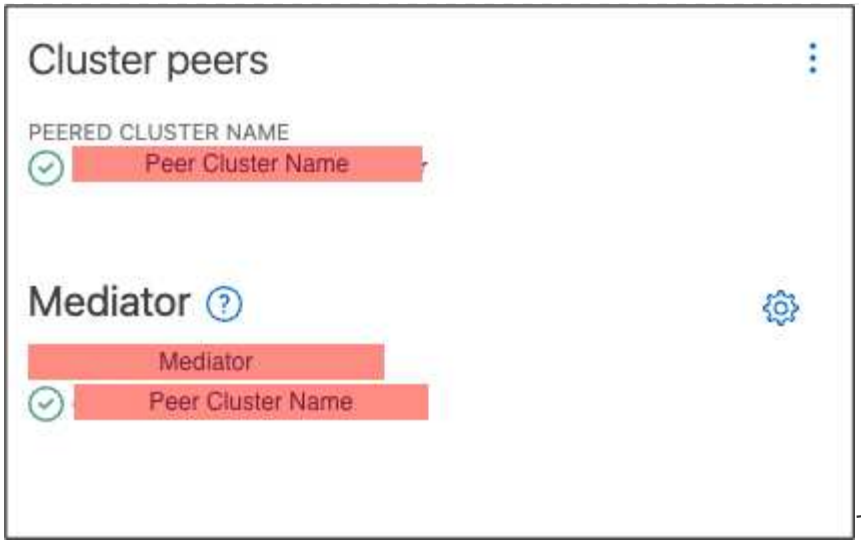
1. [* Protection] > [Overview] > [Mediator] > [Configure] * に移動します。
2. [追加] を選択し、次の ONTAP Mediator 情報を入力します。
   - IPv4アドレス
   - ユーザ名
   - パスワード
   - 証明書
3. 証明書の入力は、次の2つの方法で指定できます。
   - オプション（**A**）：*インポート*を選択して、ファイルに移動し `intermediate.crt`てインポートします。
   - オプション（**b**）：ファイルの内容をコピーし `intermediate.crt`、*証明書*フィールドに貼り付けます。

     すべての詳細を正しく入力すると、指定した証明書がすべてのピアクラスタにインストールされます。



証明書の追加が完了すると、ONTAP Mediator が ONTAP クラスタに追加されます。

次の図は、ONTAPメディエーターの設定を成功させる方法を示しています。

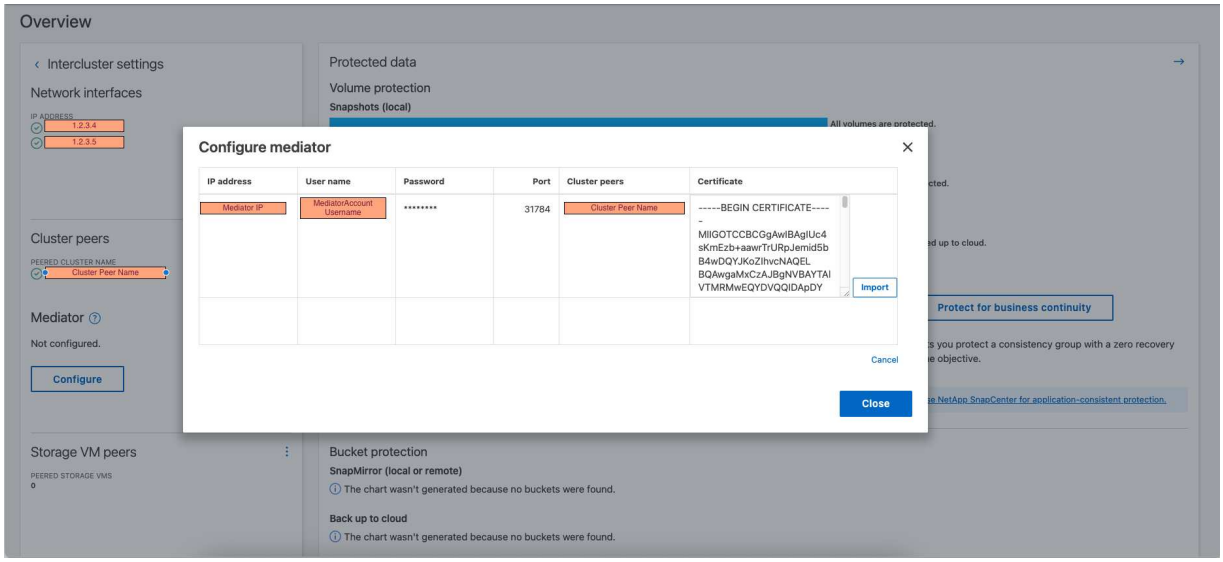


です。

ONTAPメディエーター**1.8**以前

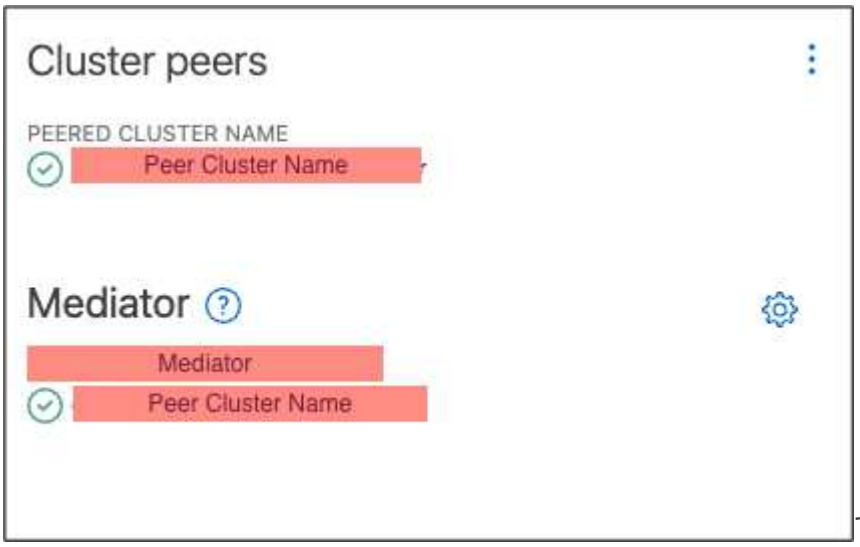
1. [* Protection] > [Overview] > [Mediator] > [Configure] * に移動します。
2. [追加] を選択し、次の ONTAP Mediator 情報を入力します。
   - IPv4アドレス
   - ユーザ名
   - パスワード
   - 証明書
3. 証明書の入力は、次の2つの方法で指定できます。
   - オプション（**A**）：*インポート*を選択して、ファイルに移動し `ca.crt`てインポートします。
   - オプション（**b**）：ファイルの内容をコピーし `ca.crt`、*証明書*フィールドに貼り付けます。

     すべての詳細を正しく入力すると、指定した証明書がすべてのピアクラスタにインストールされます。



証明書の追加が完了すると、ONTAP Mediator が ONTAP クラスタに追加されます。

次の図は、ONTAPメディエーターの設定を成功させる方法を示しています。



です。

CLI

ONTAP CLIを使用してプライマリクラスタまたはセカンダリクラスタから初期化できます。 `mediator add`一方のクラスタでコマンドを実行すると、もう一方のクラスタに ONTAP Mediator が自動的に追加されます。

ONTAPメディエーターを使用してSnapMirrorのアクティブ同期関係を監視する場合、有効な自己署名証明書または認証局（CA）証明書がないと、ONTAPメディエーターをONTAPで初期化できません。ピアクラスタの証明書ストアに有効な証明書を追加してください。ONTAPメディエーターを使用してMetroCluster IPシステムを監視する場合、初期設定後はHTTPSが使用されないため、証明書は必要ありません。

ONTAP Mediator 1.9以降

1. ONTAPメディエーターLinux VM /ホストソフトウェアのインストール先で、ONTAPメディエーターCA証明書を探します `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`。
2. ピアクラスタの証明書ストアに有効な認証局を追加します。

   例：

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. ONTAPメディエーターCA証明書をONTAPクラスタに追加します。プロンプトが表示されたら、ONTAPメディエーターから取得したCA証明書を挿入します。すべてのピアクラスタでこの手順を繰り返します。

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   例：

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 生成された証明書名を使用して、インストールされている自己署名CA証明書を表示します。

   `security certificate show -common-name <common_name>`

   例：

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 一方のクラスタでONTAP Mediatorを初期化します。もう一方のクラスタにはONTAP Mediatorが自動的に追加されます。

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 必要に応じて、ジョブIDのステータスを調べ `job show -id`て、SnapMirror Mediator addコマンドが成功したかどうかを確認します。

   例：

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. ONTAPメディエーターの設定のステータスを確認します。

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` SnapMirrorコンシステンシグループの関係がONTAPメディエーターと同期されているかどうかを示します。 `true`同期が成功したことを示します。

ONTAPメディエーター**1.8**以前

1. ONTAPメディエーターLinux VM /ホストソフトウェアのインストール先で、ONTAPメディエーターCA証明書を探します `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`。
2. ピアクラスタの証明書ストアに有効な認証局を追加します。

   例：

```
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. ONTAPメディエーターCA証明書をONTAPクラスタに追加します。プロンプトが表示されたら、ONTAPメディエーターから取得したCA証明書を挿入します。すべてのピアクラスタで上記の手順を繰り返します。

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 生成された証明書名を使用して、インストールされている自己署名CA証明書を表示します。

   `security certificate show -common-name <common_name>`

   例：

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 一方のクラスタでONTAP Mediatorを初期化します。もう一方のクラスタにはONTAP Mediatorが自動的に追加されます。

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 必要に応じて、ジョブIDのステータスを調べ `job show -id`て、SnapMirror Mediator addコマンドが成功したかどうかを確認します。

   例：

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. ONTAPメディエーターの設定のステータスを確認します。

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true
```

`Quorum Status` SnapMirrorコンシステンシグループの関係がONTAPメディエーターと同期されているかどうかを示します。 `true`同期が成功したことを示します。

サードパーティの証明書を使用して**ONTAP Mediator**を再初期化する

ONTAP Mediatorの再初期化が必要になる場合があります。ONTAPMediatorのIPアドレスの変更や証明書の有効期限切れなど、ONTAP Mediatorの再初期化が必要になる状況が発生する場合があります。

次の手順は、自己署名証明書をサードパーティの証明書に置き換える必要がある場合にONTAPメディエーターを再初期化する手順を示しています。

タスクの内容

SnapMirror Active Sync クラスタの自己署名証明書をサードパーティの証明書に置き換え、ONTAP から ONTAP Mediator 設定を削除してから、ONTAP Mediator を追加する必要があります。

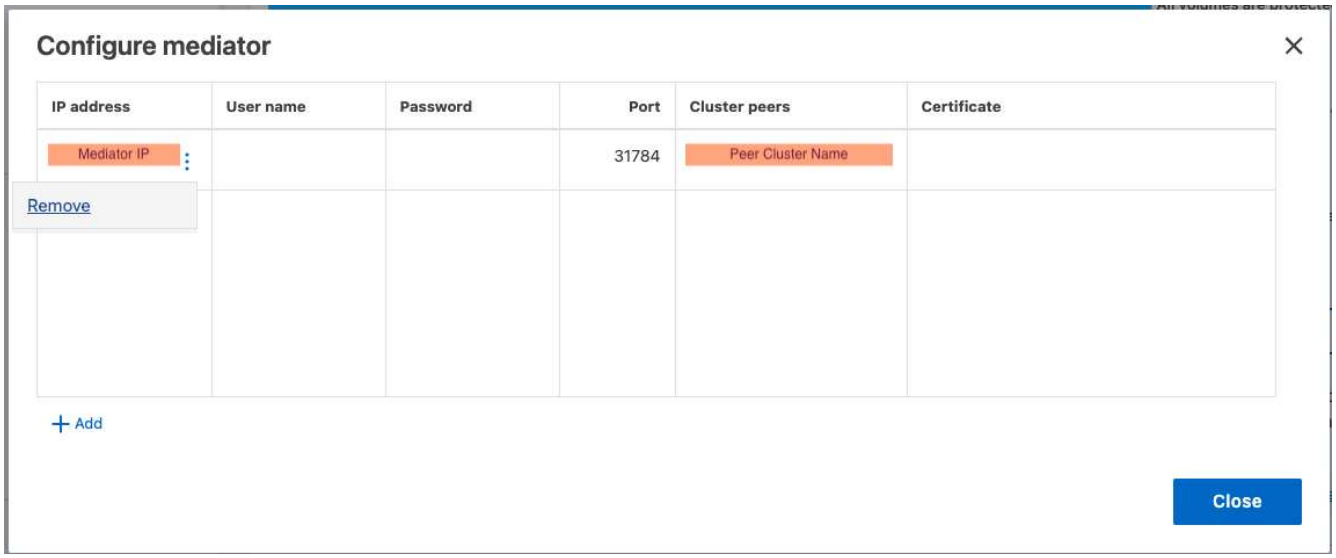
System Manager

System Manager では、古い自己署名証明書で設定された ONTAP Mediator バージョンを ONTAP クラスタから削除し、新しいサードパーティ証明書で ONTAP クラスタを再設定する必要があります。

手順

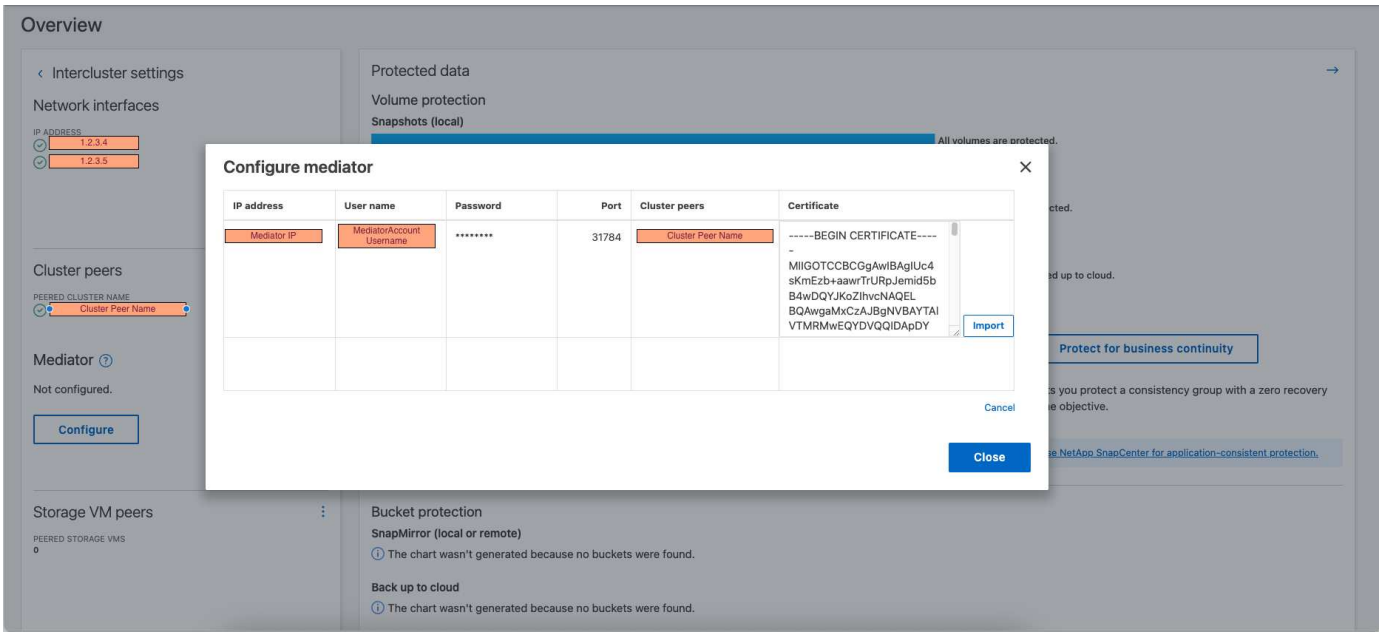
1. メニュー オプション アイコンを選択し、[削除] を選択して ONTAP Mediator を削除します。

> この手順では、自己署名されたserver-caがONTAPクラスタから削除されることはありません。NetAppでは、次の手順を実行してサードパーティ証明書を追加する前に、*[証明書]*タブに移動して手動で削除することを推奨しています。



2. 正しい証明書を使用して ONTAP Mediator を再度追加します。

ONTAP Mediator に新しいサードパーティの自己署名証明書が設定されました。



CLI

ONTAP CLI を使用して自己署名証明書をサードパーティの証明書に置き換えることで、プライマリ クラスタまたはセカンダリ クラスタから ONTAP Mediator を再初期化できます。

ONTAP Mediator 1.9以降

1. すべてのクラスタで自己署名証明書を使用していた場合は、以前にインストールした自己署名証明書を削除して `intermediate.crt`ください。次の例では、2つのクラスタがあります。

   例：

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 次のコマンドを使用して、以前に設定したONTAPメディエーターをSnapMirrorアクティブな同期クラスタから削除し `-force true`ます。

   例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 下位CA（と呼ばれる）から証明書を取得する方法については、の手順を参照してください"自己署名証明書を信頼できるサードパーティ証明書に置き換える"。 `intermediate.crt`自己署名証明書を信頼できるサードパーティ証明書に置き換える

には、 `intermediate.crt`ファイルに定義されているPKI権限に送信する必要がある要求から派生する特定のプロパティがあります。 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. ONTAPメディエーターLinux VM /ホストソフトウェアのインストール先から新しいサードパーティ製ONTAPメディエーターCA証明書を追加し `intermediate.crt`ます。

   例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. ファイルをピアクラスタに追加します `intermediate.crt`。すべてのピアクラスタについて、この手順を繰り返します。

   例：

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. 以前に設定したONTAPメディエーターをSnapMirrorアクティブな同期クラスタから削除します。

   例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator を再度追加します。

   例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status`SnapMirror整合性グループ関係がメディエーターと同期されているかどうかを示します。ステータス `true`は同期に成功したことを示します。

ONTAPメディエーター**1.8**以前

1. すべてのクラスタで自己署名証明書を使用していた場合は、以前にインストールした自己署名証明書を削除して `ca.crt`ください。次の例では、2つのクラスタがあります。

   例：

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 次のコマンドを使用して、以前に設定したONTAPメディエーターをSnapMirrorアクティブな同期クラスタから削除し `-force true`ます。

   例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 下位CA（と呼ばれる）から証明書を取得する方法については、の手順を参照してください"自己署名証明書を信頼できるサードパーティ証明書に置き換える"。 `ca.crt`自己署名証明書を信頼できるサードパーティ証明書に置き換える

   > には、 `ca.crt`ファイルに定義されているPKI権限に送信する必要がある要求から派生する特定のプロパティがあります。 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. ONTAPメディエーターLinux VM /ホストソフトウェアのインストール先から新しいサードパーティ製ONTAPメディエーターCA証明書を追加し `ca.crt`ます。

例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. ファイルをピアクラスタに追加します `intermediate.crt`。すべてのピアクラスタについて、この手順を繰り返します。

   例：

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. 以前に設定したONTAPメディエーターをSnapMirrorアクティブな同期クラスタから削除します。

   例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator を再度追加します。

   例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status`SnapMirror整合性グループ関係がメディエーターと同期されているかどうかを示します。ステータス `true`は同期に成功したことを示します。

関連情報

- "ジョブの表示"
- "セキュリティ証明書の削除"
- "セキュリティ証明書のインストール"
- "security certificate show"
- "スナップミラーメディエーターの追加"
- "スナップミラーメディエーターの削除"

- "スナップミラーメディエーターショー"

ONTAP Cloud Mediatorの設定準備

あなたの前に"ONTAP Cloud Mediatorを構成する"前提条件が満たされていることを確認する必要があります。

ファイアウォールの要件

ドメインコントローラのファイアウォール設定でHTTPSトラフィックを許可する必要があります。`api.bluexp.netapp.com`両方のクラスターから。

プロキシサーバーの要件

SnapMirror Active Sync にプロキシ サーバーを使用する場合は、プロキシ サーバーが作成されており、次のプロキシ サーバー情報があることを確認してください。

- HTTPSプロキシIP
- ポート
- ユーザ名
- パスワード

レイテンシー

NetAppコンソール クラウド サーバーとSnapMirrorアクティブ同期クラスター ピア間の推奨 ping 遅延は 200 ミリ秒未満です。

ルート**CA**証明書

クラスタの証明書を確認する

ONTAPには既知のルート CA 証明書がプリインストールされているため、ほとんどの場合、 NetAppコンソール サーバーのルート CA 証明書をインストールする必要はありません。Cloud Mediatorの設定を開始する前に、クラスタをチェックして証明書が存在することを確認できます。

例：

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
```

```
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
```

```
ca
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

プロキシサーバーにインストールされている証明書を確認する

NetAppコンソールでプロキシを使用してONTAP Cloud Mediator サービスに接続する場合は、プロキシ サーバーのルート CA 証明書がONTAPにインストールされていることを確認します。

例：

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

CA 証明書をダウンロードします。

必要に応じて、証明機関の Web サイトからルート CA 証明書をダウンロードし、クラスターにインストールできます。

例：

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

SnapMirror Active Sync 用の**ONTAP Cloud Mediator** を構成する

ONTAP 9.17.1以降では、 ONTAP Cloud Mediatorを使用して各クラスタの健全性を監視することで、ビジネス継続性を実現できます。ONTAPONTAP Mediatorはクラウドベースのサービスです。ONTAPONTAP Cloud Mediator をSnapMirror Active Sync と併用する場合は、まずNetAppコンソール サービスとクライアント情報が設定されていることを確認し、適切なクラスタ ピアリングを確保する必要があります。

ONTAP Mediatorと同様に、 ONTAP Cloud Mediatorは、 SnapMirror Active Sync関係にあるONTAPクラスタで使用される高可用性（HA）メタデータ用の永続的かつフェンスされたストアを提供します。ONTAPONTAP Mediatorは、クォーラムの決定を支援する同期ノードヘルスクエリ機能を提供し、コントローラの稼働状態検出のためのpingプロキシとして機能します。

ONTAP 9.17.1でSnapMirror Active SyncとONTAP MediatorまたはONTAP Cloud Mediatorを使用している場合は、*既知の問題と制限*を確認してください。"ONTAPリリースノート"これらの構成に関する重要な情報については、こちらをご覧ください。

開始する前に

ONTAP Cloud Mediator を設定する前に、次の情報を確認する必要があります。

- クラスターが構成されました。

  "SnapMirror Active Sync 用にONTAPクラスタを構成する"

- NetAppコンソールからNetAppコンソール組織 ID をコピーし、 ONTAP Cloud Mediator を構成するときに使用するコンソール メンバー サービス アカウントを作成しました。サービスアカウントを作成する際は、組織をONTAP Cloud Mediatorを設定したサブスクリプションに設定する必要があります。カテゴリは*アプリケーション*、ロールタイプは* ONTAP Mediatorセットアップロール*に設定する必要があります。ロールを作成する際に、クライアントIDとクライアントシークレットを保存してください。

  "NetAppコンソールのメンバーとサービスアカウントを追加する"

手順

System Manager またはONTAP CLI を使用してONTAP Cloud Mediator を追加できます。

System Manager

1. 保護 **>** 概要 **>** メディエーター に移動し、追加 を選択します。
2. メディエーターの追加 ウィンドウで、メディエーターの種類として クラウド を選択し、次の情報を入力します。
   - NetAppコンソール組織ID
   - NetAppコンソールクライアントID
   - NetAppコンソールクライアントシークレット
3. クラスター ピアを選択します。
4. HTTP プロキシを使用しており、まだ構成されていない場合は、ローカル ホストとリモート ホストの HTTP プロキシ情報を入力します。

   クラスター ピアごとに異なるプロキシ サーバーを使用することをお勧めします。
5. オプション: ONTAPにルート CA 証明書をインストールする必要がある場合 (特にプロキシ サーバを使用している場合)、指定されたテキスト ボックスに証明書を貼り付けます。
6. 「 * 追加」を選択します。
7. **[保護] > [概要]** に移動し、 SnapMirrorアクティブ同期クラスタとONTAP Cloud Mediator 間の関係のステータスを確認します。

CLI

1. ONTAP Cloud Mediator を設定します。
   ```
   snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp
   -org-id <NetApp Console Organization ID> -service-account-client-id
   <Service Account Client ID> -use-http-proxy-local <true|false> -use-http
   -proxy-remote <true|false>
   ```
2. ONTAP Cloud Mediator のステータスを確認します。
   ```
   snapmirror mediator show
   ```

   例：

   ```
   C1_cluster::> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   Type
   ---------------- ---------------- ----------------- -------------
   -------
   0.0.0.0          C2_cluster       connected         true
   cloud
   ```

ONTAP SnapMirror Active Syncで保護

SnapMirrorアクティブ同期は、非対称保護を提供し、ONTAP 9 .15.1以降では対称アクティブ/アクティブ保護を提供します。

SnapMirrorアクティブ同期を使用した非対称保護を設定するには、ONTAPソース クラスタでLUNを選択し、整合性グループに追加します。

開始する前に

- SnapMirror同期ライセンスが必要です。
- クラスタ管理者またはStorage VM管理者である必要があります。
- 整合性グループ内のコンスティチュエントボリュームは、すべて1つのStorage VM（SVM）に含まれている必要があります。
  - LUNは異なるボリュームに配置できます。
- ソースとデスティネーションのクラスタを同じにすることはできません。
- ASAクラスタと非ASAクラスタの間にSnapMirrorアクティブ同期整合性グループ関係を確立することはできません。
- SnapMirrorアクティブ同期でクラスタ ピア関係を確立するには、デフォルトのIPspaceが必要です。カスタムのIPspaceはサポートされていません。
- 整合グループの名前は一意である必要があります。
- セカンダリ（デスティネーション）クラスタ上のボリュームのタイプはDPである必要があります。
- プライマリとセカンダリのSVMでピア関係が確立されている必要があります。

手順

ONTAP CLIまたはSystem Managerを使用して整合グループを設定できます。

ONTAP 9.10.1以降、 ONTAPはSystem Managerにコンシステンシーグループのエンドポイントとメニューを追加し、追加の管理ユーティリティを提供します。ONTAPONTAP以降をご利用の場合は、以下を参照してください。 "整合グループの設定"それから"保護の設定" SnapMirrorアクティブ同期関係を作成します。

ONTAP 9.14.1 から 9.8 では、 SnapMirror Active Sync はSnapMirror Business Continuity (SM-BC) と呼ばれます。

System Manager

1. プライマリクラスタで、*[保護]>[概要]>[ビジネス継続性のための保護]>[LUNの保護]*に移動します。
2. 保護するLUNを選択し、保護グループに追加します。
3. デスティネーションのクラスタとSVMを選択します。
4. * 初期化関係 * がデフォルトで選択されています。[保存（ Save ）] をクリックして保護を開始します。
5. [Dashboard] > [Performance] に移動して、 LUN の IOPS アクティビティを確認します。
6. デスティネーションクラスタで、 System Manager を使用して、ビジネス継続性関係の保護が同期されていることを確認します。 * Protection > Relationships * 。

CLI

1. デスティネーションクラスタから整合性グループ関係を作成
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   コマンドのパラメータを `snapmirror create`使用して、最大12個のコンスティチュエントボリュームをマッピングできます `cg-item-mappings`。

   次の例では、2つの整合グループ（と `vol2`、1つのミラーデスティネーション整合グループ）`cg_dst`を作成し `cg_src_ on the source with `vol1`ます。

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. デスティネーションクラスタから、整合性グループを初期化します。

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. 初期化処理が正常に完了したことを確認します。ステータスはになります `InSync`。

   ```
   snapmirror show
   ```

4. 各クラスタにigroupを作成して、アプリケーションホストのイニシエータにLUNをマッピングします。
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

   の詳細については `lun igroup create`、を"ONTAPコマンド リファレンス"参照してください。

5. 各クラスタで、LUNをigroupにマッピングします。

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. コマンドを使用して、LUNマッピングが完了したことを確認します `lun map`。その後、アプリケーションホストで新しいLUNを検出できます。

対称保護は、System ManagerまたはONTAP CLIを使用して確立できます。どちらのインターフェイスでも、には異なる手順があります均一なコンフィギュレーションと非均一なコンフィギュレーション。

開始する前に

- 両方のクラスタでONTAP 9 .15.1以降が実行されている必要があります。
- 対称アクティブ/アクティブ構成には保護ポリシーが必要 `AutomatedFailoverDuplex`です。または、をに `automated-failover-duplex`指定する `-type`こともできますカスタムのSnapMirrorポリシーを作成する。
- ONTAP 9.15.1では、対称アクティブ/アクティブ構成は2ノードクラスタでのみサポートされます。
- ONTAP 9.16.1 GA以降では、SnapMirror Active Syncで4ノードクラスタの対称アクティブ/アクティブ構成がサポートされます。
  - 4ノードクラスタでSnapMirrorアクティブ同期を使用するには、ONTAP 9.16.1 GA以降を実行している必要があります。
  - 4ノード構成を導入する前に、を実行する必要がありクラスタピア関係を作成します。ます。
  - 4ノードクラスタのを確認します制限。
  - 2ノードクラスタにリバートする場合は、リバート前にSnapMirrorのアクティブな同期関係をクラスタから削除する必要があります。
  - 4ノード構成を使用して、ストレージとコントローラをアップグレードできます。このプロセスは無停止で実行され、ボリュームを新しいノードに移動する間にクラスタを拡張します。詳細については、を参照してください "クラスタをリフレッシュします。"。
- ONTAP 9.17.1 以降では、両方のクラスタがONTAP 9.17.1 以降を実行している場合にのみ、NVMe 名前空間で対称アクティブ/アクティブ保護を設定できます。

SCSI SnapMirrorアクティブ同期構成を使用して対称アクティブ/アクティブ保護を構成する

手順

System Manager またはONTAP CLI を使用して、SCSI プロトコル ホスト マッピングを使用した対称アクティブ/アクティブ保護を設定できます。

System Manager

統一された構成の手順

1. プライマリサイトで、"新しいLUNを使用して整合グループを作成します。"
   a. 整合グループを作成するときは、ホストイニシエータを指定してigroupを作成します。
   b. [**Enable SnapMirror *]チェックボックスをオンにして、ポリシーを選択します `AutomatedFailoverDuplex`。
   c. 表示されるダイアログボックスで、[**replicate initiator groups**]チェックボックスを選択してigroupをレプリケートします。[***Edit proximity settings**]で、ホストの近接SVMを設定します。
   d. 保存を選択します。

不均一な構成の手順

1. プライマリサイトで、"新しいLUNを使用して整合グループを作成します。"
   a. 整合グループを作成するときは、ホストイニシエータを指定してigroupを作成します。
   b. [**Enable SnapMirror *]チェックボックスをオンにして、ポリシーを選択します `AutomatedFailoverDuplex`。
   c. [***Save**]を選択して、LUN、整合グループ、igroup、SnapMirror関係、igroupマッピングを作成します。
2. セカンダリサイトでigroupを作成し、LUNをマッピングします。
   a. **Hosts> SAN Initiator Groups**に移動します。
   b. 新しいigroupを作成するには、[***+Add**]を選択します。
   c. **Name** を指定し、 **Host Operating System** を選択してから、 **Initiator Group Members** を選択します。
   d. 関係を初期化するには、[***Save**]を選択します。
3. 新しいigroupをデスティネーションLUNにマッピングします。
   a. ストレージ> **LUNs**に移動します。
   b. igroupにマッピングするLUNをすべて選択します。
   c. **More** を選択してから **Map to Initiator Groups** を選択します。

CLI

統一された構成の手順

1. アプリケーション内のすべてのボリュームをグループ化して新しいSnapMirror関係を作成します。双方向の同期レプリケーションを確立するためのポリシーを指定して `AutomatedFailOverDuplex`ください。

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   例: 次の例では、ソースに vol1 と vol2 を含む cg_src という 2 つの整合性グループを作成し、宛先にミラー化された整合性グループ cg_dst を作成します。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. SnapMirror関係を初期化します。
`snapmirror initialize -destination-path <destination-consistency-group>`
3. がおよび `Relationship Status`と表示される `SnapMirrored`のを待って、処理が成功したことを確認します `Mirrored State Insync。

```
snapmirror show -destination-path <destination_path>
```

4. ホストで、必要に応じて各クラスタにアクセスできるようにホスト接続を設定します。
5. igroup設定を確立します。ローカル クラスタのイニシエータの優先パスを設定します。逆アフィニティを実現するために設定をピアクラスタにレプリケートするオプションを指定します。

```
SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
<igroup_name> -replication-peer <peer_svm_name> -initiator <host>
```

ONTAP 9.16.1以降では、このコマンドでパラメータを使用し `-proximal-vserver local` ます。

```
SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
<os_type> -initiator <host>
```

ONTAP 9.16.1以降では、このコマンドでパラメータを使用し `-proximal-vserver peer` ます。

6. ホストからパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。
7. アプリケーションを導入し、VMワークロードをクラスタ間に分散して、必要な負荷分散を実現します。

不均一な構成の手順

1. アプリケーション内のすべてのボリュームをグループ化して新しいSnapMirror関係を作成します。双方向の同期レプリケーションを確立するためのポリシーを指定して `AutomatedFailOverDuplex`ください。

```
snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source_volume:@destination_volume>
-policy AutomatedFailOverDuplex
```

例: 次の例では、ソースに vol1 と vol2 を含む cg_src という 2 つの整合性グループを作成し、宛先にミラー化された整合性グループ cg_dst を作成します。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. SnapMirror関係を初期化します。
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. がおよび `Relationship Status`と表示される `SnapMirrored`のを待って、処理が成功したことを確認します `Mirrored State Insync。

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. ホストで、必要に応じて各クラスタにアクセスできるようにホスト接続を設定します。
5. ソースとデスティネーションの両方のクラスタでigroup構成を確立します。

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. ホストからパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。
7. アプリケーションを導入し、VMワークロードをクラスタ間に分散して、必要な負荷分散を実現します。

NVMe SnapMirrorアクティブ同期構成を使用して対称アクティブ/アクティブ保護を構成する

開始する前に

対称アクティブ/アクティブ保護を構成するための要件に加えて、NVMe プロトコルを使用するときは、サポートされている構成とサポートされていない構成に注意する必要があります。

- 整合性グループには 1 つ以上のサブシステムを含めることができます。
- 整合性グループ内のボリュームには、複数のサブシステムからの名前空間マップを設定できます。
- サブシステムは、複数の整合性グループに属する名前空間マップを持つことはできません。
- サブシステムには、整合性グループに属する名前空間マップと整合性グループに属さない名前空間マップを混在させることはできません。
- サブシステムには、同じ整合性グループの一部である名前空間マップが必要です。

手順

ONTAP 9.17.1 以降では、System Manager またはONTAP CLI を使用してコンシステンシ グループを作成し、NVMe プロトコル ホスト マッピングを使用して対称アクティブ/アクティブ保護を設定できます。

System Manager

1. プライマリサイトでは、 "新しいボリュームまたは NVMe 名前空間を使用して整合性グループを作成します。"
2. *+追加*を選択し、*新しいNVMe名前空間の使用*を選択します。
3. 一貫性グループ名を入力します。
4. *詳細*を選択します。
5. 保護*セクションで SnapMirrorを有効にする*を選択し、 `AutomatedFailoverDuplex`ポリシー。
6. ホスト マッピング セクションで、既存の **NVMe** サブシステム または 新しい **NVMe** サブシステム のいずれかを選択します。
7. 近接SVMを変更するには、「近接」を選択してください。デフォルトではソースSVMが選択されています。
8. 必要に応じて、別の NVMe サブシステムを追加します。

CLI

1. で使用されるすべてのNVMeネームスペースを含むすべてのボリュームをグループ化する新しいSnapMirror関係を作成します。 `AutomatedFailOverDuplex`双方向同期レプリケーションを確立するためのポリシー。

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   例：

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. SnapMirror関係を初期化します。
   `snapmirror initialize -destination-path <destination-consistency-group>`

   例：

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. がおよび `Relationship Status`と表示される `SnapMirrored`のを待って、処理が成功したことを確認します `Mirrored State Insync。

   ```
   snapmirror show -destination-path <destination_path>
   ```

   プライマリ ボリューム内の NVMe 名前空間に関連付けられた NVMe サブシステムは、セカンダリ クラスターに自動的に複製されます。

4. ホストで、必要に応じて各クラスタにアクセスできるようにホスト接続を設定します。
5. 各ホストに近接するSVMを指定します。これにより、優先クラスタからのパスを使用してNVMeネームスペースへのホストアクセスが可能になります。これは、プライマリクラスタ内のSVM、またはDRクラスタ内のSVMのいずれかになります。

   次のコマンドは、SVM VS_A がホスト H1 に近いことを示し、VS_A を近位 SVM として設定します。

   ```
   SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
   -proximal-vservers <VS_A>
   ```

   次のコマンドは、SVM VS_B がホスト H2 に近いことを示し、VS_B を近位 SVM として設定します。

   ```
   SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
   -proximal-vservers <VS_B>
   ```

6. ホストからパスを検出し、優先クラスターからストレージへのアクティブ/最適化されたパスがホストにあることを確認します。
7. アプリケーションを導入し、VMワークロードをクラスタ間に分散して、必要な負荷分散を実現します。

関連情報

- "スナップミラー作成"
- "スナップミラーの初期化"
- "snapmirror show"

既存の**ONTAP SnapMirror**関係を**SnapMirror Active Sync** 関係に変換する

SnapMirror保護を設定している場合は、関係をSnapMirrorアクティブ同期に変換できます。ONTAP 9.15.1以降では、対称アクティブ / アクティブ保護を使用するように関係を変換できます。

既存の **iSCSI** または **FC SnapMirror**関係を非対称**SnapMirror**アクティブ同期関係に変換します。

ソース クラスタと宛先クラスタ間に既存の iSCSI または FC SnapMirror同期関係がある場合は、それを非対称SnapMirrorアクティブ同期関係に変換できます。そうすることで、ミラー ボリュームを整合性グループに関連付けることができ、複数のボリュームにわたるワークロード全体でRPOゼロを確保できます。また、SnapMirrorアクティブ同期関係を確立する前に特定の時点にリバートする必要がある場合には、既存のSnapMirror Snapshotを保持できます。

タスクの内容

- プライマリクラスタとセカンダリクラスタのクラスタ管理者およびSVM管理者である必要があります。
- SnapMirrorポリシーを変更してRPOゼロの同期をRTOゼロの同期に変換することはできません。
- コマンドを実行する前に、LUNのマッピングが解除されていることを確認する必要があります `snapmirror create`。

  セカンダリボリューム上の既存のLUNがマッピングされていて、ポリシーが設定されている場合

AutomatedFailover、 `snapmirror create`エラーがトリガーされます。

開始する前に

- プライマリ クラスタとセカンダリ クラスタの間には、ゼロ RPO SnapMirror同期関係が存在する必要があります。
- RTOゼロのSnapMirror関係を作成するには、デスティネーションボリューム上のすべてのLUNのマッピングを解除する必要があります。
- SnapMirrorアクティブ同期でサポートされるのはSANプロトコルのみです（NFS / CIFSはサポートされません）。整合性グループのコンスティチュエントがNASアクセス用にマウントされていないことを確認します。
- "ONTAP Mediator" SnapMirrorアクティブ同期を設定する必要があります。

手順

1. セカンダリクラスタから、既存の関係に対してSnapMirror更新を実行します。

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirrorの更新が正常に完了したことを確認します。

```
SiteB::>snapmirror show
```

3. RPOゼロの各同期関係を一時停止します。

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. RPOゼロの各同期関係を削除します。

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. ソースSnapMirror関係を解放しますが、共通のSnapshotは保持します。

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. RTOゼロのSnapMirror同期関係を作成します。

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. 整合グループを再同期します。

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

既存の**iSCSI**または**FC SnapMirror**関係を対称アクティブ/アクティブに変換する

ONTAP 9.15.1 以降では、既存の iSCSI または FC SnapMirror関係をSnapMirrorアクティブ同期対称アクティブ/アクティブ関係に変換できます。

開始する前に

- ONTAP 9.15.1以降が実行されている必要があります。
- プライマリクラスタとセカンダリクラスタの間に、RPOゼロのSnapMirror同期関係が存在している必要があります。
- RTOゼロのSnapMirror関係を作成するには、デスティネーションボリューム上のすべてのLUNのマッピングを解除する必要があります。
- SnapMirrorアクティブ同期でサポートされるのはSANプロトコルのみです（NFS / CIFSはサポートされません）。整合性グループのコンスティチュエントがNASアクセス用にマウントされていないことを確認します。
- "ONTAP Mediator" SnapMirrorアクティブ同期を設定する必要があります。

手順

1. セカンダリクラスタから、既存の関係に対してSnapMirror更新を実行します。

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirrorの更新が正常に完了したことを確認します。

```
SiteB::>snapmirror show
```

3. RPOゼロの各同期関係を一時停止します。

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. RPOゼロの各同期関係を削除します。

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. ソースSnapMirror関係を解放しますが、共通のSnapshotは保持します。

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. AutomatedFailoverDuplexポリシーを使用してRTOゼロのSnapMirror同期関係を作成します。

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
```

```
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. 既存のホストがローカルのプライマリクラスタの場合は、ホストをセカンダリクラスタに追加し、各クラスタへのそれぞれのアクセスとの接続を確立します。
8. セカンダリサイトで、リモートホストに関連付けられたigroupのLUNマップを削除します。

   igroupにレプリケートされていないLUNのマッピングが含まれていないことを確認します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. プライマリサイトで、既存のホストのイニシエータ設定を変更して、ローカルクラスタのイニシエータの近接パスを設定します。

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. 新しいホスト用の新しいigroupとイニシエータを追加し、ホストとローカルサイトのアフィニティを設定します。igroupレプリケーションを有効にして設定をレプリケートし、リモートクラスタのホストローカル性を反転

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. ホスト上のパスを検出し、優先クラスタからストレージLUNへのアクティブ/最適化パスがホストにあることを確認する
12. アプリケーションを導入し、VMワークロードをクラスタ間に分散します。
13. 整合グループを再同期します。

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーの静止"
- "スナップミラーリリース"
- "snapmirror resync"
- "snapmirror show"

ONTAP SnapMirrorのアクティブ同期関係タイプを変換する

ONTAP 9 .15.1以降では、SnapMirrorアクティブ同期保護のタイプ（非対称から対称アク

ティブ/アクティブ、またはその逆）を変換できます。

対称アクティブ/アクティブ関係への変換

非対称保護を使用した iSCSI または FC SnapMirrorアクティブ同期関係を、対称アクティブ/アクティブを使用するように変換できます。

開始する前に

- 両方のクラスタでONTAP 9 .15.1以降が実行されている必要があります。
- 対称アクティブ/アクティブ構成には保護ポリシーが必要 `AutomatedFailoverDuplex`です。または、をに `automated-failover-duplex`指定する `-type`こともできますカスタムのSnapMirrorポリシーを作成する。

System Manager

統一された構成の手順

1. デスティネーションigroupを削除します。
   a. デスティネーションクラスタで、**Hosts> SAN Initiator Groups**に移動します。
   b. SnapMirror関係があるigroupを選択し、**Delete** を選択します。
   c. ダイアログボックスで、[**Unmap the associated LUNs*]**ボックスを選択し、**[**Delete*]を選択します。
2. SnapMirrorのアクティブな同期関係を編集します。
   a. 保護>関係に移動します。
   b. 変更するリレーションシップの横にあるKabobメニューを選択し、編集を選択します。
   c. 保護ポリシーをAutomatedFailoverDuplexに変更します。
   d. を選択する `AutoMatedFailoverDuplex`と、ホストプロキシミティ設定を変更するダイアログボックスが表示されます。イニシエータの場合は、[**Initiator Proximal to *]**の適切なオプションを選択してから、**[** Initiator Proximal to *]を選択します。
   e. 保存を選択します。
3. [***Protection***]メニューで、関係がと表示されたら操作が成功したことを確認します `InSync`。

不均一な構成の手順

1. デスティネーションigroupを削除します。
   a. セカンダリサイトで、**Hosts>SAN Initiator Groups**に移動します。
   b. SnapMirror関係があるigroupを選択し、**Delete** を選択します。
   c. ダイアログボックスで、[**Unmap the associated LUNs*]**ボックスを選択し、**[**Delete*]を選択します。
2. 新しいigroupを作成します。
   a. デスティネーションサイトの[**SAN**イニシエータグループ**]**メニューで、**[**追加*]を選択します。
   b. **Name** を指定し、 **Host Operating System** を選択してから、 **Initiator Group Members** を選択します。
   c. 保存を選択します。
3. 新しいigroupをデスティネーションLUNにマッピングします。
   a. ストレージ> **LUNs**に移動します。
   b. igroupにマッピングするLUNをすべて選択します。
   c. **More** を選択してから **Map to Initiator Groups** を選択します。
4. SnapMirrorのアクティブな同期関係を編集します。
   a. 保護>関係に移動します。
   b. 変更するリレーションシップの横にあるKabobメニューを選択し、編集を選択します。
   c. 保護ポリシーをAutomatedFailoverDuplexに変更します。
   d. AutoMatedFailoverDuplexを選択すると、ホストプロキシミティ設定を変更するオプションが開

始されます。イニシエータの場合は、[**Initiator Proximal to *]**の適切なオプションを選択してから、**[** Initiator Proximal to *]を選択します。

e. 保存を選択します。

5. **[*Protection]**メニューで、関係がと表示されたら操作が成功したことを確認します `InSync`。

CLI

統一された構成の手順

1. SnapMirrorポリシーをからに `AutomatedFailoverDuplex`変更し `AutomatedFailover`ます。

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. ポリシーを変更すると再同期がトリガーされます。再同期が完了してから、関係が次のようになっていることを確認し `Insync`ます。

```
snapmirror show -destination-path <destination_path>
```

3. 既存のホストがローカルのプライマリクラスタの場合は、ホストを2番目のクラスタに追加し、各クラスタへのそれぞれのアクセスとの接続を確立します。

4. セカンダリサイトで、リモートホストに関連付けられたigroupのLUNマップを削除します。

> igroupにレプリケートされていないLUNのマッピングが含まれていないことを確認します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. プライマリサイトで、権限レベルをに設定し `advanced`ます。

```
SiteA::> set -privilege advanced
```

6. 既存のホストのイニシエータ設定を変更して、ローカルクラスタ上のイニシエータの近接パスを設定します。

```
SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
-initiator <host> -proximal-vserver <server>
```

> この手順が完了したら、権限レベルをadminに戻すことができます。

7. 新しいホスト用の新しいigroupとイニシエータを追加し、ホストとローカルサイトのアフィニティを設定します。igroupレプリケーションを有効にして設定をレプリケートし、リモートクラスタのホストローカル性を反転

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
host2 -proximal-vserver vsB
```

8. ホスト上のパスを検出し、優先クラスタからストレージLUNへのアクティブ/最適化パスがホストに

あることを確認する

9. アプリケーションを導入し、VMワークロードをクラスタ間に分散します。

不均一な構成の手順

1. SnapMirrorポリシーをからに `AutomatedFailoverDuplex`変更し `AutomatedFailover`ます。

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. ポリシーを変更すると再同期がトリガーされます。再同期が完了してから、関係が次のようになっていることを確認し `Insync`ます。

```
snapmirror show -destination-path <destination_path>
```

3. 既存のホストがプライマリクラスタに対してローカルである場合は、ホストを2番目のクラスタに追加し、各クラスタへのそれぞれのアクセスとの接続を確立します。
4. セカンダリサイトで、新しいホスト用の新しいigroupとイニシエータを追加し、ローカルサイトへのホストアフィニティを設定します。LUNをigroupにマッピングします。

```
SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
<host_name>
SiteB::> lun mapping create -igroup <igroup> -path <path_name>
```

5. ホスト上のパスを検出し、優先クラスタからストレージLUNへのアクティブ/最適化パスがホストにあることを確認する
6. アプリケーションを導入し、VMワークロードをクラスタ間に分散します。

対称アクティブ/アクティブ関係から非対称**iSCSI**または**FC**関係に変換する

iSCSI または FC を使用して対称アクティブ/アクティブ保護を構成した場合は、 ONTAP CLI を使用して関係を非対称保護に変換できます。

手順

1. すべてのVMワークロードを、ソースクラスタのローカルホストに移動します。
2. VMインスタンスを管理していないホストのigroup設定を削除し、igroup設定を変更してigroupのレプリケーションを終了します。

```
igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
```

3. セカンダリサイトで、LUNのマッピングを解除します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

4. セカンダリサイトで、対称アクティブ/アクティブ関係を削除します。

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. プライマリサイトで、対称アクティブ/アクティブ関係を解放します。
   `SiteA::> snapmirror release -destination-path <destination_path> -relationship -info-only true`
6. セカンダリサイトで、ポリシーを使用して同じ一連のボリュームに対する関係を作成し `AutomatedFailover`、関係を再同期します。

```
SiteB::> snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source:@destination> -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
<policy_type>
```

> セカンダリサイトの整合性グループは、関係を再作成する前に必要です"削除対象"。デスティネーションボリューム"DPタイプに変換する必要があります"。ボリュームをDPに変換するには、ポリシー `MirrorAndVault`以外のコマンド、、 `MirrorAllSnapshots`または `Sync`を指定して-`AutomatedFailover`実行し `snapmirror resync`ます。

7. 関係のミラー状態が関係ステータスがである `Insync`ことを確認します `Snapmirrored`。

   `snapmirror show -destination-path *destination_path*`

8. ホストからパスを再検出します。

関連情報

- "SnapMirrorの削除"
- "スナップミラーの変更"
- "スナップミラーリリース"
- "snapmirror resync"
- "snapmirror show"

SnapMirrorアクティブ同期の管理とデータの保護

ONTAPコンシステンシグループ間で共通のスナップショットを作成する

定期的なSnapshot処理のほかに、プライマリSnapMirror整合性グループ内のボリュームとセカンダリSnapMirror整合性グループ内のボリューム間で共通のを手動で作成することができます"Snapshot"。

タスクの内容

スケジュールされたSnapshot作成間隔は12時間です。

開始する前に

- SnapMirrorグループ関係が同期されている必要があります。

手順

1. 共通のSnapshotを作成します。

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. 更新の進捗状況を監視します。

   ```
   destination::>snapmirror show -fields newest-snapshot
   ```

関連情報

- "snapmirror show"

SnapMirrorアクティブ同期関係にある**ONTAP**クラスタの計画的なフェイルオーバーを実行する

SnapMirrorのアクティブな同期関係にあるONTAPクラスタの計画的フェイルオーバーでは、プライマリクラスタからセカンダリクラスタにテイクオーバーされるように、プライマリクラスタとセカンダリクラスタのロールを切り替えます。フェイルオーバー中は、通常はセカンダリクラスタがクライアントの処理を中断せずにローカルで入出力要求を処理します。

計画的フェイルオーバーを実行して、ディザスタリカバリ構成の健全性をテストしたり、プライマリクラスタでメンテナンスを実行したりすることができます。

タスクの内容

計画的フェイルオーバーは、セカンダリクラスタの管理者が開始します。この処理では、セカンダリクラスタがプライマリからテイクオーバーするように、プライマリとセカンダリのロールを切り替える必要があります。新しいプライマリクラスタでは、クライアントの処理を中断することなく、入出力要求の処理をローカルで開始できます。

開始する前に

- SnapMirrorのアクティブな同期関係が同期されている必要があります。
- ノンストップオペレーションの実行中は、計画的フェイルオーバーを開始できません。ノンストップオペレーションには、ボリュームの移動、アグリゲートの再配置、ストレージフェイルオーバーなどがあります。
- ONTAPメディエーターが設定され、接続され、クォーラムを構成している必要があります。

手順

計画的フェイルオーバーは、ONTAP CLIまたはSystem Managerを使用して実行できます。

System Manager

ONTAP 9.14.1 から 9.8 では、 SnapMirror Active Sync はSnapMirror Business Continuity (SM-BC) と呼ばれます。

1. System Managerで、[**Protection]>[Overview]>[Relationships]の順に選択します。
2. フェイルオーバーするSnapMirrorのアクティブな同期関係を特定します。関係名の横にあるを選択し、[***Failover**]を選択し `…`ます。
3. フェイルオーバーのステータスを監視するには、ONTAP CLIでを使用し `snapmirror failover show`ます。

CLI

1. デスティネーションクラスタから、フェイルオーバー処理を開始します。

```
destination::>snapmirror failover start -destination-path
vs1_dst:/cg/cg_dst
```

2. フェイルオーバーの進行状況を監視します。

```
destination::>snapmirror failover show
```

3. フェイルオーバー処理が完了したら、デスティネーションからSnapMirror同期保護関係のステータスを監視できます。

```
destination::>snapmirror show
```

関連情報

- "スナップミラーフェイルオーバー表示"
- "スナップミラーフェイルオーバーの開始"
- "snapmirror show"

計画外の自動**ONTAP**クラスタ フェイルオーバー操作からの回復

自動計画外フェイルオーバー（AUFO）処理は、プライマリ クラスタが停止しているか分離されている場合に実行されます。ONTAP Mediatorは、フェイルオーバーの発生を検出し、セカンダリ クラスタへの自動計画外フェイルオーバーを実行します。セカンダリ クラスタがプライマリに変換されてクライアントへのデータの提供を開始します。この処理は、ONTAP Mediatorが使用されている場合にのみ実行されます。

自動計画外フェイルオーバーが実行されたあと、ホストのLUN I/Oパスを再スキャンしてI/Oパスの損失がないことを確認することが重要です。

計画外フェイルオーバー後の保護関係の再確立

保護関係は、System ManagerまたはONTAP CLIを使用して再確立できます。

System Manager

手順

ONTAP 9.14.1 から 9.8 では、 SnapMirror Active Sync はSnapMirror Business Continuity (SM-BC) と呼ばれます。

1. 保護 > リレーションシップ に移動し、リレーションシップの状態が「InSync」と表示されるまで待ちます。
2. 元のソースクラスタで処理を再開するには、をクリック ⋮ して*[フェイルオーバー]*を選択します。

CLI

自動計画外フェイルオーバーのステータスは、コマンドを使用して監視できます `snapmirror failover show`。

例：

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
          Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

イベントメッセージと対処方法については、を参照して"EMSリファレンス"ください。

フェイルオーバー後にファンアウト構成で保護を再開する

ONTAP 9.15.1以降では、SnapMirrorアクティブ同期でフェイルオーバーイベント後のファンアウトレッグの自動再設定がサポートされます。非同期ファンアウトレッグには、整合性グループ関係または独立したボリューム関係を指定できます。詳細については、を参照してください "ファンアウト構成"。

ONTAP 9 14.1以前を使用していて、SnapMirrorのアクティブな同期関係にあるセカンダリクラスタでフェイルオーバーが発生すると、SnapMirrorの非同期デスティネーションは正常な状態ではなくなります。SnapMirrorの非同期エンドポイントとの関係を削除して再作成し、保護を手動でリストアする必要があります。

手順

1. フェイルオーバーが正常に完了したことを確認します。
   `snapmirror failover show`
2. SnapMirror非同期エンドポイントで、ファンアウトエンドポイントを削除します。
   `snapmirror delete -destination-path` *`destination_path`*

3. 3番目のサイトで、新しいSnapMirrorアクティブな同期のプライマリボリュームと非同期のファンアウトデスティネーションボリュームの間にSnapMirror非同期関係を作成します。
`snapmirror create -source-path source_path -destination-path destination_path -policy MirrorAllSnapshots -schedule schedule`
4. 関係を再同期します。
`snapmirror resync -destination-path destination_path`
5. 関係のステータスと健全性を確認します。
`snapmirror show`

関連情報

- "スナップミラー作成"
- "SnapMirrorの削除"
- "スナップミラーフェイルオーバー表示"
- "snapmirror resync"
- "snapmirror show"

ONTAP SnapMirrorのアクティブ同期操作を監視する

次のSnapMirrorのアクティブな同期処理を監視して、SnapMirrorのアクティブな同期設定の健全性を確認できます。

- ONTAP Mediator
- 計画的フェイルオーバー処理
- 自動計画外フェイルオーバー処理
- SnapMirrorアクティブ同期の可用性

ONTAP 9.15.1以降では、どちらかのクラスタのSnapMirrorのアクティブな同期関係のステータスが表示されます。ONTAPメディエーターのステータスは、System Managerのどちらのクラスタからも監視できます。

ONTAP Mediator

通常運用時は、ONTAPメディエーターの状態は「connected」になります。それ以外の状態の場合は、エラー状態を示している可能性があります。では、エラーと適切な対処方法を確認できます"Event Management System（EMS；イベント管理システム）メッセージ"。

計画的フェイルオーバー処理

計画的フェイルオーバー処理のステータスと進捗状況は、コマンドを使用して監視できます `snapmirror failover show`。例：

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

フェイルオーバー処理が完了したら、新しいデスティネーション クラスタからSnapMirror保護のステータスを監視できます。例：

```
ClusterA::> snapmirror show
```

イベントメッセージと対処方法については、を参照して"EMSリファレンス"ください。

自動計画外フェイルオーバー処理

自動計画外フェイルオーバーの実行中は、コマンドを使用して処理のステータスを監視できます `snapmirror failover show`。

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
          Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

イベントメッセージと対処方法については、を参照して"EMSリファレンス"ください。

SnapMirrorアクティブ同期の可用性

SnapMirrorのアクティブな同期関係の可用性は、プライマリクラスタ、セカンダリクラスタ、またはその両方で一連のコマンドを使用して確認できます。

接続とクォーラムのステータスを確認するためのプライマリクラスタとセカンダリクラスタの両方でのコマンド、 `snapmirror show`および `volume show`コマンドが使用さ `snapmirror mediator show`れます。例：

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                    Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                     No-consensus
```

関連情報

- "スナップミラーフェイルオーバー表示"
- "スナップミラーフェイルオーバーの開始"
- "スナップミラーメディエーターショー"

ONTAPコンシステンシグループにボリュームを追加または削除する

アプリケーション ワークロードの要件が変更された場合は、ビジネス継続性を確保するために、整合性グループに対するボリュームの追加や削除が必要になることがありま

す。アクティブなSnapMirrorアクティブ同期関係でボリュームを追加および削除するプロセスは、使用しているONTAPのバージョンによって異なります。

ほとんどの場合、これは停止を伴うプロセスであり、SnapMirror関係を削除し、整合グループを変更してから保護を再開する必要があります。ONTAP 9 .13.1以降では、アクティブなSnapMirror関係が設定された整合グループにボリュームを追加する処理は無停止で実行されます。

タスクの内容

- ONTAP 9 .9.1では、ONTAP CLIを使用して整合グループにボリュームを追加または削除できます。
- ONTAP 9 .10.1以降では、System ManagerまたはONTAP REST APIを使用して管理することを推奨します"整合グループ"。

  ボリュームを追加または削除して整合性グループの構成を変更する場合は、最初に元の関係を削除してから、新しい構成で整合性グループを作成し直す必要があります。

- ONTAP 9.13.1以降では、アクティブなSnapMirror関係を持つ整合性グループに、ソースまたはデスティネーションから無停止でボリュームを追加できます。このアクションはNVMeプロトコルではサポートされていません。

  ボリュームの削除はシステム停止を伴う処理です。ボリュームを削除する前に、SnapMirror関係を削除する必要があります。

ONTAP 9.9.1～9.13.0

開始する前に

- 状態の整合グループは変更できません `InSync`。
- デスティネーションボリュームのタイプはDPでなければなりません。
- 整合性グループを拡張するために追加する新しいボリュームには、ソースボリュームとデスティネーションボリュームに共通のSnapshotのペアが必要です。

手順

2つのボリュームマッピングに例を示します `vol_src1`。←→ `vol_dst1`と `vol_src2←→ `vol_dst2`では、エンドポイントと `vs1_dst:/cg/cg_dst`間の整合性グループ関係を使用し `vs1_src:/cg/cg_src`ています。

1. ソースクラスタとデスティネーションクラスタで、コマンドを使用して、ソースクラスタとデスティネーションクラスタの間に共通のSnapshotがあることを確認します。 `snapshot show -vserver *svm_name* -volume *volume_name* -snapshot *snapmirror*`

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. 共通のSnapshotがない場合は、FlexVol SnapMirror関係を作成して初期化します。

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. 整合性グループ関係を削除します。

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

4. ソースSnapMirror関係を解放し、共通のSnapshotを保持します。

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. LUNのマッピングを解除し、既存の整合性グループ関係を削除します。

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   デスティネーションLUNのマッピングが解除され、プライマリ コピーのLUNでホストI/Oの処理が継続されます。

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **ONTAP 9.10.1～9.13.0**を使用している場合 ソース上のコンシステンシーグループを削除し、正しい構成で再作成してください。以下の手順に従ってください。 "整合グループを削除する"その後"単一の整合グループの設定" 。ONTAP 9.10.1以降では、System ManagerまたはONTAP REST APIで削除と作成の処理を実行する必要があります。CLIの手順はありません。

    ◦ ONTAP 9.9.1を使用している場合は、次の手順に進みます。**

7. デスティネーションに新しい構成で新しい整合性グループを作成します。

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. RTOゼロの整合性グループ関係を再同期して同期されていることを確認します。

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. 手順5でマッピングを解除したLUNを再マッピングします。

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

ONTAP 9.13.1以降

ONTAP 9.13.1以降では、アクティブなSnapMirrorのアクティブな同期関係を持つ整合性グループに無停止でボリュームを追加できます。SnapMirror Active Syncでは、ソースとデスティネーションの両方からボリュームを追加できます。

> ONTAP 9.14.1 から 9.8 では、 SnapMirror Active Sync はSnapMirror Business Continuity (SM-BC) と呼ばれます。

ソース整合性グループからのボリュームの追加の詳細については、を参照してください整合グループの変更。

デスティネーションクラスタからボリュームを追加する

1. デスティネーションクラスタで、**Protection> Relationships**を選択します。
2. ボリュームを追加するSnapMirror構成を探します。[* **Expand**]を選択します ⋮ 。
3. ボリュームを整合グループに追加するボリューム関係を選択する
4. [*展開]を選択します。

関連情報

- "SnapMirrorの削除"
- "スナップミラーの初期化"
- "スナップミラーリリース"
- "snapmirror resync"

ONTAP SnapMirror Active Sync によるアップグレードと復元

SnapMirrorアクティブ同期はONTAP 9.9.1以降でサポートされます。ONTAPクラスタまたはコントローラのアップグレードとリバートは、アップグレードまたはリバートするONTAPのバージョンによっては、SnapMirrorのアクティブな同期関係に影響します。

クラスタをリフレッシュします。

ONTAP 9.16.1以降では、SnapMirror Active Syncで対称アクティブ/アクティブ構成の4ノードクラスタがサポートされます。4ノードクラスタを使用して、コントローラとストレージをアップグレードできます。

開始する前に

- を確認します "4ノオトクラスタノヨウケン"。
- 非対称構成は機器更改プロセスで作成できますが、更新が完了したら対称構成に戻ってください。
- 以下の手順は、整合グループ数が50以下、ボリュームエンドポイント数が400以下の既存の4ノード構成に該当します。

手順

1. "すべてのSnapMirrorアクティブな同期ボリュームを_single_high-availability（HA）ペアに移動する"です。
2. "未使用のノードをクラスタから削除"です。
3. "新しいノードをクラスタに追加"です。
4. "すべてのボリュームを移動"新しいノードに追加します。
5. "未使用のノードをクラスタから削除"それからそれらを交換して"シンシイノオト"ください。

SnapMirrorアクティブ同期を使用した**ONTAP**のアップグレード

SnapMirrorアクティブ同期を使用するには、ソース クラスタとデスティネーション クラスタのすべてのノードでONTAP 9.9.1以降が実行されている必要があります。

SnapMirrorのアクティブな同期関係を含むONTAPをアップグレードする場合は、を使用する必要があります自動無停止アップグレード（ANDU）。ANDUを使用すると、アップグレードプロセス中もSnapMirrorのアクティブな同期関係が正常に同期されます。

SnapMirror Active Sync環境でONTAPのアップグレードを準備するための設定手順はありません。ただし、アップグレードの前後に次の点を確認することを推奨します。

- SnapMirrorアクティブ同期関係が同期されている
- SnapMirrorに関連するエラーがイベント ログに記録されていない
- 両方のクラスタからMediatorがオンラインで、正常な状態である
- LUNを保護するために、すべてのホストがすべてのパスを正しく認識できる

クラスタをONTAP 9 .9.1または9.9.1からONTAP 9 .10.1以降にアップグレードすると、System Managerを使用して設定できるSnapMirrorのアクティブな同期関係用に、ONTAPによってソースとデスティネーションの両方のクラスタに新しいが作成され整合グループます。

コマンドと `snampirror resume`コマンドは、 `snapmirror quiesce`SnapMirrorアクティブ同期ではサポートされていません。

ONTAP 9 .10.1からONTAP 9 .9.1にリバート

関係を9.10.1から9.9.1にリバートするには、SnapMirrorのアクティブな同期関係を削除してから9.10.1整合グループインスタンスを削除する必要があります。アクティブなSnapMirrorアクティブな同期関係を持つ整合性グループは削除できません。9.9.1以前で別のスマートコンテナまたはエンタープライズアプリケーションに関連付けられていた9.10.1にアップグレードしたFlexVolボリュームは、リバート時に関連付けられなくなります。整合性グループを削除しても、コンスティチュエントボリュームやボリューム単位のSnapshotは削除されません。このタスクの詳細については、ONTAP 9 .10.1以降のを参照してください"整合グループを削除する"。

ONTAP 9.9.1からのリバート

SnapMirrorアクティブ同期は、ONTAP 9.9.1より前のリリースが混在するONTAPクラスタではサポートされません。

ONTAP 9.9.1から以前のリリースのONTAPにリバートする場合は、次の点に注意してください。

- クラスタがSnapMirrorアクティブ同期デスティネーションをホストしている場合、関係を解除して削除するまでONTAP 9.8以前にリバートすることはできません。
- クラスタがSnapMirrorアクティブ同期ソースをホストしている場合、関係を解放するまでONTAP 9.8以前にリバートすることはできません。
- ユーザが作成したカスタムのSnapMirrorアクティブ同期ポリシーは、ONTAP 9.8以前にリバートする前にすべて削除する必要があります。

これらの要件を満たすには、を参照してください"SnapMirrorのアクティブな同期設定を削除する"。

手順

1. SnapMirrorのアクティブな同期関係にあるいずれかのクラスタで次のコマンドを入力して、リバートの準備状況を確認します。

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   次の出力例は、クラスタをリバートする準備が完了していない場合のクリーンアップ手順を示しています。

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
   ```

```
    Command to disable snapshot policies: "snapshot policy modify
-vserver
   * -enabled false"

   Break off the initialized online data-protection (DP) volumes and
delete
   Uninitialized online data-protection (DP) volumes present on the
local
   node.
    Command to list all online data-protection volumes on the local
node:
   volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
   quiesce and abort transfers on associated SnapMirror relationships
and
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
```

```
The command to delete a policy is :
 snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. リバートチェックの要件を満たしたら、を参照してください"ONTAPのリバート"。

関連情報

- "ネットワークインターフェイス"
- "スナップミラーの破損"
- "snapmirror policy delete"
- "snapmirror policy show"
- "スナップミラーの静止"
- "snapmirror show"

ONTAP SnapMirror Active Sync 構成を削除する

RTOゼロのSnapMirror同期保護が不要になった場合は、SnapMirrorのアクティブな同期関係を削除できます。

非対称構成を削除します。

- SnapMirrorのアクティブな同期関係を削除する前に、デスティネーションクラスタのすべてのLUNのマッピングを解除する必要があります。
- LUNのマッピングが解除されてホストが再スキャンされると、SCSIターゲットがLUNインベントリが変更されたことをホストに通知します。RTOゼロの関係を削除すると、RTOゼロのセカンダリボリューム上の既存のLUNに新しいIDが反映されます。ホストは、セカンダリボリュームのLUNを、ソースボリュームのLUNとは関係のない新しいLUNとして検出します。
- 関係を削除しても、セカンダリボリュームはDPボリュームのままです。コマンドを実行して、読み取り/書き込みに変換できます `snapmirror break`。
- 関係が反転されていない場合、フェイルオーバー状態の関係を削除することはできません。

手順

1. セカンダリクラスタから、ソースエンドポイントとデスティネーションエンドポイントの間のSnapMirrorのアクティブな同期整合性グループ関係を削除します。

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. プライマリクラスタで、整合性グループ関係とその関係用に作成されたSnapshotを解放します。

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. ホストの再スキャンを実行してLUNインベントリを更新します。
4. ONTAP 9 .10.1以降では、SnapMirror関係を削除しても整合性グループは削除されません。整合グループを削除する場合は、System ManagerまたはONTAP REST APIを使用する必要があります。詳細については、を参照してください 整合グループを削除する 。

iSCSIまたはFC対称アクティブ/アクティブ構成を削除します

対称構成は、System ManagerまたはONTAP CLIを使用して削除できます。どちらのインターフェイスでも、には異なる手順があります均一なコンフィギュレーションと非均一なコンフィギュレーション。

System Manager

統一された構成の手順

1. プライマリサイトで、リモートホストをigroupから削除し、レプリケーションを終了します。
   a. [**Hosts]>[*SAN Initiator Groups]に移動します。
   b. 変更するigroupを選択し、**Edit**します。
   c. リモートイニシエータを削除し、igroupレプリケーションを終了します。保存を選択します。
2. セカンダリサイトで、LUNのマッピングを解除してレプリケートされた関係を削除します。
   a. **Hosts> SAN Initiator Groups**に移動します。
   b. SnapMirror関係があるigroupを選択し、**Delete** を選択します。
   c. ダイアログボックスで、[**Unmap the associated LUNs*]**ボックスを選択し、**[**Delete*]を選択します。
   d. 保護>関係に移動します。
   e. アクティブなSnapMirror同期関係を選択し、**Release**を選択して関係を削除します。

不均一な構成の手順

1. プライマリサイトで、リモートホストをigroupから削除し、レプリケーションを終了します。
   a. [**Hosts]>[*SAN Initiator Groups]に移動します。
   b. 変更するigroupを選択し、**Edit**します。
   c. リモートイニシエータを削除し、igroupレプリケーションを終了します。保存を選択します。
2. セカンダリサイトで、SnapMirrorのアクティブな同期関係を削除します。
   a. 保護>関係に移動します。
   b. アクティブなSnapMirror同期関係を選択し、**Release**を選択して関係を削除します。

CLI

統一された構成の手順

1. すべてのVMワークロードを、SnapMirrorアクティブ同期のソースクラスタのローカルホストに移動します。
2. ソースクラスタで、igroupからイニシエータを削除し、igroupのレプリケーションを終了するようにigroup設定を変更します。

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. セカンダリサイトで、LUNマッピングを削除し、igroup設定を削除します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. セカンダリサイトで、SnapMirrorのアクティブな同期関係を削除します。

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. プライマリサイトで、プライマリサイトからSnapMirrorのアクティブな同期関係を解放します。

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. パスを再検出して、ホストへのローカルパスのみが使用可能であることを確認します。

不均一な構成の手順

1. すべてのVMワークロードを、SnapMirrorアクティブ同期のソースクラスタのローカルホストに移動します。
2. ソースクラスタで、igroupからイニシエータを削除します。

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. セカンダリサイトで、LUNマッピングを削除し、igroup設定を削除します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. セカンダリサイトで、SnapMirrorのアクティブな同期関係を削除します。

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. プライマリサイトで、プライマリサイトからSnapMirrorのアクティブな同期関係を解放します。

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. パスを再検出して、ホストへのローカルパスのみが使用可能であることを確認します。

NVMe対称アクティブ/アクティブ構成を削除する

System Manager

手順

1. ソース クラスターで、保護 > レプリケーション に移動します。
2. 削除したい関係を見つけて選択 *削除*を選択します。

CLI

1. 宛先クラスタから、 SnapMirrorアクティブ同期関係を削除します。

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   例：

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   サブシステムとその名前空間はセカンダリ クラスターから削除されます。

2. ソース クラスターから、プライマリ サイトからSnapMirrorアクティブ同期関係を解除します。

   ```
   snapmirror release -destination-path <destination_path>
   ```

   例：

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. パスを再検出して、ホストへのローカルパスのみが使用可能であることを確認します。

関連情報

- "スナップミラーの破損"
- "SnapMirrorの削除"
- "スナップミラーリリース"

ONTAP MediatorまたはONTAP Cloud Mediatorを削除します

ONTAPクラスタから既存のONTAP MediatorまたはONTAP Cloud Mediatorの設定を削除する場合は、 `snapmirror mediator remove`コマンド。たとえば、一度に使用できるMediator の種類は 1 つだけなので、1 つのインスタンスを削除してから、別のインスタンスをインストールする必要があります。

手順

次のいずれかの手順を実行すると、 ONTAP Mediator またはONTAP Cloud Mediator を削除できます。

ONTAP Mediator

1. ONTAPメディエーターを削除します。

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   例：

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAPクラウドメディエーター

1. ONTAP Cloud Mediatorを削除します。

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   例：

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

関連情報

- "スナップミラーメディエーターの削除"

トラブルシューティング

ONTAP SnapMirrorの削除操作が引き継ぎ状態で失敗する

以下の情報を使用してください。 `snapmirror delete` SnapMirrorアクティブ同期整合性グループ関係がテイクオーバー状態にある場合、コマンドは失敗します。

問題：

ONTAP 9.9.1がクラスタにインストールされている場合、 `snapmirror delete` SnapMirror アクティブ同期整合性グループ関係がテイクオーバー状態にある場合、コマンドは失敗します。

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

解決策

SnapMirror アクティブ同期関係のノードがテイクオーバー状態にある場合は、「-force」オプションを true に設定して SnapMirror の削除および解放操作を実行します。

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

関連情報

- "SnapMirrorの削除"

ONTAP SnapMirror関係の作成と整合性グループの初期化に失敗しました

SnapMirror関係の作成と整合性グループの初期化に失敗した場合は、次の情報を使用します。

問題：

SnapMirror関係の作成、および整合性グループの初期化が失敗します。

解決策：

クラスタあたりの整合グループの制限を超えていないことを確認してください。SnapMirrorアクティブ同期の整合グループの制限はプラットフォームに依存せず、ONTAPのバージョンによって異なります。ご使用のONTAPバージョンに固有のガイダンスについては、を参照してください"オブジェクトの制限"。

エラー：

整合性グループの初期化が停止した場合は、ONTAP REST API、System Manager、またはコマンドを使用して、整合性グループの初期化のステータスを確認します `sn show -expand`。

ONTAP 9.14.1 から 9.8 では、 SnapMirror Active Sync はSnapMirror Business Continuity (SM-BC) と呼ばれます。

解決策：

整合性グループの初期化に失敗した場合は、SnapMirrorのアクティブな同期関係を削除し、整合性グループを削除してから関係を再作成して初期化します。このワークフローは、使用しているONTAPのバージョンによって異なります。

ONTAP 9.9.1を使用している場合	ONTAP 9.10.1以降を使用している場合

1. "SnapMirrorのアクティブな同期設定を削除する" 2. "整合性グループ関係を作成し、整合性グループ関係を初期化"	1. [保護]>[関係]で、整合性グループ上の**SnapMirror**のアクティブな同期関係を探します。を選択し、[削除]*を選択し てSnapMirrorのアクティブな同期関係を削除します。 2. "整合グループの削除" 3. "整合グループの設定"

計画された**ONTAP**クラスタ フェイルオーバーが失敗しました

計画されたフェイルオーバー操作が失敗した場合は、次の情報を使用します。

問題：

コマンドの実行後、 `snapmirror failover start`コマンドの出力に `snapmirror failover show`無停止操作が進行中であることを示すメッセージが表示されます。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                                  08:35:04
08:35:04
```

原因：

ボリューム移動、アグリゲートの再配置、ストレージフェイルオーバーなどの無停止操作の実行中は、計画的フェイルオーバーを開始できません。

解決策：

無停止操作が完了してから、フェイルオーバー処理を再試行してください。

関連情報

- "スナップミラーフェイルオーバー表示"
- "スナップミラーフェイルオーバーの開始"

ONTAP Mediator または**ONTAP Cloud Mediator** にアクセスできないか、**Mediator** のクォーラム ステータスが **false** です

ONTAP Mediator またはONTAP Cloud Mediator にアクセスできない場合、または Mediator クォーラム ステータスが false の場合は、次の情報を使用します。

問題：

実行後 `snapmirror failover start`コマンドの出力は `snapmirror failover show`コマンドを実行すると、 ONTAP

Mediator またはONTAP Cloud Mediator のいずれかが設定されていないことを示すメッセージが表示されます。

見る"SnapMirror Active Sync用のONTAPメディエーターとクラスタの設定"または"SnapMirror Active Sync 用のONTAP Cloud Mediator を構成する" 。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

原因：

Mediatorが設定されていないか、ネットワーク接続に問題があります。

解決策：

ONTAPメディエーターが設定されていない場合は、SnapMirrorのアクティブな同期関係を確立する前にONTAPメディエーターを設定する必要があります。ネットワーク接続の問題を修正します。SnapMirror mediator showコマンドを使用して、ソースとデスティネーションの両方のサイトでMediatorが接続され、クォーラムステータスがtrueになっていることを確認します。詳細については、を参照してください "ONTAPメディエーターの設定"。

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

関連情報

- "スナップミラーフェイルオーバー表示"
- "スナップミラーフェイルオーバーの開始"
- "スナップミラーメディエーターショー"

ONTAP Cloud Mediator はアクセス可能ですが、応答が遅いです

ONTAP Cloud Meditor が、ping レイテンシが推奨レイテンシよりも高いというエラーで失敗する場合は、次の情報を使用します。

問題：

システム マネージャー: Cloud Mediator サービスはアクセス可能ですが、応答が遅いです。

CLI: `mediator add`コマンドは次のエラーで失敗します：
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms

```
which is higher than twice the recommended latency of 200 ms.
```

原因：

クラスターがNetAppコンソール クラウドの近くに配置されていないか、ネットワーク パスのボトルネックがある可能性があります。

解決策：

- NetAppコンソール クラウド (米国東部) の地理的な場所と近さを確認します。
- ネットワーク パスを最適化したり、ボトルネックを解決したりします。
- ネットワーク ツールを使用してラウンド トリップ時間 (RTT) を測定し、レイテンシを推奨制限内に短縮します。
- パフォーマンスを向上させるには、HTTP プロキシを使用します。

見る"ONTAP Cloud MediatorとクラスタをSnapMirror Active Sync用に設定する" 。

サイト**B**で自動計画外フェイルオーバーがトリガーされない

サイト A の障害によってサイト B の計画外のフェイルオーバーがトリガーされない場合は、次の情報を使用します。

問題：

サイトAで障害が発生しても、サイトBで計画外フェイルオーバーはトリガーされません。

考えられる原因**1**：

ONTAPメディエーターまたはONTAPクラウドメディエーターが設定されていません。これが原因かどうかを確認するには、 `snapmirror mediator show`サイト B クラスターのコマンド。

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

この例では、Mediator がサイト B で構成されていないことを示しています。

解決策：

両方のクラスタにMediatorを設定し、ステータスが「connected」で、クォーラムがTrueに設定されていることを確認します。

考えられる原因**2**：

SnapMirror整合性グループが同期されていません。これが原因かどうかを確認するには、イベントログを表示して、サイトAで障害が発生したときに整合性グループが同期されていたかどうかを確認します。

```
cluster::> event log show -event *out.of.sync*

Time                 Node              Severity      Event
-------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

解決策：

サイトBで強制的なフェイルオーバーを実行するには、次の手順を実行します。

1. この整合グループに属するすべてのLUNのサイトBへのマッピングを解除します。
2. オプションを使用して、SnapMirror整合性グループ関係を削除します `force`。
3. 整合性グループのコンスティチュエントボリュームに対してコマンドを入力し `snapmirror break`て、ボリュームをDPからR/Wに変換し、サイトBからのI/Oを可能にします。
4. サイトAのノードをブートして、サイトBからサイトAへのRTOゼロの関係を作成します。
5. サイトAでを使用して整合性グループを解放し `relationship-info-only`、共通のSnapshotを保持して、整合性グループに属するLUNのマッピングを解除します。
6. SyncポリシーまたはAsyncポリシーを使用してボリュームレベルの関係を設定し、サイトAのボリュームをR/WからDPに変換します。
7. を実行し `snapmirror resync`て関係を同期します。
8. サイトAでSyncポリシーが設定されたSnapMirror関係を削除します。
9. サイトBでSyncポリシーが設定されたSnapMirror関係ををを使用して解放します。 `relationship-info-only true`
10. サイトBからサイトAへの整合性グループ関係を作成します。
11. サイトAから整合性グループの再同期を実行し、整合性グループが同期されていることを確認します。
12. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

関連情報

- "スナップミラーの破損"
- "スナップミラーメディエーターショー"
- "snapmirror resync"

サイト **B** と**ONTAP Mediator** 間のリンクがダウンし、サイト **A** がダウン

ONTAPメディエーターまたはONTAPクラウドメディエーターの接続を確認するには、`snapmirror mediator show`指示。接続ステータスが到達不能で、サイトBがサイトAに到達できない場合は、次のような出力が表示されます。「解決策」の手順に従って、接続

をリストアしてください。

例：

ONTAP Cloud Mediator 出力「snapmirror mediator show」コマンドを使用します。

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

ONTAP Mediator 出力の `snapmirror mediator show` コマンドを使用します。

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

解決策

フェイルオーバーを強制的に実行してサイトBからのI/Oを可能にし、サイトBからサイトAへのRTOゼロの関係を確立します。サイトBで強制的にフェイルオーバーを実行するには、以下の手順に従います。

1. この整合グループに属するすべてのLUNのサイトBへのマッピングを解除します。
2. forceオプションを使用して、SnapMirror整合性グループ関係を削除します。
3. (`snapmirror break -destination_path *svm*:_volume_`整合性グループのコンスティチュエントボリュームに対してSnapMirror breakコマンドを入力してボリュームをDPからRWに変換し、サイトBからのI/Oを可能にします。

   整合性グループ内の関係ごとにSnapMirror breakコマンドを実行する必要があります。たとえば、整合グループにボリュームが3つある場合は、ボリュームごとにコマンドを実行します。
4. サイトAのノードをブートして、サイトBからサイトAへのRTOゼロの関係を作成します。
5. サイトAでrelationship-info-onlyを使用して整合性グループを解放し、共通のSnapshotを保持して、整合性グループに属するLUNのマッピングを解除します。
6. SyncポリシーまたはAsyncポリシーを使用してボリュームレベルの関係を設定し、サイトAのボリュームをRWからDPに変換します。
7. コマンドを実行し `snapmirror resync`て関係を同期します。
8. サイトAでSyncポリシーが設定されたSnapMirror関係を削除します。
9. サイトBでSyncポリシーが設定されたSnapMirror関係をrelationship-info-only trueを使用して解放します。
10. サイトBとサイトAの間に整合性グループ関係を作成します。
11. ソースクラスタから、整合グループを再同期します。整合性グループの状態がin syncになっていることを確認します。
12. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

関連情報

- "スナップミラーの破損"
- "スナップミラーメディエーターショー"
- "snapmirror resync"
- "snapmirror show"

サイト **A** と**ONTAP Mediator** 間のリンクがダウンし、サイト **B** がダウンしています

SnapMirrorのアクティブな同期を使用している場合、ONTAPメディエーターまたはピアクラスタ間の接続が失われる可能性があります。問題を診断するには、SnapMirrorアクティブな同期関係の各部分の接続、可用性、合意ステータスを確認し、接続を強制的に再開します。

確認事項	**CLI**コマンド	インジケータ
Mediator（サイトAから）	`snapmirror mediator show`	接続ステータスは次のように表示されます `unreachable`

確認事項	CLIコマンド	インジケータ
サイトBの接続	`cluster peer show`	可用性はとして表示されます `unavailable`
SnapMirrorアクティブ同期ボリュームの合意ステータス	`volume show volume_name -fields smbc-consensus`	この `sm-bc consensus`フィールドには、 `Awaiting-consensus`

この問題の診断と解決に関する追加情報については、"NetAppナレッジベース: SnapMirrorアクティブ同期の使用時にサイト A とメディエーター間のリンクがダウンし、サイト B がダウンする" 。

関連情報

- "cluster peer show"
- "スナップミラーメディエーターショー"

宛先ボリュームにフェンスが設定されている場合、 **ONTAP SnapMirror** の削除操作が失敗する

宛先ボリュームのいずれかにリダイレクト フェンスが設定されている場合にSnapMirrorの削除操作が失敗する場合は、次の情報を使用します。

問題：

デスティネーションボリュームでリダイレクトフェンスが設定されていると、SnapMirrorの削除処理が失敗します。

解決策

次の処理を実行してリダイレクトを再試行し、デスティネーションボリュームからフェンシングを削除します。

- SnapMirrorの再同期
- SnapMirrorの更新

ONTAPプライマリがダウンするとボリューム移動操作が停止する

SnapMirrorアクティブ同期関係でプライマリ サイトがダウンしているときに、ボリューム移動操作がカットオーバー延期状態で無期限に停止する場合は、次の情報を使用します。

問題：

SnapMirrorのアクティブな同期関係でプライマリサイトが停止すると、ボリューム移動処理がカットオーバー保留状態で無期限に停止します。プライマリサイトが停止すると、セカンダリサイトで自動計画外フェイルオーバー（AUFO）が実行されます。ボリューム移動処理の実行中にAUFOがトリガーされると、ボリューム移動は停止します。

解決策：

停止しているボリューム移動インスタンスを中止し、ボリューム移動処理を再開してください。

スナップショットを削除できない場合、 **ONTAP SnapMirror** のリリースが失敗する

スナップショットを削除できず、 SnapMirror の解放操作が失敗する場合は、次の情報を使用します。

問題：

Snapshotを削除できないと、SnapMirrorの解放処理が失敗します。

解決策：

Snapshotに一時タグが含まれています。一時的なSnapshotを削除するには、オプションを指定してコマンドを `-ignore-owners`使用し `snapshot delete`ます。
`snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true`

コマンドを再試行します `snapmirror release`。

関連情報

- "スナップミラーリリース"

ボリューム移動参照スナップショットは、 **ONTAP SnapMirror**関係の最新のものとして表示されます。

ボリューム移動操作後にボリューム移動参照スナップショットがSnapMirror関係の最新のものとして表示される場合は、次の情報を使用します。

問題：

整合性グループのボリュームに対してボリューム移動処理を実行したあとに、ボリューム移動の参照SnapshotがSnapMirror関係の最新のSnapshotとして誤って表示されることがあります。

最新のSnapshotを表示するには、次のコマンドを使用します。

```
snapmirror show -fields newest-snapshot status -expand
```

解決策：

を手動で実行する `snapmirror resync`か、ボリューム移動処理の完了後に次の自動再同期処理が実行されるまで待ちます。

関連情報

- "snapmirror resync"
- "snapmirror show"

MetroCluster および SnapMirror アクティブ同期用の ONTAP Mediator

ONTAP Mediatorの詳細

このドキュメントは、オンプレミス版のONTAP Mediatorについて説明しています。ONTAPONTAP以降で利用可能なONTAP Cloud Mediatorの詳細については、

"SnapMirrorアクティブ同期ドキュメント" 。

ONTAP Mediator は、ONTAP 機能に対していくつかの機能を提供します。

- HAメタデータ用のフェンシングされた永続的なストアを提供します。
- コントローラの稼働を維持するためのpingプロキシとして機能します。
- クォーラムの決定に役立つ同期ノード健全性クエリ機能を提供します。

ONTAP Mediator は、次の 2 つの追加の systemctl サービスを提供します。

- **`ontap_mediator.service`**

  ONTAP 関係を管理するための REST API サーバーを管理します。

- **`mediator-scst.service`**

  iSCSIモジュール（SCST）の起動とシャットダウンを制御します。

システム管理者に提供されるツール

システム管理者に提供されるツール：

- **`/usr/local/bin/mediator_change_password`**

  現在のAPIユーザ名とパスワードを指定したときに、新しいAPIパスワードを設定します。

- **`/usr/local/bin/mediator_change_user`**

  現在のAPIユーザ名とパスワードを指定した場合に、新しいAPIユーザ名を設定します。

- **`/usr/local/bin/mediator_generate_support_bundle`**

  NetAppカスタマーサポートとの通信に必要なすべてのサポート情報を含むローカルのtgzファイルを生成します。これには、アプリケーション構成、ログ、および一部のシステム情報が含まれます。バンドルはローカルディスク上で生成され、必要に応じて手動で転送できます。保存場所：/opt/netapp/data/support bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  ONTAPメディエーターパッケージとSCSTカーネルモジュールを削除します。これには、すべての設定、ログ、およびメールボックスデータが含まれます。

- **`/usr/local/bin/mediator_unlock_user`**

  認証の再試行回数が制限に達した場合、APIユーザーアカウントのロックアウトを解除します。この機能は、ブルートフォース攻撃によるパスワード導出を防ぐために使用されます。ユーザーに正しいユーザー名とパスワードの入力を求めます。

- **`/usr/local/bin/mediator_add_user`**

  （サポートのみ）インストール時にAPIユーザを追加する場合に使用します。

特記事項

ONTAPメディエーターは、SCSTを使用してiSCSIを提供します（を参照 http://scst.sourceforge.net/index.html）。このパッケージは、インストール時にカーネル専用にコンパイルされるカーネルモジュールです。カーネルを更新する場合は、SCSTの再インストールが必要になることがあります。または、ONTAP Mediator をアンインストールしてから再インストールし、ONTAP 関係を再構成します。

サーバOSカーネルの更新は、ONTAPのメンテナンス時間に合わせて行う必要があります。

ONTAP Mediatorの新機能

ONTAP Mediatorはリリースごとに新しい機能強化が提供されます。新機能は以下のとおりです。

キノウカクチョウ

SCSTのバージョン情報については、を参照してSCSTのサポートマトリックスください。

ONTAP メディエーターのバージョン	キノウカクチョウ
1.10	• RHELのサポート： ◦ 互換性: 9.5。 ◦ 推奨: 10.0、9.6、9.4、8.10。 • Rocky Linux 10.0、9.6、8.10 のサポート。 • ベース Python バージョンを Python 3.9 から Python 3.12 にアップグレードしました。
1.9.1	• RHELのサポート： ◦ 互換性: 9.3、9.1、8.9、8.7、8.6、8.5、8.4。 ◦ 推奨: 9.5、9.4、9.2、9.0、8.10、8.8。 • Rocky Linux 9.5および8.10のサポート。 • コード署名検証用の新しい証明書を追加しました。 • コード署名チェックをスキップするためのサポートを追加しました。 `-skip-code-signature-check`フラグ。 • 期限切れのコード署名証明書が検出された場合のインストーラー警告が含まれます。

1.9	• RHELのサポート： ◦ 互換性: 9.3、9.1、8.9、8.7、8.6、8.5、8.4。 ◦ 推奨: 9.5、9.4、9.2、9.0、8.10、8.8。 • Rocky Linux 9.5および8.10のサポート。 • RHELおよびRocky LinuxのFIPSサポート。 • パフォーマンスが強化され、スケーラビリティが向上しました。 • PKI署名付き証明書のセットアップを簡素化するためのファイル名の改善。
1.8	• RHELのサポート： ◦ 互換性: 8.7、8.6、8.5、8.4。 ◦ 推奨: 9.4、9.3、9.2、9.1、9.0、8.10、8.9、8.8。 • Rocky Linux 9.4および8.10のサポート。
1.7	• RHELのサポート： ◦ 互換性: 8.7、8.6、8.5、8.4。 ◦ 推奨: 9.3、9.2、9.1、9.0、8.9、8.8。 • Rocky Linux 9.3および8.9のサポート。 • 自己署名証明書およびサードパーティ署名証明書でのSAN（Subject Alternative Name）データのサポート。
1.6	• Python 3.9のアップデート。 • RHELのサポート： ◦ 互換性: 8.7、8.6、8.5、8.4。 ◦ 推奨: 9.2、9.1、9.0、8.8。 • Rocky Linux 9.2および8.8のサポート。 • RHEL 7.x / CentOSのすべてのリリースのサポートを廃止しました。
1.5	• RHEL 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6 のサポート。 • RHEL 7.x / CentOS 7.xの廃止に関する警告が追加されました。 • 大規模なSnapMirrorアクティブ同期システムの速度を最適化します。 • インストーラに暗号化コード署名が追加されました。
1.4	• RHEL 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6 のサポート。 • UFEIベースのファームウェアのセキュア ブート（SB）をサポート。

1.3	• RHEL 8.3、8.2、8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6 のサポート。
1.2	• RHEL 8.1、8.0、7.9、7.8、7.7、7.6 のサポート。 • CentOS 7.9、7.8、7.7、7.6 のサポート。 • HTTPSメールボックスのサポート。 • ONTAP 9.8以降のMCC-IP AUSOおよびSnapMirrorアクティブ同期ZRTOで使用します。
1.1	• RHEL 8.0および7.6のサポート。 • CentOS 7.6のサポート • Perlの依存関係を削除。
1.0	• iSCSIメールボックスのサポート。 • ONTAP 9.7以降MCC-IP AUSOで使用します。 • RHEL / CentOS 7.6のサポート。

OSのサポート対応表

ONTAP メディエーター用のOS	1.10	1.9.1	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
RHEL 10.0	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.6	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.5	互換性	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.4	○	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.3	いいえ	互換性	互換性	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.2	いいえ	○	○	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

RHEL 9.1	いいえ	互換性	互換性	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.0	いいえ	○	○	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.10	○	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.9	いいえ	互換性	互換性	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.8	いいえ	○	○	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.7	いいえ	互換性	互換性	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.6	いいえ	互換性	互換性	○	○	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.5	いいえ	互換性	互換性	○	○	○	○	○	いいえ	いいえ	いいえ	いいえ
RHEL 8.4	いいえ	互換性	互換性	○	○	○	○	○	いいえ	いいえ	いいえ	いいえ
RHEL 8.3	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	いいえ	いいえ	いいえ
RHEL 8.2	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	いいえ	いいえ	いいえ
RHEL 8.1	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	○	いいえ	いいえ
RHEL 8.0	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	○	○	いいえ
RHEL および CentOS 7.9	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	互換性	いいえ	いいえ

RHELおよびCentOS 7.8	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	○	いいえ	いいえ
RHELおよびCentOS 7.7	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	○	いいえ	いいえ
RHELおよびCentOS 7.6	廃止	廃止	廃止	廃止	廃止	廃止	○	○	○	○	○	○（RHELのみ）
CentOS 8およびSTREAM	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	N/A	N/A	N/A
ロッキーLinux 10.0	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Rocky Linux 9	○	○	○	○	○	○	N/A	N/A	N/A	N/A	N/A	N/A
Rocky Linux 8	○	○	○	○	○	○	N/A	N/A	N/A	N/A	N/A	N/A
Oracle Linux 10	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Oracle Linux 9	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

- 「はい」は、ONTAPメディエーターのインストールに推奨されるOSであり、完全な互換性がありサポートされていることを示します。
- 「いいえ」は、OSとONTAPメディエーターに互換性がないことを示します。
- 「互換性あり」とは、Red Hat がこれらの RHEL バージョンをサポートしなくなったものの、 ONTAP Mediator をこれらのバージョンにインストールできることを意味します。
- ONTAP Mediator 1.6では、Rocky Linux 9および8のサポートが追加されています。

- ONTAP Mediator 1.5は、RHEL 7.xブランチ オペレーティング システムでサポートされる最後のリリースです。
- CentOS 8は再分岐のため全てのリリースで削除された。CentOS Streamは本番用のターゲットOSとしては適切ではないと考えられていた。サポートは予定されていません。

SCSTのサポートマトリックス

次の表に、ONTAPメディエーターのバージョンごとにサポートされるSCSTのバージョンを示します。

ONTAP メディエーターのバージョン	サポートされる **SCST** のバージョン
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAPメディエーター1.9.1	scst-3.8.0.tar.bz2
ONTAPメディエーター1.9	scst-3.8.0.tar.bz2
ONTAPメディエーター1.8	scst-3.8.0.tar.bz2
ONTAPメディエーター1.7	scst-3.7.0.tar.bz2
ONTAPメディエーター1.6	scst-3.7.0.tar.bz2
ONTAPメディエーター1.5	scst-3.6.0.tar.bz2
ONTAPメディエーター1.4	scst-3.6.0.tar.bz2
ONTAPメディエーター1.3	scst-3.5.0.tar.bz2
ONTAPメディエーター1.2	scst-3.4.0.tar.bz2
ONTAPメディエーター1.1	scst-3.4.0.tar.bz2
ONTAPメディエーター1.0	scst-3.3.0.tar.bz2

インストールまたはアップグレード

ONTAPメディエーターのインストールワークフローの概要

ONTAP Mediator のインストールには、インストールの準備、リポジトリへのアクセスの提供、インストール パッケージのダウンロード、コード署名の検証、ONTAP Mediator パッケージのインストール、およびインストール後の設定タスクの実行が含まれます。

1. **"ONTAP Mediatorのインストールまたはアップグレードの準備"**

ONTAP Mediator をインストールまたはアップグレードするには、すべての前提条件が満たされていることを確認する必要があります。

2. **"ホストOSとMediatorのアップグレード"**

既存のONTAP Mediatorをアップグレードする場合は、まず以前のバージョンをアンインストールしてから、新しいバージョンをインストールする必要があります。ONTAPMediatorを初めてインストールする場合は、この手順をスキップできます。

3 "リポジトリへのアクセスを提供する"

インストール プロセス中に ONTAP Mediator が必要なパッケージにアクセスできるように、リポジトリへのアクセスを有効にする必要があります。

4 "ONTAPメディエーターのインストールパッケージをダウンロードする"

ONTAP Mediator ダウンロード ページから ONTAP Mediator インストール パッケージをダウンロードします。

5 "ONTAPメディエーターインストールパッケージのコード署名を確認します"

NetApp では、ONTAP Mediator インストール パッケージをインストールする前に、ONTAP Mediator コード署名を確認することを推奨しています。

6 "ONTAPメディエーターをインストールする"

ONTAP Mediator をインストールするには、インストール パッケージを取得し、ホスト上でインストーラを実行する必要があります。

7 "ONTAPメディエーターのインストールを確認する"

ONTAP Mediator をインストールした後、正常に実行されていることを確認します。

8 "インストール後の構成タスクを実行する"

ONTAP Mediator をインストールして実行した後、ONTAP Mediator 機能を使用するには追加の設定タスクを実行する必要があります。

ONTAP Mediatorのインストールまたはアップグレードの準備

ONTAPメディエーターをインストールするには、すべての前提条件が満たされていることを確認し、インストールパッケージを取得し、ホスト上でインストーラを実行する必要があります。この手順は、インストールまたは既存のインストールのアップグレードに使用されます。

- ONTAP 9 .8以降では、任意のバージョンのONTAPメディエーターを使用してSnapMirrorのアクティブな同期関係を監視できます。
- ONTAP 9 .7以降では、任意のバージョンのONTAPメディエーターを使用してMetroCluster IP設定を監視できます。

インストールとアップグレードに関する考慮事項

ONTAP Mediator をアップグレードまたはインストールする前に、次の考慮事項を確認してください。

ONTAP Mediator 1.8 以前では、Red Hat Enterprise Linux (RHEL) FIPS モードと互換性がないため、正常にインストールできません。 FIPSモードが有効になっているかどうかを確認するには、 `fips-mode-setup --check`指示。 FIPSモードを無効にするには、 `fips-modesetup --disable`指示。FIPSモードを無効にしてからリブートすれば、ONTAP Mediator 1.8以前を正常にインストールできます。

- ONTAP Mediator を最新バージョンにアップグレードしてください。以前のバージョンの ONTAP Mediator はすべての ONTAP バージョンとの下位互換性を維持していますが、最新バージョンにはすべてのサードパーティ要素に対するセキュリティパッチが含まれています。
- 新しい ONTAP Mediator バージョンにアップグレードすると、より高いバージョンが利用できない限り、インストーラは推奨される SCST バージョンに自動的にアップグレードします。上位バージョンのSCSTを手動でインストールする手順については、を参照してください"ONTAPメディエーターの管理"。サポートされているバージョンについては、を参照してください"SCSTのサポートマトリックス"。

- インストールに失敗した場合は、ONTAPメディエーターの新しいバージョンへのアップグレードが必要になることがあります。
- 2025 年 6 月 15 日以降、コード署名証明書の有効期限が切れているため、 ONTAP Mediator 1.9 および 1.8 をインストールまたはアップグレードすることはできません。インストールまたはアップグレードが失敗した場合は、代わりにONTAP Mediator 1.9.1 パッチバージョンを使用してください。

- パッケージをインストールする場合は `yum-utils`、コマンドを使用できます `needs-restarting`。
- ONTAP Mediator 1.10 以前のバージョンでは IPv6 はサポートされていません。

ホストの要件

RHEL または Rocky Linux をインストールし、関連するリポジトリを構成するときは、次の要件に従ってください。

インストールプロセスや設定プロセスを変更する場合は、追加の手順が必要になることがあります。

Linuxディストリビューションの要件

- Red Hatのベストプラクティスに従ってRHELまたはRocky Linuxをインストールします。CentOS 8.xのサポートが終了したため、互換性のあるバージョンのCentOS 8.xは推奨されません。
- ONTAP Mediator をインストールするときは、インストール プログラムが必要なすべてのソフトウェア依存関係を取得してインストールできるように、システムが必要なリポジトリにアクセスできることを確認してください。
- yumインストーラがRHELリポジトリ内の依存ソフトウェアを検出できるようにするには、インストール時またはインストール後に有効なRed Hatサブスクリプションを使用してシステムを登録します。

詳細については、Red Hat Subscription Managerのドキュメントを参照してください。

ネットワーク要件

次のポートがONTAPメディエーター用に使用可能で使用されていないことを確認します。

ポート / サービス	ソース	方向	デスティネーション	目的
22 / TCP	管理ホスト	インバウンド	ONTAP Mediator	（オプション）SSH / ONTAPメディエーターの管理
31784/TCP	クラスタ管理LIF	インバウンド	ONTAPメディエーターWebサーバ	（必須）REST API（HTTPS）
3260 / TCP[1]	ノードのデータLIFまたはノード管理LIF	双方向	ONTAPメディエーターのiSCSIターゲット	（MCCIPに必要）メールボックスのiSCSIデータ接続

1. SMBCをご利用の場合、ONTAPではポート3260を有効にしたり接続したりする必要はありません。
   - サードパーティ製のファイアウォールを使用している場合は、を参照してください"ONTAPメディエーターのファイアウォール要件"。
   - インターネットにアクセスできないLinuxホストの場合は、必要なパッケージがローカルリポジトリにあることを確認してください。

     Linux環境でLink Aggregation Control Protocol（LACP）を使用している場合は、カーネルを設定し、をに 2`設定します `sysctl net.ipv4.conf.all.arp_ignore`。

OSノヨウケン

OSが次の要件を満たしている必要があります。

- 64ビットの物理インストールまたは仮想マシン
- 8GBのRAM
- 1 GBのディスクスペース（アプリケーションのインストール、サーバログ、およびデータベースに使用）
- ユーザ：ルートアクセス

次の表に、ONTAP Mediatorのバージョンごとにサポートされるを示します。

ONTAP メディエーターのバージョン	サポートされるLinuxバージョン
1.10	• Red Hat Enterprise Linux ◦ 互換性: 9.5 [1] ◦ 推奨: 10、9.6、9.4、8.10 • Rocky Linux 10、9.6、および 8.10

1.9.1	• Red Hat Enterprise Linux ◦ 互換性: 9.3、9.1、8.9、8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.9	• Red Hat Enterprise Linux ◦ 互換性: 9.3、9.1、8.9、8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.8	• Red Hat Enterprise Linux： ◦ 互換性: 8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.4、9.3、9.2、9.1、9.0、8.10、8.9、8.8 • Rocky Linux 9.4、8.10
1.7	• Red Hat Enterprise Linux： ◦ 互換性: 8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.3、9.2、9.1、9.0、8.9、8.8 • Rocky Linux 9.3、8.9
1.6	• Red Hat Enterprise Linux： ◦ 互換性: 8.7、8.6、8.5、8.4 [1] ◦ 推奨: 9.2、9.1、9.0、8.8 • Rocky Linux 9.2、8.8
1.5	• Red Hat Enterprise Linux: 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6
1.4	• Red Hat Enterprise Linux: 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6
1.3	• Red Hat Enterprise Linux: 8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6

1.2	• Red Hat Enterprise Linux: 8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS: 7.9、7.8、7.7、7.6

1. 互換性があるとは、Red Hat がこれらの RHEL バージョンをサポートしなくなったものの、 ONTAP Mediator をこれらのバージョンにインストールできることを意味します。

OSに必要なパッケージ

ONTAP Mediator には次のパッケージが必要です。

パッケージは事前にインストールされるか、ONTAPメディエーターのインストーラによって自動的にインストールされます。

RHEL / CentOSのすべてのバージョン	RHEL 10.x / Rocky Linux 10 用の追加パッケージ	RHEL 9.x/Rocky Linux 9 用の追加パッケージ	RHEL 8.x/Rocky Linux 8 用の追加パッケージ
• openssl • openssl-devel • kernel-devel-$（uname -r） • GCC • 作成 • libselinux-utils • パッチ • bzip2 • Perl -データ-ダンパ • Perl - ExtUtils - MakeMaker • efibootmgr • モクティル	• python3.12 • python3.12-devel	• elfutils-libelf-devel • policycoreutils-python-utils • ピートン3 • Python3 -デベル	• elfutils-libelf-devel • policycoreutils-python-utils • redhat-lsb-core • ピートン39 • Python39 -デベル

Mediatorインストールパッケージは自己解凍型の圧縮tarファイルで、次の内容が含まれます。

- サポートされているリリースのリポジトリから取得できないすべての依存関係を含むRPMファイル。
- インストールスクリプト。

有効なSSL証明書を使用することを推奨します。

OSのアップグレードに関する考慮事項とカーネルの互換性

- カーネルを除くすべてのライブラリパッケージは安全に更新できますが、ONTAPメディエーターアプリケーション内で変更を適用するにはリブートが必要になる場合があります。再起動が必要な場合は、サービスウィンドウを使用することをお勧めします。
- OSカーネルを最新の状態に保つ必要があります。カーネルコアは、でサポートされているバージョンに

アップグレードできます"ONTAPメディエーターのバージョンマトリックス"。リブートは必須であるため、停止に備えてメンテナンス時間を計画する必要があります。

- リブートする前にSCSTカーネルモジュールをアンインストールし、その後再インストールする必要があります。
- カーネルOSのアップグレードを開始する前に、サポートされているバージョンのSCSTを再インストールできる状態にしておく必要があります。

- カーネルのバージョンは、オペレーティングシステムのバージョンと一致している必要があります。
- 特定のONTAPメディエーターリリースでは、サポートされているOSリリース以降のカーネルにアップグレードすることはできません。(これは、テストしたSCSTモジュールがコンパイルされないことを示している可能性があります)。

UEFIセキュアブートが有効になっている場合の**ONTAP**メディエーターのインストール

ONTAPメディエーターは、UEFIセキュアブートが有効になっているかどうかに関係なく、システムにインストールできます。

タスクの内容

UEFIセキュアブートが不要な場合、またはONTAPメディエーターのインストールに関する問題をトラブルシューティングする場合は、ONTAPメディエーターをインストールする前に、UEFIセキュアブートを無効にすることを選択できます。マシン設定からUEFIセキュアブートオプションを無効にします。

UEFIセキュアブートを無効にする手順の詳細については、ホストOSのマニュアルを参照してください。

UEFIセキュアブートを有効にしたONTAPメディエーターをインストールするには、サービスを開始する前にセキュリティキーを登録する必要があります。このキーはSCSTインストールのコンパイルステップ中に生成され、秘密鍵と公開鍵のペアとしてマシンに保存されます。ユーティリティを使用し `mokutil`て公開鍵をマシン所有者キー（Mok）としてUEFIファームウェアに追加し、システムが署名済みモジュールを信頼してロードできるようにします。パスフレーズは、システムを再起動してMokをアクティブにするときに必要になるため、安全な場所に保存して `mokutil`ください。

手順

1. システムでUEFIセキュアブートが有効になっているかどうかを確認します。

```
mokutil --sb-state
```

結果は、このシステムでUEFIセキュアブートが有効になっているかどうかを示します。

状況	手順
UEFIセキュアブートが有効	
UEFIセキュアブートが無効になっています	"ホストオペレーティングシステムをアップグレードしてから、ONTAP Mediatorをアップグレードします。"

- パスフレーズを作成するように求められます。パスフレーズは安全な場所に保存する必要があります。UEFIブートマネージャでキーを有効にするには、このパスフレーズが必要です。
- ONTAPメディエーター1.2.0以前のバージョンでは、このモードはサポートされていません。

2. ユーティリティがインストールされていない場合は `mokutil`、次のコマンドを実行します。

```
yum install mokutil
```

3. 公開鍵をMokリストに追加します。

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

秘密鍵はデフォルトの場所のままにすることも、安全な場所に移動することもできます。ただし、公開キーは、Boot Managerで使用するために既存の場所に保持する必要があります。詳細については、次のREADME.module-signingファイルを参照してください。

```
[root@hostname ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
```

4. ホストを再起動し、デバイスのUEFIブートマネージャを使用して新しいMokを承認します。でユーティリティのパスフレーズを指定する必要があります `mokutil`システムでUEFIセキュアブートが有効になっているかどうかを確認する手順。

ホスト**OS**と**ONTAP**メディエーターをアップグレードする

ONTAPメディエーター用のホストOSを新しいバージョンにアップグレードするには、最初にONTAPメディエーターをアンインストールする必要があります。

タスクの内容

leapp-upgradeツールを使用してONTAPメディエーターのホストOSを新しいメジャーバージョン（7.xから8.xなど）にアップグレードする場合は、ONTAPメディエーターをアンインストールする必要があります。これは、システムに登録されているリポジトリにインストールされているRPMの新しいバージョンが検出されるためです。

rpmファイルは**ONTAP**メディエーターのインストーラの一部としてインストールされているため、その検索に含まれます。ただし、その**.rpm**ファイルはインストーラの一部として展開され、登録されたリポジトリからダウンロードされなかったため、アップグレードが見つかりません。この場合、**leapp-upgrade**ツールはパッケージをアンインストールします。

サポートケースのトリアージに使用するログファイルを保存するには、OSをアップグレードする前にファイルをバックアップし、ONTAP Mediatorパッケージの再インストール後に復元する必要があります。ONTAP Mediatorパッケージに接続されているONTAPクラスタは、ONTAP Mediatorのインストール後に再接続する必要があります。

以下の手順は記載された順番で実行してください。ONTAP Mediatorを再インストールしたら、すぐにontap_mediatorを停止し、ログファイルを置き換えて再起動してください。これは、ログが失われないようにするためです。

手順

1. ログファイルをバックアップします。

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. leapp-upgradeツールを使用してアップグレードを実行します。

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. ONTAP Mediatorを再インストールします。

ログ ファイルが失われないように、ONTAP Mediatorの再インストール後すぐに残りの手順を実行してください。

```
[rootmediator-host ~]# ontap-mediator-1.10/ontap-mediator-1.10

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. ontap_mediator を停止します。

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. ログ ファイルを置き換えます。

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. ontap_mediator を起動します。

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. アップグレードしたONTAP Mediatorにすべてのクラスタを再接続します。

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

SnapMirrorアクティブ同期の手順

SnapMirrorアクティブ同期では、/opt/netappディレクトリ以外にTLS証明書をインストールした場合、証明書を再インストールする必要はありません。デフォルトの自己署名証明書を使用していた場合、または独自の証明書を/opt/netappディレクトリに配置していた場合は、証明書をバックアップしてリストアする必要があります。

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
```

```
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237
-peer-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true
```

```
peer1::>
```

関連情報

- "セキュリティ証明書の削除"
- "セキュリティ証明書のインストール"
- "security certificate show"
- "スナップミラーメディエーターの追加"
- "スナップミラーメディエーターの削除"
- "ストレージiscsiイニシエーターの表示"

ONTAPメディエーターをインストールするためのリポジトリアクセスの提供

インストール プロセス中に ONTAP Mediator が必要なパッケージにアクセスできるように、リポジトリへのアクセスを有効にする必要があります。

手順

1. 次の表に示すように、アクセスする必要があるリポジトリを決定します。

オペレーティングシステム	アクセスを提供するリポジトリ
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • RHEL-9-FOR-X86_64-AppStream-RPM
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • RHEL-8-FOR-x86_64-AppStream-RPM
RHEL 7.x	• rhel-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - Baseリポジトリ
ロッキーLinux 10	• AppStream • ベースオス
Rocky Linux 9	• AppStream • ベースオス

Rocky Linux 8	• AppStream • ベースオス

2. インストールプロセス中にONTAPメディエーターが必要なパッケージにアクセスできるように、上記のリポジトリへのアクセスを有効にするには、次のいずれかの手順を実行します。

> ONTAPメディエーターが「extras」および「optional」リポジトリにあるPythonモジュールに依存している場合は、 `rhel-X-for-x86_64-extras-rpms`そして `rhel-X-for-x86_64-optional-rpms` ファイル。

RHEL 10.xオペレーティング システムの手順

オペレーティング システムが **RHEL 10.x** の場合、リポジトリへのアクセスを有効にするには、次の手順に従います。

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-
rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-
x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-
x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. コマンドを実行します `yum repolist`。

新しくサブスクライブしたリポジトリがリストに表示されます。

RHEL 9.xオペレーティングシステム用手順

オペレーティングシステムが* RHEL 9.x *の場合は、次の手順を使用してリポジトリへのアクセスを有効にします。

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. コマンドを実行します `yum repolist`。

新しくサブスクライブしたリポジトリがリストに表示されます。

RHEL 8.xオペレーティングシステムでの手順

オペレーティングシステムが* RHEL 8.x *の場合は、次の手順を使用してリポジトリへのアクセスを有効にします。

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. コマンドを実行します `yum repolist`。

新しくサブスクライブしたリポジトリがリストに表示されます。

RHEL 7.xオペレーティング システムの手順

オペレーティングシステムが* RHEL 7.x *の場合は、次の手順を使用してリポジトリへのアクセスを有効にします。

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. コマンドを実行します `yum repolist`。

次の例は、このコマンドの実行例を示しています。「rhel-7-server-optional-rpms」リポジトリがリストに表示されます。

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                        repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

CentOS 7.xオペレーティングシステムでの手順

オペレーティングシステムが* CentOS 7.x *の場合、次の手順 を使用してリポジトリへのアクセスを有効にします。

以下の例はCentOS 7.6のリポジトリを示していますが、他のバージョンのCentOSでは機能しない可能性があります。使用しているCentOSのバージョンに対応したベースリポジトリを使用します。

手順

1. C7.6.1810-Baseリポジトリを追加します。C7.6.1810 - Baseヴォールトリポジトリには、ONTAPメディエーターに必要な"kernel-devel"パッケージが含まれています。
2. /etc/yum.repos.d/CentOS-Vault.repoに次の行を追加します。

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. コマンドを実行します `yum repolist`。

   次の例は、このコマンドの実行例を示しています。CentOS-7.6.1810 - Baseリポジトリがリストに表示されます。

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Rocky Linux 10、9、または8オペレーティングシステムの手順

オペレーティング システムが **Rocky Linux 10**、**Rocky Linux 9**、または **Rocky Linux 8** の場合、リポジトリへのアクセスを有効にするには、次の手順に従います。

手順

1. 必要なリポジトリにサブスクライブします。

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. 操作を実行し `clean`ます。

```
dnf clean all
```

3. リポジトリのリストを確認します。

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                          repo name
appstream                        Rocky Linux 8 - AppStream
baseos                           Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

ONTAPメディエーターのインストールパッケージをダウンロードする

インストール プロセスの一環として、ONTAP Mediator インストール パッケージをダウンロードします。

手順

1. ONTAP Mediator ダウンロード ページから ONTAP Mediator インストール パッケージをダウンロードします。

   "ONTAP メディエーターのダウンロードページ"

2. メディエーターのインストールパッケージが現在の作業ディレクトリにあることを確認します。

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.10.tgz
   ```

   ```
   ontap-mediator-1.10.tgz
   ```

   ONTAPメディエーターバージョン1.4以前の場合、インストーラの名前はです `ontap-mediator`。

   インターネットにアクセスできない場所にいる場合は、インストーラが必要なパッケージにアクセスできることを確認する必要があります。

3. 必要に応じて、Mediatorのインストールパッケージをダウンロードディレクトリから Linux Mediatorホストのインストールディレクトリに移動します。

4. インストーラパッケージを解凍します。

   ```
   tar xvfz ontap-mediator-1.10.tgz
   ```

```
ontap-mediator-1.10/
ontap-mediator-1.10/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/ONTAP-Mediator-production.pub
ontap-mediator-1.10/ontap-mediator-1.10
ontap-mediator-1.10/ontap-mediator-1.10.sig.tsr
ontap-mediator-1.10/ontap-mediator-1.10.tsr
ontap-mediator-1.10/ontap-mediator-1.10.sig
```

ONTAPメディエーターコード署名の確認

NetAppでは、ONTAPメディエーターのインストールパッケージをインストールする前に、ONTAPメディエーターコードの署名を確認することを推奨していますが、このプロセスは任意です。

開始する前に

ONTAPメディエーターコードの署名を確認する前に、システムが次の要件を満たしている必要があります。

- 2025年6月15日以降、コード署名検証証明書の有効期限が切れているため、 ONTAP Mediator 1.9および1.8のインストールまたはアップグレードはできません。代わりに、ONTAP Mediator 1.10をインストールまたはアップグレードしてください。
- システムが以下の要件を満たしていない場合は、検証プロセスは必要なく、に直接移動できます。"ONTAPメディエーターインストールパッケージのインストール"

- OpenSSLバージョン1.0.2～3.0（基本検証用）
- タイムスタンプ局（TSA）操作用のOpenSSLバージョン1.1.0以降
- OCSP検証のためのパブリックインターネットアクセス

ダウンロードパッケージには次のファイルが含まれています。

ファイル	説明
`ONTAP-Mediator-production.pub`	署名の検証に使用される公開鍵
`csc-prod-chain-ONTAP-Mediator.pem`	パブリック証明書CAの信頼チェーン
`csc-prod-ONTAP-Mediator.pem`	キーの生成に使用する証明書
`ontap-mediator-1.10`	バージョン 1.10 の製品インストール実行ファイル

ontap-mediator-1.10.sig	SHA-256はハッシュ化され、CSC-prodキーを使用してRSA署名されます（インストーラの署名）。
ontap-mediator-1.10.sig.tsr	OCSCPがインストーラの署名に使用する失効要求
ontap-mediator-1.10.tsr	タイムスタンプ署名要求ファイル
tsa-prod-ONTAP-Mediator.pem	TSRのパブリック証明書
tsa-prod-chain-ONTAP-Mediator.pem	TSRのパブリック証明書CAチェーン

手順

1. Online Certificate Status Protocol（OCSP）を使用して、で失効チェックを実行します `csc-prod-ONTAP-Mediator.pem`。

   a. 開発者証明書ではURIが指定されていない可能性があるため、証明書の登録に使用するOCSP URLを検索します。

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. 証明書のOCSP要求を生成します。

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
   ```

   c. OCSP Managerに接続してOCSP要求を送信します。

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
   ```

2. CSCの信頼チェーンと有効期限をローカルホストと照合して確認します。

   `openssl verify`

   `openssl`パスのバージョンは有効な（自己署名ではない）必要があります `cert.pem`。

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. 確認する `ontap-mediator-1.10.sig.tsr`そして `ontap-mediator-1.10.tsr`関連する証明書を使用するファイル:

```
openssl ts -verify
```

> `.tsr`ファイルには、インストーラとコード署名に関連付けられたタイムスタンプ応答が含まれています。タイムスタンプにTSAからの有効な署名があり、入力ファイルが変更されていないことが確認されます。検証はマシン上でローカルに実行されます。独立して、TSAサーバーにアクセスする必要はありません。

```
openssl ts -verify -data ontap-mediator-1.10.sig -in ontap-mediator-
1.10.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.10 -in ontap-mediator-1.10.tsr
-CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-
Mediator.pem
```

4. キーに対する署名を確認します。

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.10.sig ontap-mediator-1.10
```

ONTAPメディエーターコード署名の確認例（コンソール出力）

```
[root@scspa2695423001 ontap-mediator-1.10]# pwd
/root/ontap-mediator-1.10
[root@scspa2695423001 ontap-mediator-1.10]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.10
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.10.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.10.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.10.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.10]#
[root@scspa2695423001 ontap-mediator-1.10]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
```

```
Validation Code Signing CA - EVCS2
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
```

```
        Next Update: Mar  4 04:59:59 2023 GMT
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.10.sig -in ontap-mediator-
1.10.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.10 -in ontap-mediator-
1.10.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.10.sig ontap-mediator-1.10
Verified OK
[root@scspa2695423001 ontap-mediator-1.10]#
```

ONTAPメディエーターインストールパッケージのインストール

ONTAP Mediator をインストールするには、インストール パッケージを取得し、ホスト上でインストーラを実行する必要があります。

手順

1. インストーラを実行し、必要に応じてプロンプトに応答します。

   `./ontap-mediator-1.10/ontap-mediator-1.10 -y`

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.10/ontap-mediator-1.10 -y
   ```

   インストール中に自動署名チェックをスキップするには、次のコマンドを使用します。`./ontap-mediator-1.10/ontap-mediator-1.10 -y --skip-code-signature -check`

   インストール プロセスが開始され、必要なアカウントの作成と必要なパッケージのインストールが行われます。ホストに以前のバージョンのMediatorがインストールされている場合は、アップグレードするかどうかを確認するメッセージが表示されます。

2. ONTAP Mediator 1.4以降では、UEFIシステムでセキュア ブート メカニズムが有効になります。セキュア ブートが有効な場合、インストール後に追加の手順を実行してセキュリティ キーを登録する必要があります。

- READMEファイルの手順に従ってSCSTカーネル モジュールに署名します。

  ```
  /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing
  ```

- 必要なキーを特定します。

  ```
  /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
  ```

  READMEファイルとキーの場所は、インストール後のシステム出力にも表示されます。

ONTAP メディエーターのインストールの例（コンソール出力）

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.10.tgz
ontap-mediator-1.10/
ontap-mediator-1.10/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/ONTAP-Mediator-production.pub
ontap-mediator-1.10/ontap-mediator-1.10
ontap-mediator-1.10/ontap-mediator-1.10.sig.tsr
ontap-mediator-1.10/ontap-mediator-1.10.tsr
ontap-mediator-1.10/ontap-mediator-1.10.sig
[root@mediator_host ~]#./ontap-mediator-1.10.0/ontap-mediator-1.10.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? y(es)/N(o): yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin



Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                       Version
Repository                                             Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                             0.192-5.el10
AppStream                                              50 k
```

```
 gcc
x86_64                                          14.2.1-7.el10
AppStream                                           37 M
 kernel-devel
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                           22 M
 make
x86_64                                          1:4.4.1-9.el10
BaseOS                                             591 k
 openssl-devel
x86_64                                          1:3.2.2-16.el10
AppStream                                          3.9 M
 patch
x86_64                                          2.7.6-26.el10
AppStream                                          134 k
 perl-ExtUtils-MakeMaker
noarch                                          2:7.70-513.el10
AppStream                                          297 k
 python3-devel
x86_64                                          3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                          23.3.2-7.el10
AppStream                                          3.2 M
Installing dependencies:
 annobin-docs
noarch                                          12.92-1.el10
AppStream                                           94 k
 annobin-plugin-gcc
x86_64                                          12.92-1.el10
AppStream                                          985 k
 bison
x86_64                                          3.8.2-9.el10
AppStream                                          1.0 M
 cmake-filesystem
x86_64                                          3.30.5-2.el10
AppStream                                           29 k
 cpp
x86_64                                          14.2.1-7.el10
AppStream                                           12 M
 dwz
x86_64                                          0.15-7.el10
AppStream                                          139 k
 efi-srpm-macros
noarch                                          6-6.el10
```

```
AppStream                                          25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                         303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                          29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                          23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                          62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                         641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                          29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                         2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                          11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                          33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                          10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                         309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                          10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                         9.0 k
 package-notes-srpm-macros
noarch                                          0.5-13.el10
```

```
AppStream                                          11 k
 perl-AutoSplit
noarch                                        5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                        1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                        2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                        0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                        3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                        2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                        0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                        2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                        1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                        1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                        1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                        2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                        0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                        1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                        1:3.48-512.el10
AppStream                                         288 k
```

```
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                          16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                         9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                          68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                          16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                          26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                            273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                          83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                          13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                          78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                          72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                          41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                         202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                          21 k
 perl-Time-HiRes
x86_64                                          4:1.9777-511.el10
```

```
AppStream                                              62 k
 perl-devel
x86_64                                              4:5.40.1-512.el10
AppStream                                             772 k
 perl-doc
noarch                                              5.40.1-512.el10
AppStream                                             4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
```

```
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
  Installing       : perl-Benchmark-1.25-512.el10.noarch
```

```
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
```

```
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                   elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                        fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64                go-
srpm-macros-3.6.0-4.el10.noarch
```

```
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64              pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.10.0/ontap-mediator-1.10.0/install_20250715160240.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that reboot will be
needed.
     SCST will not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

ONTAPメディエーターのインストールステータスの確認

ONTAP Mediator をインストールした後、正常に実行されていることを確認します。

手順

1. ONTAP Mediator のステータスを表示します。
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator で使用されるポートを確認します。

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

          tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

          tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

          tcp6   0    0 :::3260          :::*            LISTEN
```

インストール後の**ONTAP**メディエーター設定

ONTAP Mediator をインストールして実行した後、ONTAP Mediator の機能を使用するには、ONTAP ストレージ システムで追加の設定タスクを実行する必要があります。

- MetroCluster IP構成でONTAPメディエーターを使用するには、 "MetroCluster IP構成からONTAPメディエーターを構成する" 。
- SnapMirrorアクティブ同期を使用するには、を参照してください"ONTAPメディエーターをインストールし、ONTAPクラスタ構成を確認します"。

ONTAPメディエーターのセキュリティポリシーの設定

ONTAP Mediator は、いくつかの構成可能なセキュリティ設定をサポートしています。すべての設定のデフォルト値は、読み取り専用ファイルで提供され `low_space_threshold_mib: 10`ます。

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

に設定した値はすべて `ontap_mediator.user_config.yaml`デフォルト値よりも優先され、ONTAPメディエーターのすべてのアップグレードで維持されます。

変更後 `ontap_mediator.user_config.yaml` ONTAPメディエーターを再起動します。

```
systemctl restart ontap_mediator
```

ONTAPメディエーターの属性を変更します。

このセクションで説明するONTAPメディエーターの属性は、必要に応じて変更できます。

> ONTAPメディエーターのアップグレード時には変更後の値が維持されないため、のその他のデフォルト値は `ontap_mediator.config.yaml`変更しないでください。

ONTAPメディエーターの属性を変更するには、必要な変数をファイルにコピーして `ontap_mediator.user_config.yaml`デフォルトの設定を上書きします。

サードパーティの**SSL**証明書のインストール

デフォルトの自己署名証明書をサードパーティのSSL証明書に置き換える必要がある場合は、次のファイルの特定の属性を変更します。

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

これらのファイル内の変数は、ONTAP Mediator で使用される証明書ファイルを制御するために使用されます。

ONTAP Mediator 1.9以降

次の表に示すデフォルトの変数は、ファイルに含まれて`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`います。

変数	パス
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days`は、クライアント証明書の有効期限を設定するために使用されます。最大値は3年（1095日）です。
- `x509_passin_pwd`は、署名済みクライアント証明書のパスフレーズです。

次の表に示すデフォルトの変数は、ファイルに含まれて`/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`います。

変数	パス
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt

ONTAPメディエーター**1.8**以前

次の表に示すデフォルトの変数は、ファイルに含まれて`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`います。

変数	パス
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days`は、クライアント証明書の有効期限を設定するために使用されます。最大値は3年（1095日）です。
- `x509_passin_pwd`は、署名済みクライアント証明書のパスフレーズです。

次の表に示すデフォルトの変数は、ファイルに含まれて`/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`います。

変数	パス
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

これらの属性を変更する場合は、変更を適用するために ONTAP Mediator を再起動します。デフォルトの証明書をサードパーティの証明書に置き換える方法の詳細については、を参照してください"自己署名証明書を信頼できるサードパーティの証明書に置き換える"。

パスワード攻撃からの保護

次の設定は、ブルートフォースパスワード推測攻撃に対する保護を提供します。

この機能を有効にするには、およびの `retry_limit`値を設定し `window_seconds`ます。

例：

- 5分間の猶予期間を設けて推測し、失敗回数をゼロにリセットします。

  ```
  authentication_lock_window_seconds: 300
  ```

- 期間内に5つの障害が発生した場合は、アカウントをロックします。

  ```
  authentication_retry_limit: 5
  ```

- 各試行を拒否する前に発生する遅延を設定することで、ブルートフォースパスワード推測攻撃の影響を軽減し、攻撃の速度を低下させます。

  ```
  authentication_failure_delay_seconds: 5
  ```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to allow
before locking API access, null = unlimited
```

パスワードの複雑さに関するルール

次のフィールドは、ONTAPメディエーターAPIユーザアカウントのパスワードの複雑さのルールを制御します。

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

空きスペースの制御

ディスク上の必要な空き容量を制御する設定があり `/opt/netapp/lib/ontap_mediator`ます。

スペースが設定されたしきい値を下回ると、サービスは警告イベントを発行します。

```
low_space_threshold_mib: 10
```

リザーブログスペースの制御

reserve_log_spaceは、特定の設定によって制御されます。デフォルトでは、ONTAP Mediator のインストール時にログ用のディスクスペースが別途作成されます。インストーラは、ONTAP Mediator のログ記録専用として、合計 700MB のディスクスペースを持つ新しい固定サイズのファイルを作成します。

この機能を無効にしてデフォルトのディスク容量を使用するには、次の手順に従います。

1. 次のファイルで、reserve_log_spaceの値を1から0に変更します。

   ```
   /opt/netapp/lib/ontap_mediator/tools/mediator_env
   ```

2. Mediatorを再起動します。

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

この機能を再度有効にするには、値を0から1に変更してMediatorを再起動します。

ディスクスペースを切り替えても、既存のログは消去されません。以前のログはすべてバックアップされ、Mediatorの切り替えと再起動のあとに現在のディスクスペースに移動されます。

ONTAPメディエーターの管理

ユーザー認証情報の変更、サービスの停止と再有効化、サービスの健全性の検証、ホストのメンテナンスのための SCST のインストールまたはアンインストールなど、ONTAP Mediator を管理します。また、自己署名証明書の再生成、信頼されたサードパーティ証明書への置き換え、証明書関連の問題のトラブルシューティングなど、証明書の管理も行うことができます。

ユーザ名の変更

ユーザ名は次の手順を使用して変更できます。

タスクの内容

ONTAP Mediator をインストールした Linux ホストでこのタスクを実行します。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

```
/usr/local/bin/mediator_username
```

手順

次のいずれかを実行してユーザ名を変更します。

- オプション（**a**）：コマンドを実行し `mediator_change_user`、次の例に示すようにプロンプトに応答します。

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- オプション（**b**）：次のコマンドを実行します。

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

パスワードの変更

パスワードは次の手順を使用して変更できます。

タスクの内容

ONTAP Mediator をインストールした Linux ホストでこのタスクを実行します。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

```
/usr/local/bin/mediator_change_password
```

手順

次のいずれかを実行してパスワードを変更します。

- オプション（**a**）：コマンドを実行し `mediator_change_password`、次の例に示すようにプロンプトに応答します。

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
          Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- オプション（**b**）：次のコマンドを実行します。

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

この例では、パスワードが「mediator1」から「mediator2」に変更されています。

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

ONTAPメディエーターを停止する

ONTAP Mediator を停止するには、次の手順を実行します。

手順

1. ONTAP メディエーターを停止します。

```
systemctl stop ontap_mediator
```

2. SCSTを停止します。

```
systemctl stop mediator-scst
```

3. ONTAP メディエーターと SCST を無効にします。

```
systemctl diable ontap_mediator mediator-scst
```

ONTAPメディエーターを再度有効にする

ONTAP Mediator を再度有効にするには、次の手順を実行します。

手順

1. ONTAP Mediator と SCST を有効にします。

```
systemctl enable ontap_mediator mediator-scst
```

2. SCSTを開始します。

```
systemctl start mediator-scst
```

3. ONTAPメディエーターを起動します。

```
systemctl start ontap_mediator
```

ONTAPメディエーターが正常であることを確認する

ONTAP Mediator をインストールした後、正常に実行されていることを確認します。

手順

1. ONTAP Mediator のステータスを表示します。
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator で使用されるポートを確認します。

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

ONTAPメディエーターのアンインストール

必要に応じて、ONTAP Mediator を削除できます。

開始する前に

ONTAP Mediator を削除する前に、ONTAP から切断する必要があります。

タスクの内容

ONTAP Mediator をインストールした Linux ホストでこのタスクを実行します。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

`/usr/local/bin/uninstall_ontap_mediator`

ステップ

1. ONTAP Mediator をアンインストールします。

```
uninstall_ontap_mediator
```

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

一時的な自己署名証明書の再生成

ONTAPメディエーター1.7以降では、次の手順を使用して一時的な自己署名証明書を再生成できます。

> この手順は、ONTAPメディエーター1.7以降を実行しているシステムでのみサポートされます。

タスクの内容

- ONTAP Mediator をインストールした Linux ホストでこのタスクを実行します。
- このタスクは、ONTAP Mediator のインストール後にホストのホスト名または IP アドレスが変更されたために、生成された自己署名証明書が古くなった場合にのみ実行できます。
- 一時的な自己署名証明書を信頼できるサードパーティ証明書に置き換えたあと、このタスクを使用して証明書を再生成します。自己署名証明書がないと、この手順は失敗します。

ステップ

現在のホストの新しい一時的な自己署名証明書を再生成するには、次の手順を実行します。

1. ONTAP メディエーターを再起動します。

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

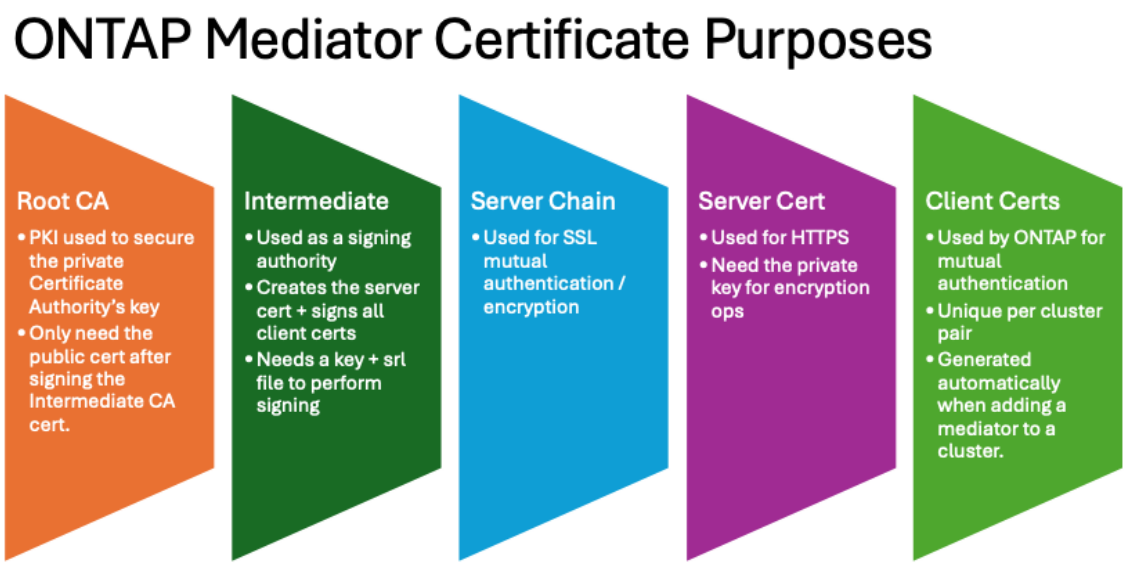
自己署名証明書を信頼できるサードパーティ証明書に置き換える

自己署名証明書がサポートされている場合は、信頼できるサードパーティの証明書に置き換えることができます。

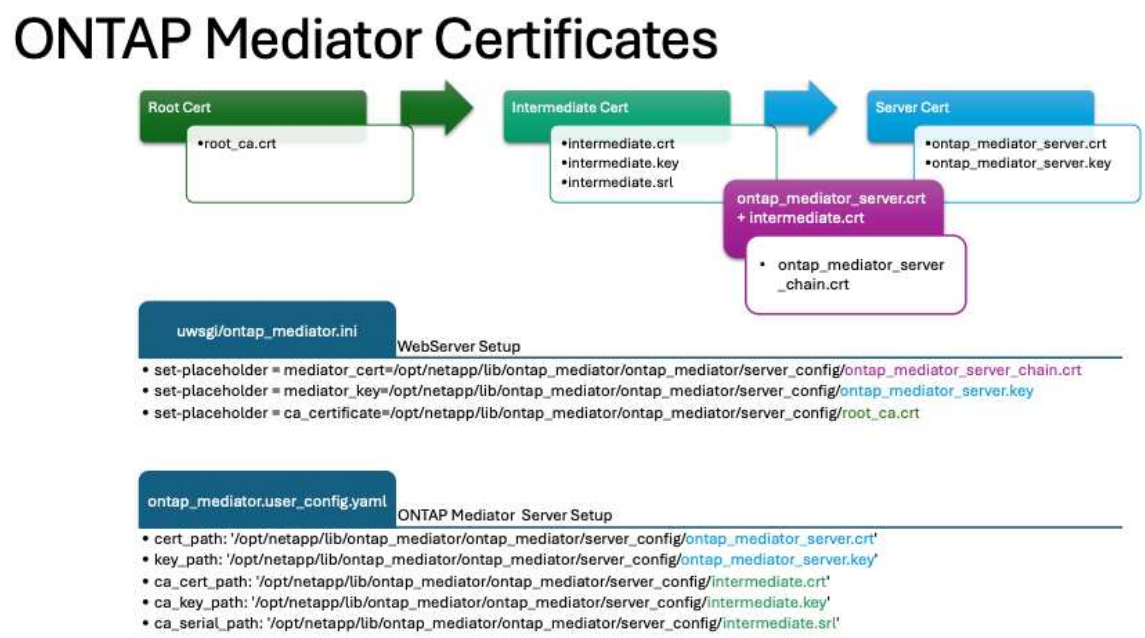
- サードパーティ証明書は、ONTAP 9 .16.1以降および一部の以前のONTAPパッチリリースでのみサポートされています。を参照して "NetApp Bugs OnlineのバグIDCONTAP-243278"
- サードパーティの証明書は、ONTAP Mediator 1.7以降を実行するシステムでのみサポートされます。

タスクの内容

- ONTAP Mediator をインストールした Linux ホストでこのタスクを実行します。
- このタスクは、生成された自己署名証明書を、信頼された下位の認証局（CA）から取得した証明書に置き換える必要がある場合に実行できます。これを実現するには、信頼できる公開キーインフラストラクチャ（PKI）権限にアクセスする必要があります。
- 次の図は、各ONTAPメディエーター証明書の目的を示しています。



- 次の図は、Web サーバのセットアップと ONTAP Mediator のセットアップの構成を示しています。



手順**1**：**CA**証明書を発行しているサードパーティから証明書を取得する

次の手順を使用して、PKI認証局から証明書を取得できます。

次の例は、にあるサードパーティの証明書アクターで自己署名証明書アクターを置き換える方法を示してい `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`ます。

この例では、ONTAP Mediator に必要な証明書の必要な基準を示します。この手順とは異なる方法で、PKI認証局から証明書を取得できます。ビジネスニーズに応じて手順を調整します。

ONTAP Mediator 1.9以降

1. PKI機関が証明書を生成するために使用する秘密鍵とコンフィギュレーションファイルを `openssl_ca.cnf`作成します `intermediate.key`。

   a. 秘密鍵を生成し `intermediate.key`ます。

      ▪ 例 *

```
openssl genrsa -aes256 -out intermediate.key 4096
```

   a. 構成ファイル `openssl_ca.cnf`（にあります `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`）は、生成された証明書に必要なプロパティを定義します。

2. 秘密鍵と構成ファイルを使用して、証明書署名要求を作成し `intermediate.csr`ます。

   ◦ 例： *

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key
-new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@scs000216655 server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. 証明書署名要求をPKI機関に送信し `intermediate.csr`て署名を求めます。

   PKI機関はリクエストを検証し、署名します。 `.csr`、証明書を生成する `intermediate.crt`。さらに、 `root_ca.crt`署名した証明書 `intermediate.crt`PKI 機関からの証明書。

> SnapMirror Business Continuity（SM-BC）クラスタの場合は、 `intermediate.crt`そして `root_ca.crt`ONTAPクラスタに証明書を追加します。見る"SnapMirror Active Sync 用に ONTAP Mediator とクラスタを構成する"。

ONTAPメディエーター1.8以前

1. PKI機関が証明書を生成するために使用する秘密鍵とコンフィギュレーションファイルを `openssl_ca.cnf`作成します `ca.key`。

   a. 秘密鍵を生成し `ca.key`ます。

      ▪ 例 *

```
openssl genrsa -aes256 -out ca.key 4096
```

   a. 構成ファイル `openssl_ca.cnf`（にあります `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.c`

nf）は、生成された証明書に必要なプロパティを定義します。

2. 秘密鍵と構成ファイルを使用して、証明書署名要求を作成し `ca.csr`ます。

   ◦ 例： *

   ```
   openssl req -key <private_key_name>.key -new -out
   <certificate_csr_name>.csr -config <config_file_name>.cnf
   ```

   ```
   [root@scs000216655 server_config]# openssl req -key ca.key -new
   -config openssl_ca.cnf -out ca.csr
   Enter pass phrase for ca.key:
   [root@scs000216655 server_config]# cat ca.csr
   -----BEGIN CERTIFICATE REQUEST-----
   <certificate_value>
   -----END CERTIFICATE REQUEST-----
   ```

3. 証明書署名要求をPKI機関に送信し `ca.csr`て署名を求めます。

   PKI認証局は要求を検証し、に署名して `.csr`証明書を生成し `ca.crt`ます。さらに、PKI認証局から証明書を取得する必要があり `root_ca.crt that signed the `ca.crt`ます。

   SnapMirrorビジネス継続性（SM-BC）クラスタの場合は、証明書と証明書をONTAPクラスタに追加する必要があります `ca.crt` `root_ca.crt` 。を参照して "SnapMirror Active Sync 用に ONTAP Mediator とクラスタを構成する"

手順**2**：サードパーティの**CA**証明書で署名してサーバ証明書を生成する

ONTAP Mediator 1.9以降

サーバ証明書は、秘密鍵とサードパーティ証明書 `intermediate.crt`によって署名されている必要があります `intermediate.key`。また、構成ファイル `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`には、OpenSSLによって発行されるサーバー証明書に必要なプロパティを指定する特定の属性が含まれています。

サーバ証明書を生成するには、次のコマンドを実行します。

手順

1. サーバ証明書署名要求（CSR）を生成するには、フォルダから次のコマンドを実行し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ます。

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. CSRからサーバ証明書を生成するには、フォルダから次のコマンドを実行し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ます。

> これらのファイルはPKI機関から取得されました。別の証明書名を使用している場合は、および `intermediate.key`を関連するファイル名に置き換え `intermediate.crt`ます。

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- `-CAcreateserial`オプションを使用してファイルを生成し `intermediate.srl`ます。

ONTAPメディエーター**1.8**以前

サーバ証明書は、秘密鍵とサードパーティ証明書 `ca.crt`によって署名されている必要があります `ca.key`。また、構成ファイル `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`には、OpenSSLによって発行されるサーバー証明書に必要なプロパティを指定する特定の属性が含まれています。

サーバ証明書を生成するには、次のコマンドを実行します。

手順

1. サーバ証明書署名要求（CSR）を生成するには、フォルダから次のコマンドを実行し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ます。

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. CSRからサーバ証明書を生成するには、フォルダから次のコマンドを実行し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ます。

これらのファイルはPKI機関から取得されました。別の証明書名を使用している場合は、および `ca.key`を関連するファイル名に置き換え `ca.crt`ます。

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- `-CAcreateserial`オプションを使用してファイルを生成し `ca.srl`ます。

手順**3**：**ONTAP**メディエーター構成で新しいサードパーティの**CA**証明書とサーバ証明書を交換する

ONTAPメディエーター**1.10**以降

証明書の設定は、次の場所にある設定ファイルでONTAPメディエーターに提供されます。 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 。このファイルには、次の属性が含まれています。

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path`および `key_path`は、サーバ証明書変数です。
- `ca_cert_path`、 `ca_key_path`、および `ca_serial_path`はCA証明書変数です。

手順

1. すべてのファイルをサードパーティの証明書に置き換えます `intermediate.*` 。
2. および証明書から証明書チェーンを作成し `intermediate.crt` `ontap_mediator_server.crt` ます。

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. 更新する `/opt/netapp/lib/ontap_mediator/uvicorn/config.json`ファイル。

   値を更新する `ssl_keyfile`、 `ssl_certfile` 、 そして `ssl_ca_certs`:

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   ssl_ca_certs:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

- その `ssl_keyfile`値はキーパスです `ontap_mediator_server.crt`ファイル、これは `ontap_mediator_server.key`。
- その `ssl_certfile`値は、 `ontap_mediator_server_chain.crt`ファイル。
- その `ssl_ca_certs`値は、 `root_ca.crt`ファイル。

4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します。
   - Linuxグループ所有者： `netapp:netapp`
   - Linux権限： `600`
5. ONTAP メディエーターを再起動します。

```
systemctl restart ontap_mediator
```

ONTAPメディエーター **1.9.1** および **1.9**

証明書の設定は、次の場所にある設定ファイルでONTAPメディエーターに提供されます。 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 。このファイルには、次の属性が含まれています。

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path`および `key_path`は、サーバ証明書変数です。
- `ca_cert_path`、 `ca_key_path`、および `ca_serial_path`はCA証明書変数です。

手順

1. すべてのファイルをサードパーティの証明書に置き換えます `intermediate.*` 。
2. および証明書から証明書チェーンを作成し `intermediate.crt` `ontap_mediator_server.crt` ます。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. ファイルを更新し `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ます。

   、、およびの値を更新し `mediator_cert` `mediator_key` `ca_certificate`ます。

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`値はファイルのパス `ontap_mediator_server_chain.crt` です。
   - `mediator_key value`は、ファイル内のキーパスです `ontap_mediator_server.crt ontap_mediator_server.key`。
   - `ca_certificate`値はファイルのパス `root_ca.crt` です。

4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します。
   - Linuxグループ所有者： `netapp:netapp`
   - Linux権限： `600`

5. ONTAP メディエーターを再起動します。

   ```
   systemctl restart ontap_mediator
   ```

ONTAPメディエーター**1.8**以前

証明書の設定は、次の場所にある設定ファイルでONTAPメディエーターに提供されます。`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 。このファイルには、次の属性が含まれています。

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path`および `key_path`は、サーバ証明書変数です。

- `ca_cert_path`、 `ca_key_path`、および `ca_serial_path`はCA証明書変数です。

手順

1. すべてのファイルをサードパーティの証明書に置き換えます `ca.*` 。
2. および証明書から証明書チェーンを作成し `ca.crt` `ontap_mediator_server.crt` ます。

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. ファイルを更新し `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ます。

   、、およびの値を更新し `mediator_cert` `mediator_key` `ca_certificate`ます。

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`値はファイルのパス `ontap_mediator_server_chain.crt` です。
   - `mediator_key value`は、ファイル内のキーパスです `ontap_mediator_server.crt ontap_mediator_server.key`。
   - `ca_certificate`値はファイルのパス `root_ca.crt` です。
4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します。
   - Linuxグループ所有者： `netapp:netapp`
   - Linux権限： `600`
5. ONTAP メディエーターを再起動します。

   ```
   systemctl restart ontap_mediator
   ```

手順**4**：必要に応じて、サードパーティの証明書に別のパスまたは名前を使用します。

ONTAPメディエーター**1.10**以降

とは別の名前のサードパーティ証明書を使用することも、サードパーティ証明書を別の場所に保存することもできます `intermediate.*`。

手順

1. ファイル内のデフォルトの変数値を上書きするようにファイルを構成し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` `ontap_mediator.config.yaml` ます。

   PKI権限から取得した秘密鍵をの場所に保存した場合、 `intermediate.crt` `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` ファイルは次の例のようになります。

   を使用して証明書に署名した場合は、 `intermediate.crt` `ontap_mediator_server.crt` `intermediate.srl` ファイルが生成されます。詳細については、を参照してください 手順2：サードパーティのCA証明書で署名してサーバ証明書を生成する 。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 証明書構造を使用している場合、 `root_ca.crt`証明書は `intermediate.crt`署名する証明書 `ontap_mediator_server.crt`証明書の場合は、 `intermediate.crt`そして `ontap_mediator_server.crt`証明書:

> この手順の前半で、PKI機関から証明書と証明書を入手しておく必要があります `intermediate.crt` `ontap_mediator_server.crt` 。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. 更新する `/opt/netapp/lib/ontap_mediator/uvicorn/config.json`ファイル。

値を更新する `ssl_keyfile`、 `ssl_certfile` 、 そして `ssl_ca_certs`:

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

ssl_certfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

ssl_ca_certs:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- その `ssl_keyfile`値はキーパスです `ontap_mediator_server.crt`ファイル、これは `ontap_mediator_server.key。
- その `ssl_certfile`値は、 `ontap_mediator_server_chain.crt`ファイル。
- その `ssl_ca_certs`値は、 `root_ca.crt`ファイル。

> SnapMirror Business Continuity（SM-BC）クラスタの場合は、 `intermediate.crt`そして `root_ca.crt`ONTAPクラスタに証明書を追加します。見る"SnapMirror Active Sync 用に ONTAP Mediator とクラスタを構成する"。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します。

- Linuxグループ所有者： `netapp:netapp`
- Linux権限： `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAPメディエーター **1.9.1** および **1.9**

とは別の名前のサードパーティ証明書を使用することも、サードパーティ証明書を別の場所に保存することもできます `intermediate.*`。

手順

1. ファイル内のデフォルトの変数値を上書きするようにファイルを構成し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` `ontap_mediator.config.yaml` ます。

   PKI権限から取得した秘密鍵をの場所に保存した場合、 `intermediate.crt` `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` ファイルは次の例のようになります。

> を使用して証明書に署名した場合は、 `intermediate.crt` `ontap_mediator_server.crt` `intermediate.srl` ファイルが生成されます。詳細については、を参照してください 手順2：サードパーティのCA証明書で署名してサーバ証明書を生成する 。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 証明書構造を使用している場合、 `root_ca.crt`証明書は `intermediate.crt`署名する証明書 `ontap_mediator_server.crt`証明書の場合は、 `intermediate.crt`そして `ontap_mediator_server.crt`証明書:

> この手順の前半で、PKI機関から証明書と証明書を入手しておく必要があります `intermediate.crt` `ontap_mediator_server.crt` 。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. ファイルを更新し `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ます。

、、およびの値を更新し `mediator_cert` `mediator_key` `ca_certificate`ます。

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`値はファイルのパス `ontap_mediator_server_chain.crt` です。
- この `mediator_key` 値は、ファイル内のキーパス（ `ontap_mediator_server.crt` ）です。 `ontap_mediator_server.key`
- `ca_certificate`値はファイルのパス `root_ca.crt` です。

> SnapMirror Business Continuity（SM-BC）クラスタの場合は、`intermediate.crt`そして `root_ca.crt`ONTAPクラスタに証明書を追加します。見る"SnapMirror Active Sync 用に ONTAP Mediator とクラスタを構成する"。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します。

- Linuxグループ所有者： `netapp:netapp`
- Linux権限： `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAPメディエーター**1.8**以前

とは別の名前のサードパーティ証明書を使用することも、サードパーティ証明書を別の場所に保存することもできます `ca.*`。

手順

1. ファイル内のデフォルトの変数値を上書きするようにファイルを構成し `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` `ontap_mediator.config.yaml` ます。

   PKI権限から取得した秘密鍵をの場所に保存した場合、 `ca.crt` `ca.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` ファイルは次の例のようになります。

> を使用して証明書に署名した場合は、 `ca.crt` `ontap_mediator_server.crt` `ca.srl` ファイルが生成されます。詳細については、を参照してください 手順2：サードパーティのCA証明書で署名してサーバ証明書を生成する 。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. 証明書が証明書に署名する証明書を提供する証明書構造を使用している場合は `root_ca.crt` `ca.crt` `ontap_mediator_server.crt` 、および証明書から証明書チェーンを作成し `ca.crt` `ontap_mediator_server.crt` ます。

> この手順の前半で、PKI機関から証明書と証明書を入手しておく必要があります `ca.crt` `ontap_mediator_server.crt` 。

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. ファイルを更新し `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ます。

、、およびの値を更新し `mediator_cert` `mediator_key` `ca_certificate`ます。

```
set-placeholder = mediator_cert =
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`値はファイルのパス `ontap_mediator_server_chain.crt` です。
- この `mediator_key` 値は、ファイル内のキーパス（ `ontap_mediator_server.crt` ）です。 `ontap_mediator_server.key`
- `ca_certificate`値はファイルのパス `root_ca.crt` です。

> SnapMirrorビジネス継続性（SM-BC）クラスタの場合は、証明書と証明書をONTAPクラスタに追加する必要があります `ca.crt` `root_ca.crt` 。を参照して "SnapMirror Active Sync 用に ONTAP Mediator とクラスタを構成する"

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します。

- Linuxグループ所有者： `netapp:netapp`
- Linux権限： `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

証明書関連の問題のトラブルシューティング

証明書の特定のプロパティを確認できます。

証明書の有効期限を確認

証明書の有効範囲を確認するには、次のコマンドを使用します。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAPメディエーター1.8以前

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

CA証明書でのX509v3拡張の確認

次のコマンドを使用して、CA証明書のX509v3拡張を確認します。

ONTAP Mediator 1.9以降

で `openssl_ca.cnf`定義されたプロパティは `**v3_ca**`、の `intermediate.crt`ように表示され `X509v3 extensions`ます。

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAPメディエーター**1.8**以前

で `openssl_ca.cnf`定義されたプロパティは `**v3_ca**`、の `ca.crt`ように表示され `X509v3 extensions`ます。

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

サーバ証明書およびサブジェクトの代替名の**X509v3**拡張を確認する

`v3_req`構成ファイルで定義されたプロパティは `openssl_server.cnf`、証明書でと表示され `X509v3 extensions`ます。

次の例では、 `alt_names`コマンドを実行してセクション `hostname -A`そして `hostname -I` ONTAP Mediator がインストールされている Linux VM 上。

変数の正しい値については、ネットワーク管理者に確認してください。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAPメディエーター1.8以前

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

秘密鍵が証明書と一致することを確認する

特定の秘密鍵が証明書と一致するかどうかを確認できます。

キーと証明書に対して、それぞれ次のOpenSSLコマンドを使用します。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAPメディエーター1.8以前

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

両方の属性が一致する場合、 `-modulus`秘密鍵と証明書のペアに互換性があり、相互に動作できることを示します。

サーバ証明書が特定の**CA**証明書から作成されていることを確認する

サーバ証明書が特定のCA証明書から作成されたことを確認するには、次のコマンドを使用します。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAPメディエーター1.8以前

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Online Certificate Status Protocol（OCSP）検証を使用している場合は、コマンドを使用し "OpenSSL -検証" ます。

ONTAPメディエーター用のホストOSの保守

最適なパフォーマンスを得るために、 ONTAP Mediator のホスト OS を定期的にメンテナンスしてください。

ホストをリブートする

クラスターが正常な場合にのみホストを再起動します。 ONTAP Mediator がオフラインの間、クラスタは障害に応答できません。再起動する前にサービス ウィンドウをスケジュールします。

ONTAP Mediator は再起動時に自動的に再開し、 ONTAPクラスタとの以前に設定された関係を再入力します。

ホストパッケージノコウシン

カーネル以外のライブラリまたは yum パッケージを更新します。変更を有効にするには、必要に応じてホストを再起動します。ホストを再起動する前にサービス ウィンドウをスケジュールします。

パッケージをインストールした場合 `yum-utils`は、コマンドを使用し `needs-restarting`て、パッケージの変更にリブートが必要かどうかを確認します。

変更はすぐには有効にならないため、 ONTAP Mediator の依存関係を更新した後は再起動してください。

ホストOSのカーネルのマイナーアップグレード

SCSTは、使用しているカーネル用にコンパイルされている必要があります。OSを更新するには、メンテナンス時間が必要です。

手順

ホストOSカーネルをアップグレードするには、次の手順を実行します。

> カーネルをアップグレードする前に、OS とONTAP Mediator のバージョンに互換性があることを確認してください。サポートされているバージョンについては、"OSのサポート対応表" 。

1. ONTAP メディエーターを停止します。
2. SCSTパッケージをアンインストールします。[ホストのメンテナンスを実行する] 。（SCSTにはアップグレード メカニズムがありません）。
3. OSをアップグレードし、再起動します。
4. SCSTパッケージを再インストールします。
5. ONTAP Mediator を再度有効にします。

ホストのメンテナンスを実行する

VM カーネルをアップグレードすると、SCST モジュールとの互換性の問題が発生する可能性があります。SCST を手動でアンインストールして再インストールします。

ステップ1：SCSTをアンインストールする

SCST をアンインストールするには、 ONTAP Mediator バージョンの tar バンドルを使用します。

手順

1. 適切な SCST バンドル (次の表を参照) をダウンロードして解凍します。

バージョン	使用するtarバンドル
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAPメディエーター1.9.1	scst-3.8.0.tar.bz2
ONTAPメディエーター1.9	scst-3.8.0.tar.bz2
ONTAPメディエーター1.8	scst-3.8.0.tar.bz2
ONTAPメディエーター1.7	scst-3.7.0.tar.bz2
ONTAPメディエーター1.6	scst-3.7.0.tar.bz2
ONTAPメディエーター1.5	scst-3.6.0.tar.bz2
ONTAPメディエーター1.4	scst-3.6.0.tar.bz2
ONTAPメディエーター1.3	scst-3.5.0.tar.bz2
ONTAPメディエーター1.1	scst-3.4.0.tar.bz2
ONTAPメディエーター1.0	scst-3.3.0.tar.bz2

   a. オープンソースパッケージにアクセスするには、"SCST SourceForge ダウンロード" 。
   b. *リリースバージョンのダウンロード*を選択します。
   c. バンドルを VM に抽出します。
2. 以下のアンインストールコマンドを実行します。 `scst`ディレクトリ：
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

ステップ**2: SCST**をインストールする

SCSTを手動でインストールするには、インストールされているバージョンのONTAPメディエーターで使用されるSCST tarバンドルが必要です（SCSTテーブルARPテーブル ）。

ONTAP Mediator をインストールする前にこの手順を実行します。使用している SCST バージョンがONTAP Mediator インストーラにバンドルされているバージョンよりも新しい場合、インストーラはこの手順をスキップします。

1. 以下のインストールコマンドを実行します。 `scst`ディレクトリ：
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`

      初めてインストールを実行し、 ONTAP Mediator を事前にインストールする場合は、次の手順に進む前に次のコマンドを実行します。

      ```
      mkdir -p
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
      ```

   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

      初回インストール時にONTAP Mediator の前に SCST を事前インストールする場合は、この手順をスキップしてください。インストーラーは関連する SCST パッチを適用します。

2. セキュアブートが有効になっている場合は、リブートする前に、次の手順を実行します。
   a. 各ファイル名を決定する `scst_vdisk`、 `scst` 、 そして `iscsi_scst`モジュール:

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. カーネルのリリースを確認します。

      ```
      [root@localhost ~]# uname -r
      ```

   c. 各モジュール ファイルをカーネルで署名します。

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. ファームウェアとともに UEFI キーをインストールします。

UEFIキーのインストール手順は、次の場所にあります。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

生成されたUEFIキーは次の場所にあります。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. システムを再起動します。

```
reboot
```

ホストがホスト名または**IP**に変更

タスクの内容

- ONTAP Mediator をインストールした Linux ホストでこのタスクを実行します。
- ONTAP Mediator のインストール後にホスト名または IP アドレスが変更されたために自己署名証明書が古くなった場合にのみ、このタスクを実行してください。
- 一時的な自己署名証明書が信頼できるサードパーティの証明書に置き換えられた後は、このタスクを使用して証明書を再生成しないでください。自己署名証明書がない場合は、この手順は使用できません。

ステップ

現在のホストの一時的な自己署名証明書を作成します。

1. ONTAP メディエーターを再起動します。

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

ONTAP System Managerを使用したMetroCluster IPサイト管理について学習します

MetroCluster構成では、別 々 の場所にある2つのONTAPクラスタ間でデータと設定を同期的にミラーリングします。ONTAP 9 .8以降では、MetroCluster IP設定を管理するためのシンプルなインターフェイスとしてSystem Managerを使用できます。

MetroCluster IP構成では、System Managerを使用してのみMetroCluster処理を実行できます。MetroCluster FC構成では、System Managerを使用してMetroCluster構成内の各ノードを管理できますが、MetroCluster固有の処理を実行することはできません。

通常、クラスタは2つの地理的に離れた場所にあるMetroCluster構成でセットアップおよび設定します。その後、クラスタ間でデータが同期および共有されるようにピアリングを設定します。ピアネットワークにある2つのクラスタは双方向のディザスタリカバリ（DR）を提供し、各クラスタをもう一方のクラスタのソースおよびバックアップとして使用できます。8ノードまたは4ノードのMetroCluster IP構成では、それぞれのサイト

に、1つまたは2つのハイアベイラビリティ（HA）ペアとして構成されたストレージコントローラが含まれます。

3つ目の場所では、ノードとそのDRパートナーの状態を監視できます"ONTAPメディエーターをインストールする"。ONTAP Mediator は、災害発生時に Mediator 支援による計画外スイッチオーバー (MAUSO) を実装できます。

ネゴシエートスイッチオーバーを実行して、計画的メンテナンスのために一方のクラスタを停止することもできます。メンテナンスを実行したクラスタを起動してスイッチバック処理を実行するまで、両方のクラスタのすべてのデータI/O処理はパートナークラスタで処理されます。

System Managerを使用してMetroCluster IP設定をセットアップおよび管理する手順については、を"MetroClusterのドキュメント"参照してください。

テープバックアップを使用したデータ保護

ONTAP FlexVolボリュームのテープバックアップについて学ぶ

ONTAPは、ネットワークデータ管理プロトコル（NDMP）を使用したテープバックアップおよびリストアをサポートしています。NDMPを使用すると、ストレージシステム内のデータを直接テープにバックアップできるため、ネットワーク帯域幅を効率的に使用できます。ONTAPでは、テープバックアップ用にダンプエンジンとSMTapeエンジンの両方がサポートされます。

NDMP準拠のバックアップアプリケーションを使用して、ダンプまたはSMTapeバックアップ/リストアを実行できます。NDMPバージョン4のみがサポートされます。

ダンプによるテープバックアップ

ダンプは、ファイルシステムのデータをテープにバックアップするSnapshotベースのバックアップです。ONTAPダンプエンジンは、ファイル、ディレクトリ、および該当するAccess Control List（ACL；アクセス制御リスト）情報をテープにバックアップします。バックアップできるのは、ボリューム全体、qtree全体、またはボリューム全体やqtree全体ではないサブツリーです。ダンプでは、ベースラインバックアップ、差分バックアップ、増分バックアップがサポートされます。

SMTapeによるテープバックアップ

SMTapeは、データのブロックをテープにバックアップする、ONTAPのSnapshotベースのディザスタリカバリソリューションです。SMTapeを使用すると、テープへのボリュームバックアップを実行できます。ただし、qtreeレベルまたはサブツリーレベルでバックアップを実行することはできません。SMTapeでは、ベースラインバックアップ、差分バックアップ、および増分バックアップがサポートされます。

ONTAP 9.13.1以降では、SMTapeを使用したテープバックアップがでサポートされSnapMirrorアクティブ同期ます。

ONTAPテープ バックアップと復元のワークフロー

NDMP対応のバックアップアプリケーションを使用して、テープバックアップおよびリストア処理を実行できます。

タスクの内容

テープバックアップとリストアのワークフローでは、テープバックアップとリストア処理の実行に関連するタスクの概要を示します。バックアップおよびリストア処理の実行の詳細については、バックアップアプリケーションのマニュアルを参照してください。

手順

1. NDMPでサポートされているテープトポロジを選択して、テープライブラリの構成を設定します。
2. ストレージシステムでNDMPサービスを有効にします。

   NDMPサービスはノードレベルまたはStorage Virtual Machine（SVM）レベルで有効にできます。これは、テープバックアップおよびリストア処理を実行するために選択したNDMPモードによって異なります。

3. NDMPオプションを使用して、ストレージシステムでNDMPを管理します。

   NDMPオプションはノードレベルまたはSVMレベルで使用できます。これは、テープバックアップおよびリストア処理を実行するために選択したNDMPモードによって異なります。

   NDMPオプションは、コマンドを使用してノードレベルで変更するか、コマンドを使用してSVMレベルで `vserver services ndmp modify` 変更できます `system services ndmp modify`。および `vserver services ndmp modify` の詳細については `system services ndmp modify`、を"ONTAPコマンド リファレンス"参照してください。

4. NDMP対応のバックアップアプリケーションを使用して、テープバックアップまたはリストア処理を実行します。

   ONTAPでは、テープバックアップおよびリストア用にダンプエンジンとSMTapeエンジンの両方がサポートされます。

   バックアップアプリケーション（ _ データ管理アプリケーション _ または _ DMA _ とも呼ばれる）を使用してバックアップまたはリストア操作を実行する方法の詳細については、バックアップアプリケーションのマニュアルを参照してください。

関連情報

一般的なNDMPテープバックアップトポロジ

FlexVolのダンプエンジンの概要

ONTAP SMTapeおよびダンプバックアップエンジンの使用例

ONTAP では、 SMTape とダンプの 2 つのバックアップエンジンがサポートされます。SMTape バックアップエンジンとダンプバックアップエンジンのユースケースについて理解しておくと、テープバックアップおよびリストア処理を実行するバックアップエンジンを選択する際に役立ちます。

ダンプは次の場合に使用できます。

- ファイルおよびディレクトリの Direct Access Recovery （ DAR ）
- 特定のパスの一部のサブディレクトリまたはファイルのバックアップ

- バックアップ中に特定のファイルおよびディレクトリを除外する
- 長期間にわたるバックアップの保持

SMTape は、次の場合に使用できます。

- ディザスタリカバリ解決策
- リストア処理時にバックアップしたデータの重複排除による削減効果および重複排除設定の保持
- 大容量ボリュームのバックアップ

テープドライブを管理します。

ONTAPテープドライブの管理について学ぶ

テープバックアップまたはリストア処理を実行する前に、テープライブラリの接続とテープドライブの情報を確認できます。未認定テープドライブを使用するには、認定テープドライブにエミュレートします。また、既存のエイリアスを表示するだけでなく、テープエイリアスを割り当てたり削除したりすることもできます。

データをテープにバックアップすると、データはテープファイルに保存されます。テープファイルはファイルマークで区切られ、ファイル名はありません。テープファイルは、テープ上の位置で指定します。テープファイルへの書き込みには、テープデバイスを使用します。テープファイルを読み取るときは、テープファイルの書き込みに使用した圧縮形式と同じデバイスを指定する必要があります。

テープドライブ、メディアチェンジャー、およびテープドライブ操作を管理するための**ONTAP**コマンド

クラスタ内のテープドライブとメディアチェンジャに関する情報を表示するコマンド、テープドライブをオンラインまたはオフラインにするコマンド、テープドライブのカートリッジ位置を変更するコマンド、テープドライブのエイリアス名を設定およびクリアするコマンド、およびテープドライブをリセットするコマンドが用意されています。また、テープドライブの統計を表示およびリセットすることもできます。

状況	使用するコマンド
テープドライブをオンラインにする	`storage tape online`
テープドライブまたはメディアチェンジャのエイリアス名を消去します	`storage tape alias clear`
テープドライブのテープのトレース処理を有効または無効にします	`storage tape trace`
テープドライブのカートリッジ位置を変更する	`storage tape position`

状況	使用するコマンド
テープドライブをリセットします。	`storage tape reset` このコマンドは、 advanced 権限レベルでのみ使用できます。
テープドライブまたはメディアチェンジャのエイリアス名を設定する	`storage tape alias set`
テープドライブをオフラインにする	`storage tape offline`
すべてのテープドライブとメディアチェンジャに関する情報を表示する	`storage tape show`
クラスタに接続されているテープドライブに関する情報を表示します	• `storage tape show-tape-drive` • `system node hardware tape drive show`
クラスタに接続されているメディアチェンジャに関する情報を表示します	`storage tape show-media-changer`
クラスタに接続されているテープドライブに関するエラー情報を表示します	`storage tape show-errors`
クラスタ内の各ノードに接続されており、 ONTAP で認定およびサポートされているすべてのテープドライブを表示します	`storage tape show-supported-status`
クラスタ内の各ノードに接続されているすべてのテープドライブとメディアチェンジャのエイリアスを表示します	`storage tape alias show`
テープドライブの統計値をゼロにリセットします	`storage stats tape zero tape_name` このコマンドはノードシェルで使用する必要があります。
ONTAP でサポートされているテープドライブを表示します	`storage show tape supported [-v]` このコマンドはノードシェルで使用する必要があります。オプションを使用すると、各テープドライブの詳細を表示できます `-v`。

状況	使用するコマンド
テープのパフォーマンスを把握し、使用パターンを確認するには、テープデバイスの統計を表示します	`storage stats tape tape_name` このコマンドはノードシェルで使用する必要があります。

関連情報

- "ストレージテープ"
- "ストレージテープショー"
- "ストレージテープサポートステータスの表示"
- "ストレージテープ テープドライブの表示"
- "ストレージテープエイリアスクリア"
- "ストレージテープエイリアスセット"
- "ストレージテープエイリアス表示"
- "ストレージテープトレース"

ONTAPテープ バックアップには非認定テープ ドライブを使用します。

未認定テープドライブが認定テープドライブをエミュレートできる場合は、そのドライブをストレージシステムで使用できます。その後、認定テープドライブとして扱われます。未認定テープドライブを使用するには、そのドライブが認定テープドライブをエミュレートするかどうかを最初に確認する必要があります。

タスクの内容

未認定テープドライブは、ストレージシステムに接続されているドライブですが、ONTAPではサポートまたは認識されません。

手順

1. コマンドを使用して、ストレージシステムに接続されている未認定テープドライブを表示します `storage tape show-supported-status`。

   次のコマンドは、ストレージシステムに接続されているテープドライブ、および各テープドライブのサポートおよび認定ステータスを表示します。未認定テープドライブも表示されます。 `tape_drive_vendor_name`は、ストレージシステムに接続されていますが、ONTAPでサポートされていない未認定テープドライブです。

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. 認定テープドライブをエミュレートします。

   "NetAppのダウンロード:テープデバイス構成ファイル"

関連情報

- 認定テープドライブとは
- "ストレージテープサポートステータスの表示"

ONTAPテープ バックアップ用のテープ ドライブまたはメディア チェンジャーにテープ エイリアスを割り当てます。

テープドライブまたはメディアチェンジャにテープエイリアスを割り当てると、デバイスを簡単に識別できるようになります。エイリアスは、バックアップデバイスの論理名と、テープドライブまたはメディアチェンジャに永続的に割り当てられた名前を対応させます。

手順

1. コマンドを使用して、テープドライブまたはメディアチェンジャにエイリアスを割り当てます `storage tape alias set`。

   の詳細については `storage tape alias set`、を"ONTAPコマンド リファレンス"参照してください。

   テープドライブに関するシリアル番号（SN）情報は、コマンドを使用して確認できます。テープライブラリについては、コマンドを使用して `system node hardware tape library show`確認できます `system node hardware tape drive show`。

   次のコマンドは、ノード cluster1-01 に接続されているシリアル番号 SN[123456]L4 のテープドライブにエイリアス名を設定します。

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

次のコマンドは、ノード cluster1-01 に接続されているシリアル番号 SN[65432] のメディアチェンジャにエイリアス名を設定します。

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

関連情報

- テープのエイリアス設定とは
- テープエイリアスの削除
- "ストレージテープエイリアスセット"

ONTAPテープ バックアップ用のテープ ドライブまたはメディア チェンジャーへのテープ エイリアスを削除します。

テープドライブまたはメディアチェンジャで永続的なエイリアスが不要になった場合は、コマンドを使用してエイリアスを削除できます `storage tape alias clear`。

手順

1. コマンドを使用して、テープドライブまたはメディアチェンジャからエイリアスを削除します `storage tape alias clear`。

   の詳細については `storage tape alias clear`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドでは、エイリアスのクリア処理の範囲をに指定して、すべてのテープドライブのエイリアスを削除し `tape`ます。

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

終了後

NDMPを使用してテープバックアップまたはリストア処理を実行する場合は、テープドライブまたはメディアチェンジャからエイリアスを削除したあとに、テープデバイスに引き続きアクセスするには、テープドライブまたはメディアチェンジャに新しいエイリアス名を割り当てる必要があります。

関連情報

- テープのエイリアス設定とは
- テープエイリアスの割り当て
- "ストレージテープエイリアスクリア"

ONTAPテープ予約を有効または無効にする

オプションを使用すると、ONTAPによるテープデバイスの予約の管理方法を制御できます `tape.reservations`。デフォルトでは、テープ予約機能は無効になっています。

タスクの内容

テープ予約オプションを有効にすると、テープドライブ、メディアチェンジャ、ブリッジ、またはライブラリが正常に動作しない場合に問題が発生することがあります。テープ・コマンドで、他のストレージ・システムがデバイスを使用していないにもかかわらず、デバイスが予約されていると報告される場合は、このオプションを無効にしてください。

手順

1. SCSI予約/リリースメカニズムまたはSCSI永続的予約機能を使用してテープ予約を無効にするには、クラスタシェルで次のコマンドを入力します。

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi`SCSI予約/リリースメカニズムを選択します。

   `persistent`SCSI永続的予約を選択します。

   `off`テープ予約を無効にします。

関連情報

テープ予約機能とは

テープライブラリの接続を確認するためのONTAPコマンド

ストレージシステムと、ストレージシステムに接続されているテープライブラリの構成との間の接続パスに関する情報を表示できます。この情報を使用して、テープライブラリ構成への接続パスを確認したり、接続パスに関連する問題のトラブルシューティングを行ったりできます。

テープライブラリに関する次の詳細情報を表示して、新しいテープライブラリを追加または作成したあと、またはテープライブラリへのシングルパスアクセスまたはマルチパスアクセスで障害が発生したパスをリストアしたあとに、テープライブラリの接続を確認できます。この情報は、パス関連のエラーのトラブルシューティング時や、テープライブラリへのアクセスに失敗した場合にも使用できます。

- テープライブラリの接続先のノード
- デバイスID
- NDMPパス
- テープライブラリ名
- ターゲットポートとイニシエータポートのID
- 各ターゲットポートまたはFCイニシエータポートのテープライブラリへのシングルパスアクセスまたはマルチパスアクセス
- パス関連のデータ整合性の詳細（「パスエラー」や「パス品質」など）

- LUNグループとLUN数

状況	使用するコマンド
クラスタ内のテープライブラリに関する情報を表示する	`system node hardware tape library show`
テープライブラリのパス情報を表示する	`storage tape library path show`
各イニシエータポートのテープライブラリのパス情報を表示する	`storage tape library path show-by-initiator`
ストレージテープライブラリとクラスタ間の接続情報を表示する	`storage tape library config show`

関連情報

- "ストレージテープライブラリ構成の表示"
- "システムノードハードウェアテープライブラリの表示"
- "ストレージテープライブラリパスの表示"
- "ストレージテープライブラリパスのイニシエータ別表示"

テープ・ドライブについて

認定された**ONTAP**テープドライブについて

ストレージシステムで正常に動作することがテストで確認された認定テープドライブを使用する必要があります。テープのエイリアス設定に従い、テープ予約機能を有効にして、一度に1つのストレージシステムだけがテープドライブにアクセスするようにすることができます。

認定テープドライブとは、ストレージシステムで正常に動作することがテストによって確認されたテープドライブです。テープ構成ファイルを使用すると、既存の ONTAP リリース用にテープドライブを認定できます。

ONTAPテープ構成ファイルの形式

テープ構成ファイルの形式は、テープドライブのベンダーID、製品ID、圧縮形式の詳細などのフィールドで構成されています。このファイルには、テープドライブの自動ロード機能を有効にしたり、テープドライブのコマンドタイムアウト値を変更したりするためのオプションのフィールドも含まれています。

次の表に、テープ構成ファイルの形式を示します。

項目	サイズ	説明
vendor_id（文字列）。	最大8バイト	コマンドで表示されるベンダーID SCSI Inquiry。
product_id（文字列）。	最大16バイト	コマンドで報告される製品ID SCSI Inquiry。
id_match_size（数値）		識別されるテープドライブの検出に使用される製品IDのバイト数。Inquiryデータの製品IDの最初の文字から始まります。
vendor_pretty（文字列）。	最大16バイト	このパラメータを使用する場合は、コマンドによって返される文字列を指定します storage tape show -device-names。値を指定しないと、INQ_VENDOR_IDと表示されます。
product_pretty（文字列）。	最大16バイト	このパラメータを使用する場合は、コマンドによって返される文字列を指定します storage tape show -device-names。値を指定しないと、INQ_PRODUCT_IDと表示されます。

`vendor_pretty`フィールドと`product_pretty`フィールドはオプションですが、いずれかのフィールドに値が設定されている場合は、もう一方のフィールドにも値が設定されている必要があります。

次の表に、、 m、、 h`などのさまざまな圧縮形式の説明、密度コード、および圧縮アルゴリズムを示し `l`a`ます。

項目	サイズ	説明
`{l	m	h
a}_description=(string)`	最大24バイト	ノードシェルコマンドに対して出力される文字列。 `sysconfig -t`特定の密度設定の特性を示します。
`{l	m	h

項目	サイズ	説明
a}_density=(hex codes)`		l、m、h、またはaの目的の密度コードに対応するSCSIモードページブロック記述子で設定される密度コード。
`{l	m	h
a}_algorithm=(hex codes)`		密度コードと目的の密度特性に対応する、SCSI圧縮モードページで設定する圧縮アルゴリズム。

次の表に、テープ構成ファイルで使用できるオプションのフィールドを示します。

フィールド	説明
`autoload=(Boolean yes/no)`	テープドライブに自動ロード機能がある場合は、このフィールドがに設定され `yes` `ます。つまり、テープカートリッジを挿入すると、（`start/stop unit`）コマンドを実行しなくても、テープドライブの準備が整います。 `SCSI load` `このフィールドのデフォルトはです `no。
`cmd_timeout_0x`	個々のタイムアウト値。このフィールドは、テープドライバでデフォルトとして使用されているタイムアウト値とは異なるタイムアウト値を指定する場合にのみ使用する必要があります。このサンプルファイルには、テープドライブで使用されるデフォルトのSCSIコマンドタイムアウト値が記載されています。タイムアウト値は、分（m）、秒（s）、またはミリ秒（ms）で指定できます。 このフィールドは変更しないでください。

テープ構成ファイルはNetAppサポートサイトからダウンロードして表示できます。

テープ構成ファイル形式の例

HP LTO5 Ultriumテープドライブのテープ構成ファイルの形式は次のとおりです。

```
vendor_id="HP"

product_id="Ultrium 5-SCSI"

id_match_size= 9

vendor_pretty="Hewlett-Packard"
```

product_pretty="LTO-5"

l_description="LTO-3（ro）/ 4 4 / 800GB "

l_density= 0x00

l_algorithm= 0x00

m_description="LTO-3（ro）/ 4 8 / 1600GB CMP "

m_density= 0x00

m_algorithm= 0x01

h_description="LTO-5 1600GB"

h_density= 0x58

h_algorithm= 0x00

a_description="LTO-5 3200GB CMP"

a_density= 0x58

a_algorithm= 0x01

autoload="はい"

関連情報

- "ネットアップのツール：テープデバイス構成ファイル"
- "ストレージテープショー"

ONTAPストレージシステムがテープドライブを動的に認定する方法

ストレージシステムは、テープドライブのベンダーIDと製品IDをテープ認定テーブルに格納されている情報と照合することで、テープドライブを動的に認定します。

ストレージシステムにテープドライブを接続すると、テープ検出時に取得したベンダーIDと製品IDと、内部テープ認定テーブル内の情報が照合されます。一致する情報が検出されると、そのテープドライブが認定ドライブとしてマークされ、ストレージシステムからそのテープドライブにアクセスできるようになります。一致する情報が見つからない場合、そのテープドライブは未認定のままになり、ストレージシステムからアクセスできません。

テープデバイスの概要

ONTAPテープデバイスについて学ぶ

テープデバイスは、テープドライブを表したものです。テープドライブの巻き戻し形式と圧縮機能の特定の組み合わせです。

テープデバイスは、巻き戻し形式と圧縮機能の組み合わせごとに作成されます。したがって、1つのテープドライブまたはテープライブラリに複数のテープデバイスを関連付けることができます。テープの移動、書き込み、または読み取りを行うには、テープデバイスを指定する必要があります。

ストレージシステムにテープドライブまたはテープライブラリを取り付けると、ONTAPによって、そのテープドライブまたはテープライブラリに関連付けられたテープデバイスが作成されます。

ONTAP は、テープドライブとテープライブラリを検出し、論理番号とテープデバイスを割り当てます。ONTAPは、ファイバチャネル、SAS、パラレルSCSIテープドライブとライブラリがインターフェイスポートに接続されている場合に検出します。ONTAPでは、インターフェイスが有効になると、これらのドライブが検出されます。

ONTAPテープデバイス名の形式

各テープデバイスには関連付けられた名前があり、定義された形式で表示されます。この形式には、デバイスのタイプ、巻き戻し形式、エイリアス、および圧縮形式に関する情報が含まれます。

テープデバイス名の形式は次のとおりです。

```
rewind_type st alias_number compression_type
```

`rewind_type`は、巻き戻し形式です。

次に、巻き戻しタイプのさまざまな値について説明します。

- * R *

  ONTAP は、テープファイルの書き込み終了後に、テープを巻き戻します。

- * nr *

  ONTAP は、テープファイルの書き込み終了後に、テープを巻き戻しません。同じテープに複数のテープファイルを書き込む場合は、この巻き戻し形式を使用する必要があります。

- * ur *

  アンロード/リロード巻き戻しタイプです。この巻き戻し形式を使用すると、テープファイルの最後に達した時点でテープライブラリによってテープがアンロードされ、次のテープがある場合はそのテープがロードされます。

  この巻き戻し形式は、次の場合にのみ使用する必要があります。

  - このデバイスに関連付けられているテープドライブが、テープライブラリに収容されているか、ライブラリモードのメディアチェンジャに収容されている場合
  - このデバイスに関連付けられているテープドライブがストレージシステムに接続されている場合
  - このテープドライブに対して定義されているライブラリテープシーケンス内に、実行中の処理に対応する十分な数のテープがある場合

ノーリワインドデバイスを使用してテープを記録する場合は、テープを読み取る前にテープを巻き戻す必要があります。

`st`は、テープドライブの標準的な指定です。

`alias_number`は、ONTAPがテープドライブに割り当てるエイリアスです。ONTAP ONTAP は、新しいテープドライブを検出すると、そのテープドライブにエイリアスを割り当てます。

`compression_type`は、テープ上のデータ密度と圧縮形式を表すドライブ固有のコードです。

次に、のさまざまな値について説明し `compression_type`ます。

- * a *

  最高密度の圧縮

- * H *

  高い圧縮率

- * M *

  中密度の圧縮

- *L *

  低密度の圧縮

例

`nrst0a`は、テープドライブ0上のノーリワインドデバイスで、最高の圧縮を使用していることを示しています。

テープデバイスのリストの例

次の例は、HP Ultrium 2-SCSIに関連付けられているテープデバイスを示しています。

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,         format is: HP (200GB)
nrst0l -  no rewind device,      format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,         format is: HP (200GB)
nrst0m -  no rewind device,      format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,         format is: HP (200GB)
nrst0h -  no rewind device,      format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,         format is: HP (400GB w/comp)
nrst0a -  no rewind device,      format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

上記の例で使用されている略語の意味は、次のとおりです。

- GB - ギガバイト。テープの容量を示します。

- w/comp - 圧縮あり。圧縮時のテープ容量を示します。

同時にサポートされる**ONTAP**テープデバイスの数

ONTAPは、ファイバチャネル、SCSI、SAS接続の任意の組み合わせで、各ストレージシステム（ノードあたり）につき、最大64個のテープドライブの同時接続、16個のメディアチェンジャ、および16個のブリッジまたはルータデバイスをサポートします。

テープドライブまたはメディアチェンジャは、物理または仮想テープライブラリ内のデバイス、またはスタンドアロンデバイスにすることができます。

ストレージシステムでは64個のテープドライブ接続を検出できますが、同時に実行できるバックアップセッションとリストアセッションの最大数は、バックアップエンジンのスケーラビリティ制限によって異なります。

関連情報

ダンプバックアップおよびリストアセッションのスケーラビリティ制限

テープのエイリアス設定

テープのエイリアス設定の概要

エイリアシングにより、デバイスの識別プロセスが簡素化されます。エイリアス設定では、テープまたはメディアチェンジャのPhysical Path Name（PPN；物理パス名）またはSerial Number（SN；シリアル番号）を、変更可能な永続的なエイリアス名にバインドします。

次の表に、テープのエイリアス設定を使用して、テープドライブ（またはテープライブラリやメディアチェンジャ）に常に単一のエイリアス名を関連付ける方法を示します。

シナリオ	エイリアスの再割り当て
システムのリブート時	テープドライブには、以前のエイリアスが自動的に再割り当てされます。
テープデバイスを別のポートに移動するタイミング	エイリアスは、新しいアドレスを指すように調整できます。
複数のシステムで特定のテープデバイスを使用する場合	ユーザは、エイリアスをすべてのシステムで同じに設定できます。

Data ONTAP 8 .1.xからData ONTAP 8 .2.xにアップグレードする場合、Data ONTAP 8 .2.xのテープエイリアス機能によって既存のテープエイリアス名が変更されます。このような場合は、バックアップアプリケーションでテープエイリアス名を更新しなければならないことがあります。

テープエイリアスを割り当てることで、バックアップデバイスの論理名（st0やmc1など）と、ポート、テープドライブ、またはメディアチェンジャに永続的に割り当てられた名前を関連付けることができます。

st0とst00は異なる論理名です。

論理名とシリアル番号は、デバイスへのアクセスにのみ使用されます。デバイスにアクセスすると、物理パス名を使用してすべてのエラーメッセージが返されます。

エイリアスに使用できる名前には、物理パス名とシリアル番号の2種類があります。

物理パス名について学ぶ

PPN は、 ONTAP がテープドライブおよびテープライブラリに割り当てる数値アドレスです。 PPN は、テープドライブおよびテープライブラリが、ストレージシステム上のどの SCSI-2 / 3 アダプタまたはスイッチ（特定の場所）に接続されているかに基づいて割り当てられます。PPN は、「エレクトリカル名」とも呼ばれます。

直接接続されたデバイスのPPNは、次の形式になります。 `host_adapter device_id_lun`

LUNの値は、テープやメディアチェンジャのLUNの値が0以外の場合にのみ表示されます。つまり、LUNの値が0の場合、 `lun`PPNの部分は表示されません。

たとえば、 PPN が 8.6 となっている場合、ホストアダプタ番号が 8 、デバイス ID が 6 、論理ユニット番号（ LUN ）が 0 であることを示します。

SAS テープデバイスも直接接続されたデバイスです。たとえば、 PPN が 5c.4 となっている場合、ストレージシステムでは、 SAS HBA がスロット 5 で接続されており、 SAS テープが SAS HBA のポート C に接続されており、デバイス ID が 4 であることを示します。

ファイバチャネルスイッチ接続デバイスのPPNは、次の形式になります。 `switch:port_id device_id_lun`

たとえば、 PPN が MY_SWITCH ： 5.3L2 となっている場合、スイッチ MY_SWITCH のポート 5 にテープドライブが接続されており、そのテープドライブのデバイス ID が 3 、 LUN が 2 であることを示します。

LUN はドライブで決定されます。ファイバチャネル、 SCSI テープドライブ / ライブラリ、およびディスクには PPN が使用されます。

テープドライブおよびライブラリの PPN が変更されるのは、スイッチ名を変更した場合、テープドライブまたはライブラリを移動したり再設定したりした場合のみです。リブート後も PPN は変更されません。たとえば、 MY_SWITCH ： 5.3L2 という名前のテープドライブを取り外して、デバイス ID および LUN が同じである新しいテープドライブをスイッチ MY_SWITCH のポート 5 に接続した場合、引き続き、 MY_SWITCH ： 5.3L2 という名前を使用して新しいテープドライブにアクセスできます。

シリアル番号について学ぶ

シリアル番号（ SN ）は、テープドライブやメディアチェンジャに割り当てられる一意の識別子です。ONTAP では、 WWN ではなく SN に基づいてエイリアスが生成されます。

SN はテープドライブやメディアチェンジャに割り当てられる一意の識別子なので、テープドライブやメディアチェンジャに接続するパスが複数あってもエイリアスは変わりません。これにより、ストレージシステムでは、テープライブラリの構成で同じテープドライブまたはメディアチェンジャを追跡できます。

テープドライブまたはメディアチェンジャの接続先のファイバチャネルスイッチの名前を変更しても、テープ

ドライブまたはメディアチェンジャの SN は変わりません。ただし、テープライブラリでは、既存のテープドライブを新しいものに交換すると、 ONTAP によって新しいエイリアスが生成されます。これは、テープドライブの SN が変わるためです。また、既存のテープドライブをテープライブラリ内の新しいスロットに移動したり、テープドライブのLUNを再マッピングしたりすると、ONTAPはそのテープドライブ用の新しいエイリアスを生成します。

新しく生成されたエイリアスを使用してバックアップアプリケーションを更新する必要があります。

テープデバイスのSNは、次の形式を使用します。 `SN[xxxxxxxxxx]L[X]`

`x`は英数字です。Lはテープデバイスの LUNです。xLUNが0の場合、文字列のLx部分は表示されません。

各 SN は最大 32 文字で構成されます。 SN の形式では大文字と小文字は区別されません。

ONTAPマルチパステープアクセスを構成する際の考慮事項

ストレージシステムからテープライブラリのテープドライブにアクセスするパスを 2 つ設定できます。いずれかのパスで障害が発生した場合、そのパスをすぐに修復しなくても、他のパスを使用してテープドライブにアクセスできます。これにより、テープ処理を再開できます。

ストレージシステムからのマルチパステープアクセスを設定する際には、次の点を考慮する必要があります。

- LUN マッピングをサポートするテープライブラリでは、 LUN グループへのマルチパスアクセスのために、各パスで対称になるように LUN マッピングを行う必要があります。

  テープドライブとメディアチェンジャは、テープライブラリ内の LUN グループ（同じイニシエータのパスセットを共有する LUN のセット）に割り当てられます。複数のすべてのパスにおけるバックアップおよびリストア処理で、 LUN グループのすべてのテープドライブが使用可能である必要があります。

- ストレージシステムからテープライブラリのテープドライブにアクセスするパスを最大 2 つ設定できます。
- マルチパステープアクセスでは負荷分散がサポートされます。デフォルトでは、ロードバランシングは無効になっています。

次の例では、ストレージシステムは、 2 つのイニシエータパス 0b および 0d を介して LUN グループ 0 にアクセスします。これらの両方のパスで、 LUN グループの LUN 番号、 0 、 LUN 数 5 は同じです。ストレージシステムは、 1 つのイニシエータパス 3D のみを使用して LUN グループ 1 にアクセスします。

```
STSW-3070-2_cluster::> storage tape library config show

Node                      LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
------------------------ ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5          IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2          IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

関連情報

- "ストレージテープライブラリ構成の表示"

ONTAPストレージシステムにテープドライブとライブラリを追加する方法を学びます

テープドライブとライブラリをストレージシステムに動的に追加できます（ストレージシステムをオフラインにする必要はありません）。

新しいメディアチェンジャを追加すると、ストレージシステムによって、追加したメディアチェンジャが検出されて構成に追加されます。メディアチェンジャがすでにエイリアス情報内に定義されている場合、新しい論理名は作成されません。定義されていない場合は、ストレージシステムによってそのメディアチェンジャのエイリアスが新しく作成されます。

テープライブラリの構成では、ターゲットポートの LUN 0 にテープドライブまたはメディアチェンジャを設定して、そのターゲットポート上のすべてのメディアチェンジャとテープドライブを ONTAP が検出できるようにする必要があります。

ONTAPテープ予約について学ぶ

テープドライブ、メディアチェンジャ、ブリッジ、テープライブラリは、複数のストレージシステムで共有できます。テープ予約機能を使用すると、すべてのテープドライブ、メディアチェンジャ、ブリッジ、およびテープライブラリに対してSCSI予約/リリースメカニズムまたはSCSI永続的予約機能のいずれかを有効にすることで、一度に1つのストレージシステムだけがデバイスにアクセスするようになります。

> スイッチが含まれているかどうかにかかわらず、ライブラリ内のデバイスを共有するすべてのシステムは、同じ予約方法を使用する必要があります。

デバイスを予約するためのSCSI予約/リリースメカニズムは、通常の状態では正常に機能します。ただし、インターフェイスエラーのリカバリ手順中に予約が失われることがあります。この場合、予約された所有者以外のイニシエータはデバイスにアクセスできます。

SCSI永続的予約で行われた予約は、ループリセットやターゲットリセットなどのエラーリカバリメカニズムの影響を受けません。ただし、すべてのデバイスでSCSI永続的予約が正しく実装されているわけではありません。

ストレージシステム間でのデータ転送

ndmpcopyを使用して**ONTAP**データを転送する

ノードシェルコマンドは `ndmpcopy`、NDMP v4をサポートするストレージシステム間でデータを転送します。フルデータ転送と増分データ転送の両方を実行できます。ボリューム、qtree、ディレクトリの全体または一部、または個 々 のファイルを転送できます。

タスクの内容

ONTAP 8.x以前のリリースでは、増分転送は最大2つのレベル（1つのフルバックアップと最大2つの増分バックアップ）に制限されます。

ONTAP 9 .0以降のリリースでは、増分転送は最大9レベル（1つのフルバックアップと最大9つの増分バックアップ）に制限されています。

は、ソースストレージシステムとデスティネーションストレージシステム、またはデータ転送のソースでもデスティネーションでもないストレージシステムのノードシェルコマンドラインで実行できます `ndmpcopy`。また、データ転送のソースとデスティネーションの両方になっている単一のストレージシステムでを実行することもできます `ndmpcopy`。

コマンドでは、ソースストレージシステムとデスティネーションストレージシステムのIPv4アドレスまたはIPv6アドレスを使用できます `ndmpcopy`。パスの形式はです `/vserver_name/volume_name \[path\]`。

手順

1. ソースストレージシステムとデスティネーションストレージシステムでNDMPサービスを有効にします。

ソースまたはデスティネーションでデータ転送を実行するモード	使用するコマンド
SVMを対象としたNDMPモード	`vserver services ndmp on` 管理SVMにおけるNDMP認証の場合、ユーザアカウントはで、ユーザ `admin`ロールは `admin`またはです `backup`。データSVMでは、ユーザアカウントはで、ユーザロールは `vsadmin`または `vsadmin-backup`です `vsadmin`。
ノードを対象としたNDMPモード	`system services ndmp on`

2. ノードシェルでコマンドを使用して、ストレージシステム内またはストレージシステム間でデータを転送し `ndmpcopy`ます。

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

DNS名はndmpcopyではサポートされません。ソースとデスティネーションのIPアドレスを指定する必要があります。送信元IPアドレスまたは宛先IPアドレスでは、ループバックアドレス（127.0.0.1）はサポートされません。

- `ndmpcopy`このコマンドは、制御接続のアドレスモードを次のように決定します。
  - 制御接続用のアドレスモードは、指定された IP アドレスに対応します。
  - これらのルールは、オプションと `-mcd`オプションを使用して上書きできます `-mcs`。
- ソースまたはデスティネーションが ONTAP システムの場合は、 NDMP モード（ノードを対象とした NDMP モードまたは SVM を対象とした NDMP モード）に応じて、ターゲットボリュームへのアクセスを許可する IP アドレスを使用します。
- `source_path`と `destination_path`は、ボリューム、qtree、ディレクトリ、またはファイルの詳細レベルまでの絶対パス名です。
- `-mcs`ソースストレージシステムへの制御接続で優先されるアドレス指定モードを指定します。

  `inet`IPv4アドレスモードを示し、IPv6アドレスモードを示します。 `inet6`

- `-mcd`デスティネーションストレージシステムへの制御接続で優先的に使用するアドレス指定モードを指定します。

  `inet`IPv4アドレスモードを示し、IPv6アドレスモードを示します。 `inet6`

- `-md`ソースストレージシステムとデスティネーションストレージシステム間のデータ転送で優先されるアドレス指定モードを指定します。

  `inet`IPv4アドレスモードを示し、IPv6アドレスモードを示します。 `inet6`

  コマンドでオプションを `ndmpcopy`使用しない場合、 `-md`データ接続のアドレス指定モードは次のように決定されます。

  - 制御接続用に指定されたいずれかのアドレスが IPv6 アドレスの場合、データ接続用のアドレスモードは IPv6 になります。
  - 制御接続用に指定された両方のアドレスがIPv4アドレスの場合、 `ndmpcopy`コマンドは最初にデータ接続に対してIPv6アドレスモードを試行します。

    これに失敗した場合は、IPv4アドレスモードを使用します。

    IPv6アドレスを指定する場合は角かっこで囲む必要があります。

    このコマンド例では(`source_path`、ソースパスからデスティネーションパスにデータを移行し(`destination_path`ます）。

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
次のコマンド例では、制御接続とデータ接続でIPv6アドレスモードを使用するように明示的に設定します。

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ndmpcopyコマンドのオプション

ノードシェルコマンドで使用できるオプションについて理解しておく必要があります `ndmpcopy`"データの転送"。

次の表に、使用可能なオプションを示します。

オプション	説明
-sa username：[password]	このオプションは、ソースストレージシステムに接続するための、ソース側の認証のユーザ名とパスワードを設定します。これは必須オプションです。 管理者権限がないユーザの場合は、そのユーザのシステムによって生成されたNDMP固有のパスワードを指定する必要があります。システムによって生成されたパスワードは、adminユーザとadmin以外のユーザの両方に必須です。
-da username：[password]	このオプションは、デスティネーションストレージシステムに接続するための、デスティネーション側の認証のユーザ名とパスワードを設定します。これは必須オプションです。
-st{md5	text}

オプション	説明
このオプションは、ソースストレージシステムに接続するときに使用する、ソース側の認証タイプを設定します。これは必須オプションであるため、オプションまたは `md5`オプションのいずれかを指定する必要があります `text。	-dt{md5
text}	このオプションは、デスティネーションストレージシステムに接続するときに使用する、デスティネーション側の認証タイプを設定します。
-l	このオプションは、転送に使用するダンプレベルを、指定したレベルの値に設定します。有効な値は、、 1、~ 9`です `0 0。はフル転送を、は 9`増分転送 `1`を指定します。デフォルトはです `0。
-d	このオプションを指定すると、ndmpcopyデバッグログメッセージの生成が有効になります。ndmpcopyデバッグログファイルはルートボリュームにあり`/mroot/etc/log`ます。ndmpcopyデバッグログファイルの名前は、の形式になり `ndmpcopy.yyyymmdd`ます。
-f	このオプションは、強制モードを有効にします。このモードでは、7-Modeボリュームのルートでディレクトリのシステムファイルを上書きでき`/etc`ます。
-h	このオプションを選択すると、ヘルプメッセージが出力されます。
-p	ソース側とデスティネーション側の認証用のパスワードを入力するよう求められます。このパスワードは、および`-da`オプションで指定したパスワードよりも優先され`-sa`ます。 このオプションは、対話型コンソールでコマンドを実行する場合にのみ使用できます。
-exclude	データ転送用に指定するパスから、指定されたファイルまたはディレクトリを除外します。ディレクトリ名またはファイル名（や **.txt**`など）をカンマで区切ったリストを値として指定できます `.pst。サポートされる除外パターンの最大数は32、サポートされる最大文字数は255です。

FlexVol用NDMP

ONTAP FlexVolボリュームのNDMPについて学ぶ

Network Data Management Protocol（NDMP；ネットワークデータ管理プロトコル）は、プライマリストレージデバイスとセカンダリストレージデバイス（ストレージシステムやテープライブラリなど）間のバックアップやリカバリなどのデータ転送を制御するための標準化されたプロトコルです。

ストレージシステム上で NDMP のサポートを有効にすると、バックアップまたはリカバリ操作に使用する NDMP 対応のネットワーク接続型バックアップアプリケーション（ Data Management Applications_or_DMA_ とも呼ばれる）、データサーバ、およびテープサーバとの通信をストレージシステムが実行できるようになります。すべてのネットワーク通信は、TCPIPまたはTCP/IPネットワークを介して行われます。NDMPは、テープドライブとメディアチェンジャの低レベルの制御も提供します。

ノードを対象としたNDMPモードとStorage Virtual Machine（SVM）を対象としたNDMPモードのどちらでもテープバックアップおよびリストア処理を実行できます。

NDMPを使用する際の考慮事項、環境変数のリスト、およびサポートされるNDMPテープバックアップトポロジを確認しておく必要があります。拡張DAR機能を有効または無効にすることもできます。ONTAPでストレージシステムへのNDMPアクセスの認証にサポートされている認証方式は、プレーンテキストとチャレンジの2つです。

関連情報

ONTAPでサポートされる環境変数

NDMPの動作モードについて

ONTAP NDMPの動作モードについて学ぶ

テープバックアップおよびリストア処理をノードレベルまたはStorage Virtual Machine（SVM）レベルで実行することができます。これらの処理をSVMレベルで正常に実行するには、SVMでNDMPサービスを有効にする必要があります。

Data ONTAP 8 .2からData ONTAP 8 .3にアップグレードした場合、8.2で使用していたNDMPの動作モードは、8.2から8.3へのアップグレード後も維持されます。

Data ONTAP 8 .2以降を使用して新しいクラスタをインストールする場合、デフォルトではSVMを対象としたNDMPモードになります。ノードを対象としたNDMPモードでテープバックアップおよびリストア処理を実行するには、ノードを対象としたNDMPモードを明示的に有効にする必要があります。

ノードスコープのONTAP NDMP モードについて学ぶ

ノードを対象としたNDMPモードでは、テープバックアップおよびリストア処理をノードレベルで実行できます。Data ONTAP 8 .2で使用されているNDMPの動作モードは、8.2から8.3へのアップグレード後も維持されます。

ノードを対象としたNDMPモードでは、ボリュームを所有するノードでテープバックアップおよびリストア処理を実行できます。これらの処理を実行するには、ボリュームまたはテープデバイスを所有するノードでホストされているLIFでNDMP制御接続を確立する必要があります。

このモードは廃止され、今後のメジャーリリースで削除される予定です。

SVM スコープのONTAP NDMP モードについて学ぶ

NDMPサービスがStorage Virtual Machine（SVM）で有効になっている場合、テープバックアップおよびリストア処理をStorage Virtual Machine（SVM）レベルで正常に実行できます。バックアップアプリケーションでCAB拡張がサポートされている場合は、クラスタのSVMの異なるノード間でホストされているすべてのボリュームをバックアップおよびリストアできます。

NDMP制御接続は、さまざまなLIFタイプで確立できます。SVMを対象としたNDMPモードでは、これらのLIFはデータSVMまたは管理SVMに属しています。LIFで接続を確立できるのは、このLIFを所有するSVMでNDMPサービスが有効になっている場合だけです。

データLIFはデータSVMに属しています。クラスタ間LIF、ノード管理LIF、およびクラスタ管理LIFは管理SVMに属しています。

SVMを対象としたNDMPモードでは、バックアップおよびリストア処理に使用できるボリュームとテープデバイスは、NDMP制御接続が確立されるLIFタイプとCAB拡張のステータスによって異なります。バックアップアプリケーションでCAB拡張がサポートされていて、ボリュームとテープデバイスが同じアフィニティを共有している場合は、3ウェイバックアップまたはリストア処理の代わりにローカルバックアップまたはリストア処理をバックアップアプリケーションで実行できます。

関連情報

ノードを対象としたNDMPモードの管理用コマンド

ONTAP NDMP サービスを使用する際の考慮事項

ストレージシステムでNDMPサービスを開始するときは、いくつかの考慮事項を考慮する必要があります。

- 接続されたテープドライブを使用すると、各ノードで最大16個のバックアップ/リストア、またはこの2つの組み合わせが同時にサポートされます。
- NDMPサービスでは、NDMPバックアップアプリケーションからの要求に応じてファイル履歴データを生成できます。

  バックアップアプリケーションでは、ファイル履歴を使用して、選択したデータサブセットをバックアップイメージから最適にリカバリできます。ファイル履歴の生成と処理は、ストレージシステムとバックアップアプリケーションの両方で時間がかかり、CPUに負荷がかかる場合があります。

  SMTapeでは、ファイル履歴はサポートされません。

  バックアップイメージ全体がリカバリされるディザスタリカバリ用にデータ保護が設定されている場合は、ファイル履歴の生成を無効にしてバックアップ時間を短縮できます。NDMPファイル履歴の生成を無効にできるかどうかについては、バックアップアプリケーションのマニュアルを参照してください。

- NDMPのファイアウォールポリシーは、すべてのLIFタイプでデフォルトで有効になっています。
- ノードを対象としたNDMPモードでFlexVol volumeをバックアップするには、バックアップアプリケーションを使用して、ボリュームを所有するノードでバックアップを開始する必要があります。

  ただし、ノードルートボリュームはバックアップできません。

- ファイアウォールポリシーで許可されている場合は、任意のLIFからNDMPバックアップを実行できます。

  データLIFを使用する場合は、フェイルオーバー用に設定されていないLIFを選択する必要があります。NDMP処理中にデータLIFがフェイルオーバーすると、NDMP処理は失敗するため、再度実行する必要があります。

- ノードを対象としたNDMPモードおよびStorage Virtual Machine（SVM）を対象としたNDMPモードでCAB拡張がサポートされていない場合、NDMPデータ接続ではNDMP制御接続と同じLIFを使用します。
- LIFの移行中は、実行中のバックアップおよびリストア処理が中断されます。

  LIFの移行後にバックアップ処理とリストア処理を開始する必要があります。

- NDMPバックアップパスの形式は、 `*/vserver_name/volume_name/path_name*`です。

  `*path_name*`はオプションで、ディレクトリ、ファイル、またはSnapshotのパスを指定します。

- ダンプエンジンを使用してSnapMirrorデスティネーションをテープにバックアップする場合は、ボリューム内のデータのみがバックアップされます。

  ただし、SMTapeを使用してSnapMirrorデスティネーションをテープにバックアップする場合は、メタデータもバックアップされます。SnapMirror関係および関連するメタデータはテープにバックアップされません。そのため、リストア時には、そのボリュームのデータのみがリストアされますが、関連するSnapMirror関係はリストアされません。

関連情報

Cluster Aware Backup拡張の機能

"システム管理"

環境変数

ONTAP NDMP でサポートされている環境変数について学習します

環境変数は、 NDMP 対応のバックアップアプリケーションとストレージシステムの間でバックアップまたはリストア処理に関する情報をやり取りするために使用されます。

たとえば、バックアップアプリケーションのバックアップをユーザが指定した場合、 `/vserver1/vol1/dir1`バックアップアプリケーションはFILESYSTEM環境変数をに設定し `/vserver1/vol1/dir1`ます。同様に、ユーザがバックアップをレベル1バックアップにするように指定した場合、バックアップアプリケーションはLEVEL環境変数を1に設定します。

環境変数の設定と確認は、通常、バックアップ管理者に対して透過的に行われます。つまり、バックアップアプリケーションによって環境変数が自動的に設定されます。

バックアップ管理者が環境変数を指定することはほとんどありませんが、環境変数の値をバックアップアプリケーションで設定した値から変更して、機能上またはパフォーマンス上の問題の特性を特定したり、対処したりすることができます。たとえば、管理者がファイル履歴の生成を一時的に無効にして、バックアップアプリケーションによるファイル履歴情報の処理がパフォーマンスの問題や機能上の問題の原因になっているかどうかを確認できます。

多くのバックアップアプリケーションには、環境変数を上書きまたは変更したり、追加の環境変数を指定したりする手段が用意されています。詳細については、バックアップアプリケーションのマニュアルを参照してください。

ONTAPでサポートされる環境変数

ONTAP は、関連付けられたデフォルト値を持つ環境変数をサポートしています。ただし、これらのデフォルト値は手動で変更できます。

バックアップアプリケーションによって設定された値を手動で変更すると、アプリケーションが想定外の動作をする可能性があります。これは、バックアップ アプリケーションの想定とは異なるバックアップまたはリストア処理が行われるためです。ただし、状況によっては、適切な変更によって問題の特定や回避に役立つ場合があります。

次の表に、動作がダンプとSMTapeで共通で、ダンプとSMTapeでのみサポートされる環境変数を示します。また、 ONTAP でサポートされる環境変数が使用された場合の動作の説明も記載されています。

ほとんどの場合、値を持つ変数 `Y`も受け入れ、 `N`受け入れ `T`ます `F`。

ダンプとSMTapeでサポートされる環境変数

環境変数	有効な値	デフォルト	説明
デバッグ	`Y`または `N`	N	デバッグ情報を出力するように指定します。
ファイルシステム	string	none	バックアップされるデータのルートのパス名を指定します。
NDMP_VERSION	return_only	none	NDMP_VERSION 変数は変更しないでください。NDMP_VERSION 変数はバックアップ処理によって作成され、 NDMP のバージョンを返します。 ONTAP は、内部使用のため、および情報としてバックアップアプリケーションに渡すために、バックアップ時に NDMP_VERSION 変数を設定します。NDMP セッションの NDMP バージョンは、この変数では設定されません。

環境変数	有効な値	デフォルト	説明
pathname_separator	`return_value`	`none`	パス名の区切り文字を指定します。 この文字は、バックアップ対象のファイルシステムによって異なります。ONTAP の場合、文字 “/” はこの変数に割り当てられます。NDMP サーバでは、この変数を設定してからテープバックアップ処理を開始します。
タイプ	`dump`または `smtape`	`dump`	テープバックアップおよびリストア処理の実行がサポートされているバックアップのタイプを指定します。
詳細	`Y`または `N`	`N`	テープバックアップまたはリストア処理の実行中のログメッセージの数を増やします。

ダンプ用にサポートされる環境変数

環境変数	有効な値	デフォルト	説明
acl_start	`return_only`	`none`	ACL_START 変数は、バックアップ処理によって作成され、直接アクセスリストアまたは再開可能 NDMP バックアップ処理で使用されるオフセット値を示します。 オフセット値は、ダンプファイル内で ACL データ（ Pass V ）が始まるバイトオフセットであり、バックアップ終了時に返されます。直接アクセスリストア処理でバックアップデータを正しくリストアするには、開始時に ACL_START 値がリストア処理に渡されなければなりません。NDMP 再開可能バックアップ処理では、 ACL_START 値を使用して、バックアップストリームで再開できない部分の開始位置をバックアップアプリケーションに伝えます。
BASE_DATE	`0` `-1`、、または `DUMP_DATE`値	`-1`	増分バックアップの開始日を指定します。 に設定する `-1` と、`BASE_DATE`インクリメンタル指定子は無効になります。レベル`0`バックアップでに設定すると `0`、増分バックアップが有効になります。最初のバックアップ後、前回の増分バックアップの DUMP_DATE 変数の値が BASE_DATE 変数に代入されます。 これらの変数は、 LEVEL または UPDATE に基づく増分バックアップに代わるものです。

環境変数	有効な値	デフォルト	説明
直販	`Y`または `N`	`N`	リストアの際に、テープ全体をスキャンするのではなく、ファイルデータがある場所まで直接早送りするように指定します。 直接アクセスリカバリを使用するには、バックアップアプリケーションが位置情報を提供する必要があります。この変数がに設定されている場合、`Y`バックアップアプリケーションはファイル名またはディレクトリ名と位置情報を指定します。
dmp_name	`string`	`none`	複数サブツリーバックアップの名前を指定します。 この変数は、複数サブツリーバックアップに必須です。
DUMP_DATE	`return_value`	`none`	この変数を直接変更することはありません。BASE_DATE変数が以外の値に設定されている場合、バックアップによって作成され`-1`ます。 DUMP_DATE 変数は、ダンプソフトウェアによって計算された 32 ビットの時刻値の前に 32 ビットのレベル値を付けることによって生成されます。レベルは、 BASE_DATE 変数に最後に渡されたレベル値から増分されます。作成された値は、次回の増分バックアップの BASE_DATE 値として使用されます。

環境変数	有効な値	デフォルト	説明
ENHANCED_DAR_ENABLED 環境	`Y`または `N`	`N`	拡張 DAR 機能が有効になっているかどうかを示します。拡張DAR機能は、ディレクトリDARおよびNTストリームを含むファイルのDARをサポートします。パフォーマンスが向上します。 リストア時に拡張 DAR 機能を使用できるのは、次の条件が満たされている場合のみです。 • ONTAP で拡張 DAR がサポートされている。 • バックアップ時にファイル履歴が有効である（ HIST=Y ）。 • この `ndmpd.offset_map.enable`オプションはに設定されてい `on`ます。 • リストア時にENHANCED_DAR_ENABLED変数がに設定されている `Y`。

環境変数	有効な値	デフォルト	説明
シヨカイ	`pattern_string`	`none`	データのバックアップ時に除外するファイルまたはディレクトリを指定します。 除外リストは、ファイル名またはディレクトリ名をカンマで区切ったリストです。ファイルまたはディレクトリの名前がリスト内の名前の 1 つに一致した場合、バックアップから除外されます。 除外リストで名前を指定する際に適用されるルールは次のとおりです。 • 正確なファイル名またはディレクトリ名を使用する必要があります。 • ワイルドカード文字であるアスタリスク（ * ）は、文字列の最初または最後の文字にする必要があります。 使用できるアスタリスクの数は文字列ごとに 2 つです。 • ファイル名またはディレクトリ名のカンマの前にバックスラッシュを付ける必要があります。 • 除外リストに含めることができる名前は 32 個までです。

環境変数	有効な値	デフォルト	説明
展開する	Y、 N、または E	N	バックアップデータセットのサブツリーをリストアするように指定します。 バックアップアプリケーションでは、抽出するサブツリーの名前を指定します。指定されたファイルが、内容がバックアップされたディレクトリに一致する場合、ディレクトリは再帰的に抽出されます。 DARを使用せずにリストア時にファイル、ディレクトリ、またはqtreeの名前を変更するには、EXTRACT環境変数をに設定する必要があります E。
extract_acl	Y`または `N	Y	リストア処理でバックアップファイルの ACL がリストアされるように指定します。 デフォルトでは、 DAR （ DIRECT=Y ）を除いて、データをリストアするときに ACL がリストアされます。

環境変数	有効な値	デフォルト	説明
[-force]	`Y`または `N`	`N`	デスティネーションボリュームで使用可能なボリュームスペースと inode をリストア処理で確認する必要があるかどうかを指定します。 この変数をに設定する `Y` と、デスティネーションパスで使用可能なボリュームスペースとinodeのチェックがリストア処理でスキップされます。 デスティネーションボリュームのボリュームスペースまたは inode が不足している場合は、デスティネーションボリュームで使用可能なボリュームスペースと inode で許容される量のデータがリストア処理によってリカバリされます。ボリュームスペースと inode を使用できない場合は、リストア処理が停止します。

環境変数	有効な値	デフォルト	説明
霧	`Y`または `N`	N	ファイル履歴情報をバックアップアプリケーションに送信するように指定します。 ほとんどの市販のバックアップアプリケーションでは、HIST変数がに設定されてい `Y`ます。バックアップ処理の速度を上げる場合や、ファイル履歴の収集に関する問題のトラブルシューティングを行う場合は、この変数をに設定します `N`。 バックアップアプリケーションでファイル履歴がサポートされていない場合は、HIST変数をに設定しないで`Y`ください。

環境変数	有効な値	デフォルト	説明
IGNORE_CTime	`Y`または `N`	`N`	前回の増分バックアップ以降に変更されたのがctime 値だけである場合は、ファイルを増分バックアップしないことを指定します。 ウィルススキャンソフトウェアなどの一部のアプリケーションは、ファイルやファイル属性が変更されていなくても、inode 内のファイルのctime 値を変更します。その結果、変更されていないファイルが増分バックアップによってバックアップされることがあります。この`IGNORE_CTIME`変数を指定する必要があるのは、ctime値が変更されたために増分バックアップに許容できない時間またはスペースが使用されている場合だけです。 この`NDMP dump`コマンドは、デフォルトでに `false`設定され`IGNORE_CTIME`ます。に設定する `true`と、次のデータが失われる可能性があります。 1. ボリュームレベルの増分でがtrueに設定されている`ndmpcopy`場合、`IGNO

環境変数	有効な値	デフォルト	説明
IGNORE_qtrees	`Y`または `N`	`N`	リストア処理でバックアップ qtree から qtree 情報をリストアしないことを指定します。
「レベル」	`0-31`	`0`	バックアップレベルを指定します。 レベル 0 では、データセット全体がコピーされます。0 より大きい値で指定された増分バックアップレベルでは、前回の増分バックアップ以降に新規作成または変更されたすべてのファイルがコピーされます。たとえば、レベル 1 では、レベル 0 バックアップ以降に新規または変更されたファイルがバックアップされ、レベル 2 ではレベル 1 バックアップ以降に新規または変更されたファイルがバックアップされます。
リスト	`Y`または `N`	`N`	データを実際にはリストアせずに、バックアップファイル名と inode 番号を一覧表示します。
リスト qtree	`Y`または `N`	`N`	データを実際にはリストアせずに、バックアップ qtree を一覧表示します。

は、`IGNORE_CTIME`ボリュームレベルまたは`ndmpcopy`でを`false`に設定する必要があります `NDMP dumps`。

環境変数	有効な値	デフォルト	説明
multi_subtree_names	`string`	`none`	バックアップが複数のサブツリーであることを指定します。 複数のサブツリーは、改行で区切られた null で終わるサブツリー名のリストの文字列で指定されます。サブツリーは、共通のルートディレクトリを基準とした相対パス名で指定されます。このパス名は、リストの最後の要素として指定する必要があります。 この変数を使用する場合は、 DMP_NAME 変数も使用する必要があります。
NDMP_Unicode_FH	`Y`または `N`	`N`	ファイルの NFS 名のほかに Unicode 名もファイル履歴情報に含めるように指定します。 このオプションは、ほとんどのバックアップアプリケーションでは使用されないため、バックアップアプリケーションがこれらの追加のファイル名を受け取るように設計されている場合以外は設定しないでください。HIST 変数も設定する必要があります。
no_ACLs	`Y`または `N`	`N`	データのバックアップ時に ACL をコピーしないように指定します。

環境変数	有効な値	デフォルト	説明
NON_QUOTA_TREE	`Y`または `N`	`N`	データのバックアップ時に qtree 内のファイルおよびディレクトリを無視するように指定します。 に設定する `Y` と、FILESYSTEM変数で指定されたデータセット内のqtree内の項目はバックアップされません。この変数は、 FILESYSTEM 変数でボリューム全体が指定された場合のみ有効になります。NON_QUOTA_TREE 変数は、レベル 0 バックアップでのみ機能し、MULTI_SUBTREE_NAMES 変数が指定された場合は機能しません。 NON_QUOTA_TREE を同時に設定した場合、バックアップから除外するように指定したファイルまたはディレクトリは除外されません `Y`。
NOWRITE	`Y`または `N`	`N`	リストア処理でデータをディスクに書き込まないように指定します。 この変数はデバッグに使用されます。

環境変数	有効な値	デフォルト	説明

再帰的	`Y`または `N`	`Y`	DAR リストア中にディレクトリエントリが拡張されるように指定します。
			
			DIRECTおよびENHANCED_DAR_ENABLED環境変数も有効（に設定）する必要があります `Y`。RECURSIVE変数が無効になっている（に設定されている）場合は `N`、ディレクトリの内容ではなく、元のソースパス内のすべてのディレクトリの権限とACLのみがテープからリストアされます。RECURSIVE変数がに設定されている場合、またはRECOVER_FULL_PATHS変数がに設定されて`Y`いる場合、 `N`リカバリパスは元のパスで終了する必要があります。
			
			RECURSIVE 変数が無効で、複数のリカバリパスがある場合には、すべてのリカバリパスを最長のリカバリパス内に含める必要があります。それ以外の場合は、エラーメッセージが表示されます。
			
			たとえば、すべてのリカバリパスがに含まれているため、次のリカバリパスは有効`foo/dir1/deepdir/myfile`です。
			
			• `/foo`
			`/foo/dir`
			`/foo/dir1/deepdi`

環境変数	有効な値	デフォルト	説明
RECOVER_FULL_paths	`Y`または `N`	`N`	フルリカバリパスの権限および ACL が、 DAR のあとでリストアされるように指定します。 DIRECTおよびENHANCED_DAR_ENABLEDも有効（に設定）する必要があります `Y` 。recover_full_pathsがに設定されている場合、 `Y` リカバリパスは元のパスで終了する必要があります。デスティネーションボリュームにすでにディレクトリが存在する場合は、権限および ACL はテープからリストアされません。
更新	`Y`または `N`	`Y`	レベルベースの増分バックアップを有効にするために、メタデータ情報を更新します。

SMTape 用にサポートされる環境変数

環境変数	有効な値	デフォルト	説明
BASE_DATE	DUMP_DATE	-1	増分バックアップの開始日を指定します。 `BASE_DATE`は、参照スナップショット識別子の文字列表現です。SMTapeでは、文字列を使用して`BASE_DATE`参照Snapshotを特定します。 `BASE_DATE`は、ベースラインバックアップには必要ありません。増分バックアップの場合は、前回のベースラインバックアップまたは増分バックアップの変数の値が`DUMP_DATE`変数に代入され`BASE_DATE`ます。 バックアップアプリケーションは、前回のSMTapeのベースラインバックアップまたは増分バックアップの値を割り当て`DUMP_DATE`ます。

環境変数	有効な値	デフォルト	説明
DUMP_DATE	`return_value`	`none`	SMTapeバックアップの終了時に、DUMP_DATEには、そのバックアップに使用されるSnapshotを識別する文字列識別子が含まれます。このスナップショットは、次回の増分バックアップの参照スナップショットとして使用できます。 結果の DUMP_DATE の値が、次回の増分バックアップの BASE_DATE 値として使用されます。
smtape _backup_set_ID	`string`	`none`	ベースラインバックアップに関連付けられた増分バックアップのシーケンスを識別します。 バックアップセット ID は、ベースラインバックアップで生成される 128 ビットの一意の ID です。バックアップアプリケーションは、増分バックアップ時にこのIDを変数に入力として割り当て`SMTAPE_BACKUP_SET_ID`ます。
smtape snapshot _name	ボリューム内の有効なSnapshot	`Invalid`	SMTAPE_SNAPSHOT_NAME変数をSnapshotに設定すると、そのSnapshotとその古いSnapshotがテープにバックアップされます。 増分バックアップの場合、この変数は増分スナップショットを指定します。BASE_DATE変数は、ベースラインSnapshotを指定します。

環境変数	有効な値	デフォルト	説明
smtape delete _snapshot	`Y`または `N`	`N`	SMTAPE_DELETE_SNAPSHOT変数がに設定されている場合は、バックアップ処理の完了後にSMTapeで自動的に作成されたSnapshotがSMTape `Y`によって削除されます。ただし、バックアップアプリケーションで作成されたSnapshotは削除されません。
smtape break _mirror	`Y`または `N`	`N`	SMTAPE_BREAK_MIRROR変数をに設定する `Y`と、リストアが成功すると、タイプがのボリュームが `DP`ボリュームに変更され `RW`ます。

一般的な**ONTAP NDMP** テープ バックアップ トポロジについて学習します。

NDMPは、バックアップアプリケーションと、データ（ファイルシステム）サービスとテープサービスを提供するストレージシステムまたは他のNDMPサーバとの間で、さまざまなトポロジおよび構成をサポートします。

ストレージシステムからローカルテープへ

最も単純な構成では、バックアップアプリケーションは、ストレージシステムのデータを、ストレージシステムに接続されたテープサブシステムにバックアップします。NDMP制御接続はネットワーク境界を越えて存在します。ストレージシステム内でデータサービスとテープサービスの間に存在するNDMPデータ接続を、NDMPローカル構成と呼びます。

ストレージシステムから別のストレージシステムに接続されているテープへ

バックアップアプリケーションは、ストレージシステムから、別のストレージシステムに接続されているテープライブラリ（1つ以上のテープドライブを備えたメディアチェンジャ）にデータをバックアップすることもできます。この場合、データサービスとテープサービスの間のNDMPデータ接続は、TCPまたはTCP / IPv6ネットワーク接続によって提供されます。これは、NDMP 3ウェイストレージシステムからストレージシステムへの構成と呼ばれます。

ストレージシステムからネットワーク接続テープライブラリ

NDMP対応のテープライブラリには、3ウェイ構成のバリエーションがあります。この場合、テープライブラリはTCP / IPネットワークに直接接続され、内部NDMPサーバを介してバックアップアプリケーションおよびストレージシステムと通信します。

ストレージシステムからデータサーバ、テープ、またはデータサーバからストレージシステムからテープ

NDMPでは、ストレージシステムからデータサーバ、およびデータサーバからストレージシステムへの3ウェイ構成もサポートされていますが、これらのバリエーションはあまり広くは使用されていません。ストレージシステムからサーバへの接続を使用すると、ストレージシステムのデータを、バックアップアプリケーションホストまたは別のデータサーバシステムに接続されたテープライブラリにバックアップできます。サーバからストレージシステムへの構成では、サーバのデータをストレージシステムに接続されたテープライブラリにバックアップできます。

ONTAPがサポートする**NDMP**認証方法

NDMP接続要求を許可する認証方式を指定できます。ONTAPでは、ストレージシステムへのNDMPアクセスを認証する方法として、プレーンテキストとチャレンジの2つがサポートされています。

ノードを対象としたNDMPモードでは、チャレンジとプレーンテキストの両方がデフォルトで有効になります。ただし、チャレンジを無効にすることはできません。プレーンテキストは有効または無効にすることができます。プレーンテキスト認証方式では、ログインパスワードはクリアテキストとして送信されます。

Storage Virtual Machine（SVM）を対象としたNDMPモードでは、デフォルトの認証方式はチャレンジです。ノードを対象としたNDMPモードとは異なり、このモードでは、プレーンテキスト認証方式とチャレンジ認証方式の両方を有効または無効にできます。

関連情報

ノードを対象としたNDMPモードでのユーザ認証

SVMを対象としたNDMPモードでのユーザ認証

ONTAPでサポートされる**NDMP**の拡張機能

NDMP v4 は、 NDMP v4 プロトコルの中核部分を変更することなく、 NDMP v4 プロトコルの機能拡張を可能にするメカニズムを備えています。ONTAP でサポートされる NDMP v4 の拡張機能を確認しておく必要があります。

ONTAP でサポートされる NDMP v4 の拡張機能は次のとおりです。

- クラスタ対応バックアップ（CAB）

  この拡張機能は、 SVM を対象とした NDMP モードでのみサポートされます。

- IPv6 のサポートのための Connection Address Extension （ CAE ）
- 拡張クラス 0x2050

  この拡張機能は、再開可能なバックアップ処理と Snapshot Management Extension をサポートします。

この `NDMP_SNAP_RECOVER`メッセージは'Snapshot Management Extensionsの一部であり'リカバリ・オペレーションを開始し'リカバリされたデータをローカル・スナップショットからローカル・ファイル・システムの場所に転送するために使用されますONTAP では、このメッセージをボリュームと通常のファイルのリカバリのみに使用できます。

この `NDMP_SNAP_DIR_LIST`メッセージを使用すると、ボリュームのSnapshotを参照できます。参照処理の実行中にノンストップオペレーションが行われた場合、バックアップアプリケーションで参照処理を再開する必要があります。

- NDMP 再開可能バックアップ拡張機能

  NDMP の Restartable Backup Extension （ RBE ）機能を使用すると、障害発生前のデータストリームの既知のチェックポイントからバックアップを再開できます。

ONTAP NDMP の拡張 **DAR** 機能について学ぶ

拡張DAR（Direct Access Recovery）機能は、ディレクトリDAR、ファイルのDAR、およびNTストリームに対して使用できます。デフォルトでは、拡張DAR機能が有効になっています。

拡張DAR機能を有効にすると、オフセットマップを作成してテープに書き込む必要があるため、バックアップのパフォーマンスに影響することがあります。ノードを対象としたNDMPモードとStorage Virtual Machine（SVM）を対象としたNDMPモードの両方で拡張DARを有効または無効にすることができます。

NDMPセッションの**ONTAP**スケーラビリティ制限

システムメモリ容量が異なるストレージシステムで同時に確立できる NDMP セッションの最大数に注意する必要があります。この最大数は、ストレージシステムのシステムメモリによって異なります。

次の表に、 NDMP サーバの制限を示します。「ダンプバックアップおよびリストアセッションの計算性の制限」に記載されている制限は、ダンプおよびリストアセッションの制限です。

ダンプバックアップおよびリストアセッションのスケーラビリティ制限

ストレージシステムのシステムメモリ	**NDMP** セッションの最大数
16GB未満	8
16GB以上24GB未満	20
24GB以上	36

コマンド（ノードシェルから利用可能）を使用して、ストレージシステムのシステムメモリを取得できます `sysconfig -a`。の詳細については `sysconfig -a`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP FlexGroupボリュームでのNDMPサポートについて学ぶ

ONTAP 9 .7以降では、FlexGroupボリュームでNDMPがサポートされます。

ONTAP 9 .7以降では、ndmpcopyコマンドでFlexVolとFlexGroupの間のデータ転送がサポートされています。

ONTAP 9 .7から以前のバージョンにリバートした場合、以前の転送の差分転送情報は保持されないため、リバート後にベースラインコピーを実行する必要があります。

8以降では、FlexGroupボリュームで次のONTAP 9機能がサポートされます。

- 拡張クラス0x2050のNDMP_SNAP_RECOVERメッセージは、FlexGroupボリューム内の個 々 のファイルのリカバリに使用できます。
- FlexGroupボリュームでは、NDMPのRestartable Backup Extension（RBE）がサポートされます。
- FlexGroupボリュームでは、環境変数EXCLUDEおよびMULTI_SUBTREE_NAMESがサポートされます。

ONTAP SnapLockボリュームを使用したNDMPについて学ぶ

規制対象データのコピーを複数作成すると、冗長なリカバリシナリオが実現します。また、NDMPダンプおよびリストアを使用することで、ソースファイルのWrite Once Read Many（WORM）特性をSnapLockボリュームに保持できます。

SnapLockボリューム内のファイルのWORM属性は、データのバックアップ、リストア、およびコピー時に保持されますが、WORM属性が適用されるのはSnapLockボリュームへのリストア時のみです。SnapLockのバックアップをSnapLock以外のボリュームにリストアした場合、WORM属性は維持されますが無視され、ONTAPでは適用されません。

FlexVolのノードを対象としたNDMPモードを管理します。

FlexVolボリュームのONTAPノード スコープ NDMP モードの管理について学習します。

NDMPオプションとコマンドを使用して、ノードレベルでNDMPを管理できます。NDMPオプションは、コマンドを使用して変更できます `options`。テープバックアップおよびリストア処理を実行するには、NDMP固有のクレデンシャルを使用してストレージシステムにアクセスする必要があります。

の詳細については `options`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPノードスコープ NDMP モードを管理するためのコマンド

コマンドを使用すると、NDMPをノードレベルで管理でき `system services ndmp`ます。これらのコマンドの一部は非推奨となっており、今後のメジャーリリースで削除される予定です。

次の NDMP コマンドは、 advanced 権限レベルでのみ使用できます。

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`

- `system services ndmp log start`
- `system services ndmp log stop`

状況	使用するコマンド
NDMPサービスを有効にする	`system services ndmp on*`
NDMPサービスを無効にする	`system services ndmp off*`
NDMP設定を表示する	`system services ndmp show*`
NDMPの設定を変更する	`system services ndmp modify*`
デフォルトの NDMP バージョンを表示する	`system services ndmp version*`
NDMPサービス設定を表示する	`system services ndmp service show`
NDMPサービス設定を変更する	`system services ndmp service modify`
すべての NDMP セッションを表示する	`system services ndmp status`
すべての NDMP セッションに関する詳細情報を表示する	`system services ndmp probe`
指定したNDMPセッションを終了する	`system services ndmp kill`
すべてのNDMPセッションを終了する	`system services ndmp kill-all`
NDMPパスワードの変更	`system services ndmp password*`
ノードを対象としたNDMPモードを有効にする	`system services ndmp node-scope-mode on*`
ノードを対象とした NDMP モードを無効にします	`system services ndmp node-scope-mode off*`
ノードを対象とした NDMP モードのステータスを表示する	`system services ndmp node-scope-mode status*`
すべての NDMP セッションを強制的に終了します	`system services ndmp service terminate`
NDMPサービスデーモンを開始する	`system services ndmp service start`
NDMP サービスデーモンを停止します	`system services ndmp service stop`

状況	使用するコマンド
指定したNDMPセッションのロギングを開始する	`system services ndmp log start*`
指定したNDMPセッションのロギングを停止する	`system services ndmp log stop*`

- これらのコマンドは廃止され、今後のメジャーリリースで削除される予定です。

の詳細については `system services ndmp`、を"ONTAPコマンド リファレンス"参照してください。

ノードを対象とした**NDMP**モードでのユーザ認証

ノードを対象としたNDMPモードでは、テープバックアップおよびリストア処理を実行するために、NDMP固有のクレデンシャルを使用してストレージシステムにアクセスする必要があります。

デフォルトのユーザ ID は「 root 」です。ノードでNDMPを使用する前に、NDMPユーザに関連付けられているデフォルトのNDMPパスワードを変更しておく必要があります。デフォルトのNDMPユーザIDを変更することもできます。

関連情報

ノードを対象としたNDMPモードの管理用コマンド

ノードを対象としたNDMPモードとは

FlexVolのSVMを対象とした**NDMP**モードを管理します。

FlexVolボリュームの**ONTAP SVM** スコープ **NDMP** モードの管理について学習します。

NDMPオプションとコマンドを使用すると、SVM単位でNDMPを管理できます。NDMPオプションは、コマンドを使用して変更できます `vserver services ndmp modify`。SVMを対象としたNDMPモードでは、ユーザ認証がロールベースアクセス制御メカニズムと統合されます。

コマンドを使用して、許可するプロトコルまたは許可しないプロトコルのリストにNDMPを追加できます `vserver modify`。デフォルトでは、NDMPは許可されるプロトコルのリストに含まれています。許可しないプロトコルのリストにNDMPが追加されると、NDMPセッションを確立できません。

オプションを使用すると、NDMPデータ接続を確立するLIFタイプを制御できます `-preferred-interface-role`。NDMPデータ接続の確立時に、このオプションで指定したLIFタイプに属するIPアドレスがNDMPによって選択されます。IPアドレスがこれらのどのLIFタイプにも属していない場合は、NDMPデータ接続を確立できません。の詳細については `vserver services ndmp modify`、を"ONTAPコマンド リファレンス"参照してください。

ONTAP SVM スコープの **NDMP** モードを管理するためのコマンド

コマンドを使用して、各Storage Virtual Machine（SVM、旧Vserver）上のNDMPを管理できます `vserver services ndmp`。

状況	使用するコマンド
NDMPサービスを有効にする	`vserver services ndmp on` クラスタ内のすべてのノードでNDMPサービスを常に有効にする必要があります。ノードでNDMPサービスを有効にするには、コマンドを使用し`system services ndmp on`ます。デフォルトでは、NDMPサービスはノードで常に有効になっています。
NDMPサービスを無効にする	`vserver services ndmp off`
NDMP設定を表示する	`vserver services ndmp show`
NDMPの設定を変更する	`vserver services ndmp modify`
デフォルトのNDMPバージョンを表示する	`vserver services ndmp version`
すべての NDMP セッションを表示する	`vserver services ndmp status`
すべての NDMP セッションに関する詳細情報を表示する	`vserver services ndmp probe`
指定したNDMPセッションを終了する	`vserver services ndmp kill`
すべてのNDMPセッションを終了する	`vserver services ndmp kill-all`
NDMPパスワードの生成	`vserver services ndmp generate-password`
NDMPの拡張機能のステータスを表示する	`vserver services ndmp extensions show` このコマンドは、advanced権限レベルで使用できます。
NDMPの拡張機能のステータスを変更（有効化または無効化）する	`vserver services ndmp extensions modify` このコマンドは、advanced権限レベルで使用できます。
指定したNDMPセッションのロギングを開始する	`vserver services ndmp log start` このコマンドは、advanced権限レベルで使用できます。

状況	使用するコマンド
指定したNDMPセッションのロギングを停止する	`vserver services ndmp log stop` このコマンドは、advanced権限レベルで使用できます。

の詳細については `vserver services ndmp`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

SVMを対象としたNDMPモードの管理用コマンド

Cluster Aware Backup拡張の機能

SVMを対象としたNDMPモードとは

"システム管理"

ONTAP NDMP の **Cluster Aware Backup** 拡張機能について学ぶ

Cluster Aware Backup（CAB）は、NDMP v4プロトコルの拡張機能です。この拡張機能を使用すると、NDMPサーバでボリュームを所有するノード上でデータ接続を確立できます。これにより、ボリュームとテープデバイスがクラスタ内の同じノードに配置されているかどうかもバックアップアプリケーションで確認できます。

ボリュームを所有するノードをNDMPサーバで識別し、そのノードでデータ接続を確立できるようにするには、バックアップアプリケーションでCAB拡張がサポートされている必要があります。CAB拡張では、バックアップアプリケーションが、データ接続を確立する前に、バックアップまたはリストアするボリュームをNDMPサーバに通知する必要があります。これにより、NDMPサーバはボリュームをホストするノードを特定し、データ接続を適切に確立できます。

バックアップアプリケーションでCAB拡張がサポートされている場合、NDMPサーバはボリュームとテープデバイスに関するアフィニティ情報を提供します。ボリュームとテープデバイスがクラスタ内の同じノードにある場合は、このアフィニティ情報を使用して、バックアップアプリケーションで3ウェイバックアップの代わりにローカルバックアップを実行できます。

さまざまな**LIF**タイプでのバックアップとリストアのための**ONTAP**ボリュームとテープデバイスの可用性

クラスタ内の任意のタイプのLIFでNDMP制御接続を確立するようにバックアップアプリケーションを設定できます。Storage Virtual Machine（SVM）を対象としたNDMPモードでは、これらのLIFタイプおよびCAB拡張のステータスに応じて、バックアップおよびリストア処理に使用できるボリュームとテープデバイスを決定できます。

次の表に、NDMP制御接続のLIFタイプおよびCAB拡張のステータスで使用できるボリュームとテープデバイスを示します。

CAB拡張がバックアップアプリケーションでサポートされていない場合に使用できるボリュームとテープデバイス

NDMP 制御接続の **LIF** タイプ	バックアップまたはリストアに使用できるボリューム	バックアップまたはリストアに使用できるテープデバイス
ノード管理LIF	ノードでホストされるすべてのボリューム	ノード管理LIFをホストするノードに接続されているテープデバイス
Data LIF	データLIFをホストするノードでホストされるSVMに属するボリュームのみ	なし
クラスタ管理LIF	クラスタ管理LIFをホストするノードでホストされるすべてのボリューム	なし
クラスタ間LIF	クラスタ間LIFをホストするノードでホストされるすべてのボリューム	クラスタ間LIFをホストするノードに接続されているテープデバイス

CAB拡張がバックアップアプリケーションでサポートされている場合に使用できるボリュームとテープデバイス

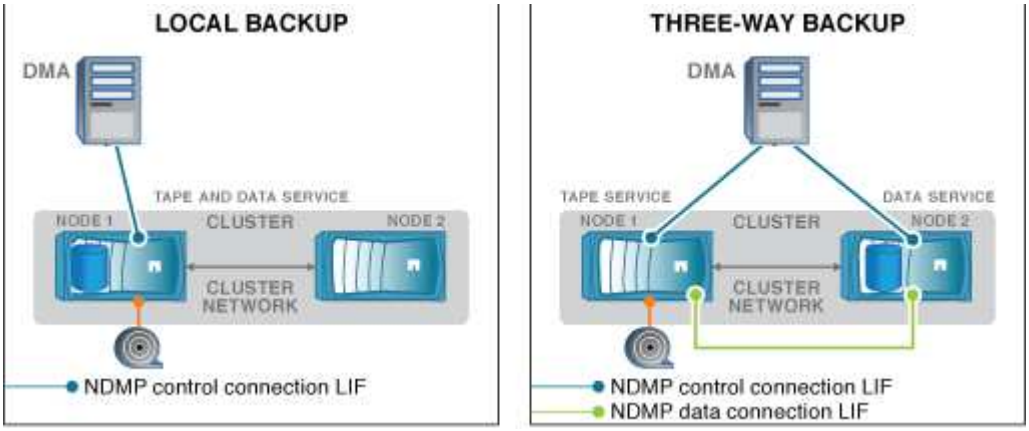
NDMP 制御接続の **LIF** タイプ	バックアップまたはリストアに使用できるボリューム	バックアップまたはリストアに使用できるテープデバイス
ノード管理LIF	ノードでホストされるすべてのボリューム	ノード管理LIFをホストするノードに接続されているテープデバイス
Data LIF	データLIFをホストするSVMに属するすべてのボリューム	なし
クラスタ管理LIF	クラスタ内のすべてのボリューム	クラスタ内のすべてのテープデバイス
クラスタ間LIF	クラスタ内のすべてのボリューム	クラスタ内のすべてのテープデバイス

ONTAP NDMPのアフィニティ情報について学ぶ

CAB対応のバックアップアプリケーションでは、ボリュームとテープデバイスに関する一意の場所情報がNDMPサーバから提供されます。ボリュームとテープデバイスが同じアフィニティを共有している場合、バックアップアプリケーションでは、このアフィニティ情報を使用して3ウェイバックアップの代わりにローカルバックアップを実行できます。

ノード管理LIF、クラスタ管理LIF、またはクラスタ間LIFでNDMP制御接続が確立されると、バックアップアプリケーションでは、アフィニティ情報を使用してボリュームとテープデバイスが同じノードに配置されているかどうかを判断し、ローカルまたは3ウェイのバックアップまたはリストア処理を実行できます。データLIFでNDMP制御接続が確立されると、バックアップアプリケーションは常に3ウェイバックアップを実行します。

ローカル**NDMP**バックアップと**3**ウェイ**NDMP**バックアップ



DMA（バックアップアプリケーション）は、ボリュームとテープデバイスに関するアフィニティ情報を使用して、クラスタ内のノード1にあるボリュームとテープデバイスでローカルNDMPバックアップを実行します。ボリュームがノード1からノード2に移動すると、ボリュームとテープデバイスに関するアフィニティ情報が変更されます。したがって、後続のバックアップでは、DMAは3ウェイNDMPバックアップ処理を実行します。これにより、ボリュームの移動先のノードに関係なく、ボリュームのバックアップポリシーが継続されます。

関連情報

Cluster Aware Backup拡張の機能

NDMPサーバーは**SVM**スコープモードで安全な**ONTAP**制御接続をサポートします

セキュアソケット（ SSL/TLS ）を通信メカニズムとして使用することで、 Data Management Application （ DMA ；データ管理アプリケーション）と NDMP サーバの間でセキュアな制御接続を確立できます。この SSL 通信は、サーバ証明書に基づいて行われます。NDMP サーバはポート 30000 （ IANA が「 ndmps 」サービス用に割り当てているポート）でリスンします。

このポートでクライアントから接続を確立すると、標準の SSL ハンドシェイクが開始され、サーバからクライアントに証明書が提示されます。クライアントが証明書を受け入れると、 SSL ハンドシェイクが完了します。このプロセスが完了すると、クライアントとサーバの間のすべての通信が暗号化されます。NDMP プロトコルのワークフローは、それまでとまったく同じです。セキュアな NDMP 接続で必要になるのは、サーバ側の証明書の認証のみです。DMA は、セキュアな NDMP サービスまたは標準の NDMP サービスのいずれかに接続して接続を確立できます。

デフォルトでは、Storage Virtual Machine（SVM）ではセキュアNDMPサービスは無効になっています。特定のSVMでセキュアなNDMPサービスを有効または無効にするには、コマンドを使用し `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]`ます。

NDMP ONTAPデータ接続タイプ

Storage Virtual Machine（SVM）を対象としたNDMPモードでは、サポートされるNDMPデータ接続タイプは、NDMP制御接続のLIFタイプおよびCAB拡張のステータスによって異なります。このNDMPデータ接続タイプは、ローカルまたは3ウェイNDMPバックアップまたはリストア処理を実行できるかどうかを示します。

TCPまたはTCP / IPv6ネットワーク経由で、3ウェイNDMPバックアップまたはリストア処理を実行できます。次の表に、NDMP制御接続のLIFタイプおよびCAB拡張のステータスに基づくNDMPデータ接続タイプを示します。

NDMPデータ接続タイプ（**CAB**拡張がバックアップアプリケーションでサポートされている場合）

NDMP 制御接続の **LIF** タイプ	**NDMP** データ接続タイプ
ノード管理LIF	ローカル、TCP、TCP / IPv6
Data LIF	TCP、TCP / IPv6
クラスタ管理LIF	ローカル、TCP、TCP / IPv6
クラスタ間LIF	ローカル、TCP、TCP / IPv6

NDMPデータ接続タイプ（**CAB**拡張がバックアップアプリケーションでサポートされていない場合）

NDMP 制御接続の **LIF** タイプ	**NDMP** データ接続タイプ
ノード管理LIF	ローカル、TCP、TCP / IPv6
Data LIF	TCP、TCP / IPv6
クラスタ管理LIF	TCP、TCP / IPv6
クラスタ間LIF	ローカル、TCP、TCP / IPv6

関連情報

Cluster Aware Backup拡張の機能

"ネットワーク管理"

SVM スコープの **NDMP** モードでの**ONTAP**ユーザー認証

Storage Virtual Machine（SVM）を対象としたNDMPモードでは、NDMPユーザ認証がロールベースアクセス制御と統合されます。SVM のコンテキストでは、 NDMP ユーザには「 vsadmin 」または「 vsadmin-backup 」のいずれかのロールが必要です。クラスタのコンテキストでは 'admin' または backup のいずれかのロールが NDMP ユーザーに割り当てられている必要があります

これらの事前定義されたロール以外に ' カスタム・ロールに関連づけられたユーザー・アカウントを NDMP 認証に使用することもできますただし ' カスタム・ロールのコマンド・ディレクトリには vserver services ndmp フォルダがあり ' フォルダのアクセス・レベルが none でない場合に限られますこのモードでは、特定のユーザアカウント用のNDMPパスワードを生成する必要があります。このパスワードは、ロールベースアクセス制御を使用して作成されます。adminロールまたはbackupロールのクラスタユーザは、ノード管理LIF、クラスタ管理LIF、またはクラスタ間LIFにアクセスできます。vsadmin-backupロールまたはvsadminロールの

ユーザは、そのSVMのデータLIFにのみアクセスできます。そのため、ユーザのロールによって、バックアップおよびリストア処理に使用できるボリュームとテープデバイスが異なります。

このモードでは、NISユーザとLDAPユーザのユーザ認証もサポートされます。そのため、NISユーザとLDAPユーザは、共通のユーザIDとパスワードを使用して複数のSVMにアクセスできます。ただし、NDMP認証ではActive Directoryユーザはサポートされません。

このモードでは、ユーザ・アカウントは SSH アプリケーションと「ユーザ・パスワード」認証方式に関連付けられている必要があります。

関連情報

SVMを対象としたNDMPモードの管理用コマンド

"システム管理"

ONTAP NDMPユーザー用の**NDMP**固有のパスワードを生成する

Storage Virtual Machine（SVM）を対象としたNDMPモードでは、特定のユーザID用のパスワードを生成する必要があります。NDMPユーザの実際のログインパスワードに基づいてパスワードが生成されます。実際のログインパスワードが変更された場合は、NDMP固有のパスワードを再度生成する必要があります。

手順

1. コマンドを使用し `vserver services ndmp generate-password`て、NDMP固有のパスワードを生成します。

   このパスワードは、パスワードの入力を必要とする現在または将来のNDMP処理で使用できます。

   Storage Virtual Machine（SVM、旧Vserver）のコンテキストから、そのSVMにのみ属しているユーザ用のNDMPパスワードを生成できます。

   次に、user1というユーザIDに対してNDMP固有のパスワードを生成する例を示します。

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. 通常のストレージシステムアカウントのパスワードを変更した場合は、この手順を繰り返して、新しいNDMP固有のパスワードを取得します。

ONTAP MetroCluster構成における災害復旧時にテープバックアップとリストア操作が受ける影響

MetroCluster構成では、ディザスタリカバリ時にテープバックアップおよびリストア処理を同時に実行できます。ディザスタリカバリ時にこれらの処理が受ける影響を理解しておく必要があります。

ディザスタリカバリ関係にあるSVMのボリュームでテープバックアップおよびリストア処理が実行される場合は、スイッチオーバーとスイッチバックのあとに増分テープバックアップおよびリストア処理を引き続き実行できます。

FlexVolのダンプエンジンについて

FlexVolボリューム用のONTAPダンプ エンジンについて学習します。

ダンプは、ONTAPが提供するSnapshotベースのバックアップおよびリカバリソリューションです。Snapshotからテープデバイスにファイルとディレクトリをバックアップし、バックアップしたデータをストレージシステムにリストアするのに役立ちます。

ダンプバックアップを使用して、ディレクトリ、ファイル、および関連するセキュリティ設定などのファイルシステムデータをテープデバイスにバックアップできます。バックアップ対象には、ボリューム全体、qtree全体、またはボリューム全体でもqtree全体でもないサブツリーを指定できます。

NDMP準拠のバックアップアプリケーションを使用して、ダンプバックアップまたはリストアを実行できます。

ダンプバックアップを実行するときに、バックアップに使用するSnapshotを指定できます。バックアップ用のSnapshotを指定しない場合は、ダンプエンジンによってバックアップ用のSnapshotが作成されます。バックアップ処理が完了すると、ダンプエンジンによってこのSnapshotが削除されます。

ダンプエンジンを使用して、テープへのレベル0バックアップ、増分バックアップ、または差分バックアップを実行できます。

> Data ONTAP 8 3より前のリリースにリバートした場合は、ベースラインバックアップ処理を実行してから増分バックアップ処理を実行する必要があります。

関連情報

"アップグレード、リバート、ダウングレード"

ONTAP NDMPでのダンプバックアップの仕組み

ダンプバックアップでは、事前定義されたプロセスを使用して、ファイルシステムデータがディスクからテープに書き込まれます。バックアップできるのは、ボリューム、qtree、またはボリューム全体でもqtree全体でもないサブツリーです。

次の表に、ダンプパスで指定されたオブジェクトについて、 ONTAP が実行するバックアッププロセスを示します。

段階	アクション
1	フルボリュームバックアップまたはフルqtreeバックアップ以外の場合、ONTAPはディレクトリをトラバースしてバックアップ対象のファイルを特定します。ボリューム全体またはqtree全体をバックアップする場合、ONTAPはこの段階を第2段階と組み合わせます。

段階	アクション
2	フルボリュームバックアップまたはフルqtreeバックアップの場合、ONTAPはボリュームまたはqtree内のバックアップ対象のディレクトリを特定します。
3	ONTAPはディレクトリをテープに書き込みます。
4	ONTAPはファイルをテープに書き込みます。
5	ONTAPはACL情報（該当する場合）をテープに書き込みます。

ダンプバックアップでは、バックアップにデータのSnapshotが使用されます。したがって、バックアップを開始する前にボリュームをオフラインにする必要はありません。

ダンプバックアップでは、作成した各Snapshotにという名前を付け `snapshot_for_backup.n`ます（ `n`は0から始まる整数）。ダンプバックアップでSnapshotが作成されるたびに、この整数が1ずつ増分されます。この整数は、ストレージシステムのリブート後に0にリセットされます。バックアップ処理が完了すると、ダンプエンジンによってこのSnapshotが削除されます。

ONTAPで複数のダンプバックアップを同時に実行すると、ダンプエンジンによって複数のSnapshotが作成されます。たとえば、ONTAPで2つのダンプバックアップを同時に実行すると、データのバックアップ元のボリューム内にとの `snapshot_for_backup.1`Snapshotが作成されます `snapshot_for_backup.0`。

Snapshotからバックアップする場合、ダンプエンジンでは追加のSnapshotは作成されません。

ダンプエンジンでバックアップされるデータの種類

ダンプエンジンを使用すると、データをテープにバックアップして災害やコントローラの停止から保護できます。ダンプエンジンでは、ファイル、ディレクトリ、 qtree 、ボリューム全体などのデータオブジェクトだけでなく、各ファイルに関するさまざまな種類の情報もバックアップできます。ダンプエンジンでバックアップできるデータの種類と考慮すべき制限を理解しておくと、ディザスタリカバリのアプローチを計画する際に役立ちます。

ダンプエンジンでは、ファイルのデータをバックアップするだけでなく、必要に応じて、各ファイルに関する次の情報もバックアップできます。

- UNIX GID 、所有者の UID 、およびファイルのアクセス権
- UNIX のアクセス時間、作成時間、および変更時間
- ファイルタイプ
- ファイルサイズ
- DOS 名、 DOS 属性、および作成時間
- 1 、 024 個の Access Control Entry （ ACE ；アクセス制御エントリ）を含む ACL
- qtree 情報
- ジャンクションパス

ジャンクションパスはシンボリックリンクとしてバックアップされます。

- LUN クローンおよび LUN クローン

  LUN オブジェクト全体をバックアップできますが、 LUN オブジェクト内の個別のファイルをバックアップすることはできません。同様に、 LUN オブジェクト全体をリストアできますが、 LUN オブジェクト内の個別のファイルをリストアすることはできません。

  ダンプエンジンでバックアップした LUN クローンは、独立した LUN になります。

- VM-aligned ファイル

  Data ONTAP 8.1.2 より前のリリースでは、 VM-aligned ファイルのバックアップはサポートされていません。

Snapshot でバックアップされた LUN クローンを Data ONTAP 7-Mode から ONTAP に移行した場合、一貫性のない LUN になります。ダンプエンジンでは、一貫性のない LUN はバックアップされません。

データをボリュームにリストアする場合は、リストア対象の LUN でクライアント I/O が制限されます。LUN に関するこの制限が解除されるのは、ダンプリストア処理が完了した場合のみです。同様に、 SnapMirror による単一ファイルまたは LUN のリストア処理中は、リストア対象のファイルと LUN でクライアント I/O が制限されます。この制限が解除されるのは、単一ファイル / LUN のリストア処理が完了した場合のみです。ダンプリストアまたは SnapMirror による単一ファイルまたは LUN のリストア処理を実行中のボリュームでダンプバックアップが実行される場合は、クライアント I/O が制限されているファイルまたは LUN がバックアップに含まれません。クライアント I/O の制限が解除されると、これらのファイルまたは LUN は後続のバックアップ処理に含まれます。

Data ONTAP 8.3 で実行されているテープにバックアップした LUN は、 8.3 以降のリリースにのみリストアできます。 8.3 より前のリリースにはリストアできません。以前のリリースに LUN をリストアする場合、その LUN はファイルとしてリストアされます。

SnapVault セカンダリボリュームまたは Volume SnapMirror デスティネーションをテープにバックアップする場合は、ボリュームのデータだけがバックアップされます。関連付けられているメタデータはバックアップされません。したがって、ボリュームをリストアしようとすると、そのボリュームのデータだけがリストアされます。Volume SnapMirror 関係に関する情報はバックアップで使用できないため、リストアされません。

Windows NT のアクセス権しかないファイルをダンプし、 UNIX 形式の qtree またはボリュームにリストアした場合、リストアされたファイルには、その qtree またはボリュームに対する UNIX のデフォルトのアクセス権が付与されます。

UNIX のアクセス権しかないファイルをダンプし、 NTFS 形式の qtree またはボリュームにリストアした場合、リストアされたファイルには、その qtree またはボリュームに対する Windows のデフォルトのアクセス権が付与されます。

それ以外の場合は、ダンプとリストア後もアクセス権は維持

VM-alignedファイルとオプションをバックアップできます `vm-align-sector`。VM-alignedファイルの詳細については、を参照してください"論理ストレージ管理"。

増分チェーンと**ONTAP NDMP**について学ぶ

増分チェーンとは、同じパスの一連の増分バックアップです。任意のレベルのバックア

ップをいつでも指定できるため、バックアップとリストアを効率的に実行するには、増分チェーンについて理解しておく必要があります。31レベルの増分バックアップ処理を実行できます。

漸増チェーンには次の2種類があります。

- 連続した増分チェーン。レベル0から始まり、後続のバックアップごとに1ずつ増加する一連の増分バックアップです。
- 連続しない増分チェーン。増分バックアップでは、レベルがスキップされるか、連続していないレベル（0、2、3、1、4、より一般的には0、1、1、0、1、0、1、2、1、2など）があります。

増分バックアップでは、よりレベルが低い最新のバックアップがベースとして使用されます。たとえば、バックアップレベル0、2、3、1、4のシーケンスでは、2つの増分チェーン（0、2、3および0、1、4）が提供されます。次の表に、増分バックアップのベースを示します。

バックアップ順序	増分レベル	漸増チェーン	ベース	バックアップされるファイル
1	0	両方	ストレージシステム上のファイル	バックアップパスのすべてのファイル
2	2	0、2、3	Level-0バックアップ	レベル0バックアップ以降に作成されたバックアップパスのファイル
3	3	0、2、3	レベル2バックアップ	レベル2バックアップ以降に作成されたバックアップパスのファイル
4	1	0、1、4	レベル0バックアップ（レベル1バックアップよりも低い最新レベルであるため）	レベル0バックアップ以降に作成されたバックアップパスのファイル（レベル2およびレベル3バックアップのファイルを含む）
5	4	0、1、4	レベル1バックアップ（レベル0、レベル2、またはレベル3のバックアップよりも下位レベルで最新であるため）	レベル1バックアップ以降に作成されたファイル

ブロッキングファクタと**ONTAP NDMP**について学ぶ

テープブロックは 1 、 024 バイトのデータから構成されています。テープバックアップ

またはリストア中には、各読み取り / 書き込み処理で転送するテープブロックの数を指定できます。この数を「ブロック化因数」と呼びます。

4~256 のブロック化因数を使用できます。バックアップのリストア先のシステムがバックアップ元と異なる場合は、バックアップで使用したブロック化因数がリストア先のシステムでサポートされている必要があります。たとえば、ブロック化因数を 128 としてバックアップをリストアする場合、リストア先のシステムでは、ブロック化因数として 128 をサポートしている必要があります。

NDMP バックアップでは、ブロック化因数は MOVER_RECORD_SIZE によって決定されます。ONTAP は、MOVER_RECORD_SIZE の最大値として、 256KB をサポートしています。

ONTAPダンプバックアップを再開するタイミング

テープ書き込みエラー、停電、ユーザによる誤った操作、ストレージシステム内部の不整合など、内外のさまざまなエラーが原因で、ダンプバックアップが完了しないことがあります。これらのいずれかの理由でバックアップに失敗した場合に、バックアップを再開できます。

ストレージシステム上のトラフィックが大量に発生する時間を避けるため、またはテープドライブなどのストレージシステム上の限られたリソース間の競合を回避するために、バックアップを中断して再開することができます。より緊急性の高いリストア（またはバックアップ）で同じテープドライブが必要な場合は、長いバックアップを中断してあとで再開できます。再開可能なバックアップはリブート後も維持されます。中止されたテープへのバックアップは、次の条件に該当する場合にのみ再開できます。

- 中止されたバックアップがフェーズ 4 である
- dumpコマンドでロックされた、関連付けられているすべてのSnapshotを使用できます。
- ファイル履歴が有効になっている必要があります。

このようなダンプ処理が中止され、再開可能な状態のままになると、関連するSnapshotがロックされます。これらのスナップショットは、バックアップコンテキストが削除された後に解放されます。バックアップコンテキストのリストを表示するには、コマンドを使用し `vserver services ndmp restartable backup show`ます。

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                       Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
                Has Offset Map?: true
                  Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

ONTAP NDMP でのダンプリストアの仕組み

ダンプリストアは、定義済みのプロセスに基づいてテープからディスクにファイルシステムのデータを書き込みます。

次の表に、ダンプリストアの動作を示します。

段階	アクション
1	ONTAP により、テープから抽出する必要のあるファイルがカタログ化されます。
2	ONTAP は、ディレクトリと空のファイルを作成します。

段階	アクション
3	ONTAP は、テープからファイルを読み取り、ディスクに書き込み、 ACL などのアクセス権を設定します。
4	指定したファイルがテープからすべて複製されるまで、 ONTAP はステージ 2 と 3 を繰り返します。

ダンプエンジンでリストアされるデータの種類

災害が発生したりコントローラが停止した場合、ダンプエンジンでは、単一ファイルからファイル属性やディレクトリ全体まで、バックアップしたすべてのデータをさまざまな方法でリカバリできます。ダンプエンジンでリストアできるデータの種類と使用するリカバリ方法を理解しておくと、ダウンタイムを最小限に抑えるのに役立ちます。

マッピングされたオンラインのLUNにデータをリストアできます。ただし、リストア処理が完了するまで、ホストアプリケーションはこのLUNにアクセスできません。リストア処理の完了後、LUNデータのホストキャッシュをフラッシュして、リストアされたデータとの一貫性を確保する必要があります。

ダンプエンジンでは次のデータをリカバリできます。

- ファイルおよびディレクトリの内容
- UNIX ファイルアクセス権
- ACL

  UNIX ファイルアクセス権だけを持つファイルを NTFS の qtree またはボリュームにリストアした場合、そのファイルには Windows NT ACL が含まれません。対象のファイルについて Windows NT ACL を作成しないかぎり、ストレージシステムではこのファイルに対して UNIX ファイルアクセス権だけを使用します。

  Data ONTAP 8.2 を実行するストレージシステムから、 Data ONTAP 8.1.x 以前を実行するストレージシステムに ACE の最大数が 1 、 024 より小さい ACL をリストアした場合、デフォルトの ACL がリストアされます。

- qtree 情報

  qtree 情報は、 qtree がボリュームのルートにリストアされる場合にのみ使用されます。などの下位のディレクトリにqtreeをリストアすると、qtree情報は使用されず、qtreeとしての機能は失われ`/vs1/vol1/subdir/lowerdir`ます。

- その他のすべてのファイルおよびディレクトリ属性
- Windows NT ストリーム
- LUN
  - LUN としての機能を維持するには、 LUN をボリュームレベルまたは qtree レベルでリストアする必要があります。

    ディレクトリにリストアすると、有効なメタデータが含まれないため、ファイルとしてリストアされます。

- 7-Mode LUN は、 ONTAP ボリュームで LUN としてリストアされます。

- 7-Mode ボリュームは、 ONTAP ボリュームにリストアできます。
- デスティネーションボリュームにリストアされた VM-aligned ファイルは、デスティネーションボリュームの VM-align のプロパティを継承します。
- リストア処理のデスティネーションボリュームに、強制ロックまたは助言ロックが設定されたファイルが含まれていることがあります。

  そのようなデスティネーションボリュームへのリストア処理を実行する場合、ダンプエンジンはそれらのロックを無視します。

ONTAP NDMPでデータをリストアする前に考慮すべき事項

バックアップされたデータを元のパスまたは別の場所にリストアできます。バックアップされたデータを別の場所にリストアする場合は、リストア先を準備しておく必要があります。

データを元のパスまたは別の場所にリストアするには、次の情報を入手しておく必要があります。また、次の要件を満たす必要があります。

- リストアのレベル
- データのリストア先のパス
- バックアップ時に使用されたブロック化因数
- 増分リストアを実行する場合は、すべてのテープがバックアップチェーンに含まれている必要があります
- リストア元のテープと互換性がある、使用可能なテープドライブ

データを別の場所にリストアするには、次の処理を実行する必要があります。

- ボリュームをリストアする場合は、新しいボリュームを作成する必要があります。
- qtree またはディレクトリをリストアする場合は、リストアするファイルと名前が同一と思われるファイルについて、名前を変更するか場所を移動します。

ONTAP 9では、qtree名でUnicode形式がサポートされます。以前のリリースの ONTAP では、この形式はサポートされていません。コマンドを使用するか、テープ内のバックアップイメージからリストアして、ONTAP 9内のUnicode名を持つqtreeを以前のリリースのONTAPにコピーする `ndmpcopy`と、そのqtreeはUnicode形式のqtreeではなく、通常のディレクトリとしてリストアされます。

リストアされたファイルの名前が既存のファイルと同じである場合、既存のファイルはリストアされたファイルで上書きされます。ただし、ディレクトリは上書きされません。

DARを使用せずにリストア時にファイル、ディレクトリ、またはqtreeの名前を変更するには、EXTRACT環境変数をに設定する必要があります `E`。

デスティネーションストレージシステムに必要なスペース

リストア先のストレージシステムには、リストアするデータのサイズに約 100MB を加えたサイズのスペース

が必要です。

> リストア処理の開始時には、デスティネーションボリュームで使用可能なボリュームスペースと inode が確認されます。FORCE環境変数をに設定する `Y`と、デスティネーションパスで使用可能なボリュームスペースとinodeのチェックがリストア処理でスキップされます。デスティネーションボリュームのボリュームスペースまたは inode が不足している場合は、デスティネーションボリュームで使用可能なボリュームスペースと inode で許容される量のデータがリストア処理によってリカバリされます。ボリュームスペースと inode を使用できなくなると、リストア処理が停止します。

ONTAPダンプ バックアップおよびリストア セッションのスケーラビリティ制限

システムメモリ容量が異なるストレージシステムで同時に実行できるダンプバックアップおよびリストアセッションの最大数に注意する必要があります。この最大数は、ストレージシステムのシステムメモリによって異なります。

次の表に、ダンプエンジンまたはリストアエンジンの制限を示します。NDMPセッションのスケーラビリティ制限に記載されている制限はNDMPサーバ用であり、エンジンの制限よりも高くなります。

ストレージシステムのシステムメモリ	ダンプバックアップおよびリストアセッションの総数
16GB未満	4
16GB以上24GB未満	16
24GB以上	32

> コマンドを使用し `ndmpcopy`てストレージシステム内のデータをコピーすると、ダンプバックアップ用とダンプリストア用の2つのNDMPセッションが確立されます。

コマンド（ノードシェルから利用可能）を使用して、ストレージシステムのシステムメモリを取得できます `sysconfig -a`。の詳細については `sysconfig -a`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

NDMPセッションのスケーラビリティ制限

ONTAP SVM名とコンテキスト**ID**を指定して、再起動可能なコンテキストを削除します。

コンテキストを再開せずにバックアップを開始する場合は、コンテキストを削除できます。

タスクの内容

コマンドでSVM名とコンテキストIDを指定すると、再開可能なコンテキストを削除できます `vserver services ndmp restartable-backup delete`。

手順

1. 再開可能なコンテキストを削除します。

`vserver services ndmp restartable-backup delete -vserver *vserver-name* -context-id *context_identifier*`です。

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

ONTAP SnapVaultセカンダリボリュームでのダンプの仕組み

SnapVaultセカンダリボリュームでミラーリングされたデータに対してテープバックアップ処理を実行できます。バックアップできるのは、SnapVaultセカンダリボリュームでテープにミラーリングされたデータのみで、SnapVault関係のメタデータはバックアップできません。

データ保護ミラー関係を解除する(`snapmirror break`場合）またはSnapMirrorを再同期する場合は、必ずベースラインバックアップを実行する必要があります。

関連情報

- "スナップミラーの破損"

ONTAPストレージフェイルオーバーおよび **ARL** 操作でのダンプの仕組み

ダンプバックアップまたはリストア処理を実行する前に、これらの処理とストレージフェイルオーバー（テイクオーバーとギブバック）処理またはアグリゲートの再配置（ARL）処理との連携について理解しておく必要があります。オプションは `-override-vetoes`、ストレージフェイルオーバーまたはARL処理時のダンプエンジンの動作を決定します。

ダンプバックアップまたはリストア処理が実行中で、オプションがに設定されている `false`**`場合は `-**

override-vetoes、ユーザが開始したストレージフェイルオーバーまたはARL処理が停止します。ただし、この `–override-vetoes`オプションをに設定する `true`と、ストレージフェイルオーバーまたはARL処理が続行され、ダンプバックアップまたはリストア処理が中止されます。ストレージフェイルオーバーまたはARL処理がストレージシステムによって自動的に開始されると、アクティブなダンプバックアップまたはリストア処理は常に中止されます。ストレージフェイルオーバーまたはARL処理が完了したあとも、ダンプバックアップおよびリストア処理を再開することはできません。

CAB拡張がサポートされている場合のダンプ処理

バックアップアプリケーションでCAB拡張がサポートされている場合は、ストレージフェイルオーバーまたはARL処理のあとにバックアップポリシーを再設定することなく、増分ダンプバックアップおよびリストア処理を引き続き実行できます。

CAB拡張がサポートされていない場合のダンプ処理

バックアップアプリケーションでCAB拡張がサポートされていない場合は、バックアップポリシーで設定されたLIFをデスティネーションアグリゲートをホストするノードに移行すれば、増分ダンプバックアップおよびリストア処理を引き続き実行できます。それ以外の場合は、ストレージフェイルオーバーおよびARL処理のあとに、ベースラインバックアップを実行してから増分バックアップ処理を実行する必要があります。

ストレージフェイルオーバー処理の場合は、バックアップポリシーで設定されているLIFをパートナーノードに移行する必要があります。

関連情報

"高可用性"

ONTAPボリューム移動でのダンプの仕組み

ストレージシステムで最終フェーズ（カットオーバー試行）が実行されるまでは、テープバックアップおよびリストア処理とボリューム移動を並行して実行できます。このフェーズのあとは、移動するボリュームで新しいテープバックアップおよびリストア処理を実行することはできません。ただし、現在の処理は完了するまで引き続き実行されます。

次の表に、ボリューム移動処理後のテープバックアップおよびリストア処理の動作を示します。

テープバックアップおよびリストア処理を実行する場合のモード	そしたら...。
Storage Virtual Machine（SVM）を対象としたNDMPモード（CAB拡張がバックアップアプリケーションでサポートされている場合）	バックアップポリシーを再設定することなく、読み取り/書き込みボリュームおよび読み取り専用ボリュームで増分テープバックアップおよびリストア処理を引き続き実行できます。

テープバックアップおよびリストア処理を実行する場合のモード	そしたら...。
SVMを対象としたNDMPモード（CAB拡張がバックアップアプリケーションでサポートされていない場合）	バックアップポリシーで設定されたLIFをデスティネーションアグリゲートをホストするノードに移行する場合は、読み取り/書き込みボリュームおよび読み取り専用ボリュームで増分テープバックアップおよびリストア処理を引き続き実行できます。それ以外の場合は、ボリューム移動後にベースラインバックアップを実行してから増分バックアップ処理を実行する必要があります。

ボリュームを移動する際に、デスティネーションノード上の別のSVMに属しているボリュームの名前が移動後のボリュームの名前と同じであると、移動後のボリュームの増分バックアップ処理を実行できません。

ONTAP FlexVol volumeがいっぱいになったときのダンプの動作

増分ダンプバックアップ処理を実行する前に、FlexVol volumeに十分な空きスペースがあることを確認する必要があります。

処理に失敗した場合は、サイズを大きくするかSnapshotを削除して、FlexVolの空きスペースを増やす必要があります。その後、増分バックアップ処理を再度実行します。

ONTAPボリュームのアクセスタイプが変更された場合のダンプの動作

SnapMirrorデスティネーションボリュームまたはSnapVaultセカンダリボリュームの状態が読み取り/書き込みから読み取り専用に、または読み取り専用から読み取り/書き込みに変わった場合は、ベースラインテープバックアップまたはリストア処理を実行する必要があります。

SnapMirrorデスティネーションボリュームとSnapVaultセカンダリボリュームは読み取り専用ボリュームです。このようなボリュームでテープバックアップおよびリストア処理を実行する場合は、ボリュームの状態が読み取り専用から読み取り/書き込み、または読み取り/書き込みから読み取り専用に変わるたびに、ベースラインバックアップまたはリストア処理を実行する必要があります。

ONTAP SnapMirrorの単一ファイルまたは**LUN**リストアでのダンプの仕組み

SnapMirrorテクノロジを使用して単一ファイルまたはLUNのリストア先となるボリュームでダンプバックアップまたはリストア処理を実行する前に、ダンプ処理と単一ファイルまたはLUNのリストア処理との連携について理解しておく必要があります。

SnapMirrorの単一ファイル/ LUNのリストア処理中は、リストア対象のファイルまたはLUNでクライアントI/Oが制限されます。単一ファイル/ LUNのリストア処理が終了すると、ファイルまたはLUNに対するI/Oの制限が解除されます。単一ファイルまたはLUNのリストア先のボリュームでダンプバックアップが実行される場合、クライアントI/Oが制限されているファイルまたはLUNはダンプバックアップに含まれません。後続のバックアップ処理では、I/Oの制限が解除されたあとに、このファイルまたはLUNがテープにバックアップされます。

ダンプリストアとSnapMirror単一ファイル/ LUNのリストア処理を同じボリュームで同時に実行することはで

きません。

ONTAP MetroCluster構成におけるダンプバックアップとリストア操作への影響

MetroCluster 構成でダンプバックアップおよびリストア処理を実行するには、スイッチオーバー処理またはスイッチバック処理の実行時にダンプ処理が受ける影響について理解しておく必要があります。

ダンプバックアップまたはリストア処理のあとにスイッチオーバーが行われる場合

クラスタ 1 とクラスタ 2 の 2 つのクラスタがあるとします。クラスタ 1 でダンプバックアップまたはリストア処理を実行しているときに、クラスタ 1 からクラスタ 2 へのスイッチオーバーが開始されると、次のような結果になります。

- このオプションの値がに設定されている `false`場合 `override-vetoes`は、スイッチオーバーが中止され、バックアップまたはリストア処理が続行されます。
- このオプションの値がに設定されている場合 `true`は、ダンプバックアップまたはリストア処理が中止され、スイッチオーバーが続行されます。

ダンプバックアップまたはリストア処理のあとにスイッチバックが行われる場合

クラスタ 1 からクラスタ 2 へのスイッチオーバーが実行され、クラスタ 2 でダンプバックアップまたはリストア処理が開始されます。クラスタ 2 にあるボリュームがダンプ処理によってバックアップまたはリストアされます。この時点で、クラスタ 2 からクラスタ 1 へのスイッチバックが開始されると、次のような結果になります。

- このオプションの値がの `false`場合は `override-vetoes`、スイッチバックがキャンセルされ、バックアップまたはリストア処理が続行されます。
- このオプションの値がの場合は `true`、バックアップまたはリストア処理が中止され、スイッチバックが続行されます。

スイッチオーバーまたはスイッチバックの実行中にダンプバックアップまたはリストア処理が開始された場合

クラスタ 1 からクラスタ 2 へのスイッチオーバーの実行中に、クラスタ 1 でダンプバックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチオーバーが続行されます。

クラスタ 2 からクラスタ 1 へのスイッチバックの実行中に、クラスタ 2 でダンプバックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチバックが続行されます。

FlexVolのSMTapeエンジンについて

FlexVolボリューム用のONTAP SMTapeエンジンについて学ぶ

SMTape は、データのブロックをテープにバックアップする、 ONTAP のディザスタリカバリ解決策です。SMTapeを使用すると、テープへのボリュームバックアップを実行できます。ただし、qtreeレベルまたはサブツリーレベルでバックアップを実行することはできません。SMTapeでは、ベースラインバックアップ、差分バックアップ、および増分バックアップがサポートされます。SMTape の場合、ライセンスは必要ありません。

NDMP 準拠のバックアップアプリケーションを使用して、 SMTape バックアップおよびリストア処理を実行できます。Storage Virtual Machine （ SVM ）を対象とした NDMP モードでのみバックアップおよびリストア処理を実行する SMTape を選択できます。

SMTape バックアップまたはリストアセッションを実行中のリバートプロセスはサポートされていません。セッションが終了するまで待機するか、 NDMP セッションを中止する必要があります。

SMTapeを使用すると、255個のSnapshotをバックアップできます。以降のベースラインバックアップ、増分バックアップ、または差分バックアップでは、古いバックアップSnapshotを削除する必要があります。

ベースラインリストアを実行する前に、データのリストア先のボリュームのタイプがであり、このボリュームが制限状態である必要があり `DP`ます。リストアが成功すると、このボリュームは自動的にオンラインになります。このボリュームでは、バックアップの実行順序に従って以降の増分リストアまたは差分リストアを実行できます。

SMTapeバックアップ中の**ONTAP**スナップショットの使用について学習します

SMTapeのベースラインバックアップおよび増分バックアップでのSnapshotの使用方法を理解しておく必要があります。また、SMTapeを使用してバックアップを実行する際に注意する必要がある考慮事項もあります。

ベースラインバックアップ

ベースラインバックアップの実行時に、テープにバックアップするSnapshotの名前を指定できます。Snapshotを指定しない場合は、ボリュームのアクセスタイプ（読み取り/書き込みまたは読み取り専用）に応じて、Snapshotが自動的に作成されるか、既存のSnapshotが使用されます。バックアップのSnapshotを指定すると、指定したSnapshotよりも古いすべてのSnapshotもテープにバックアップされます。

バックアップのSnapshotを指定しないと、次の処理が実行されます。

- 読み取り/書き込みボリュームの場合は、Snapshotが自動的に作成されます。

  新しく作成されたSnapshotと古いすべてのSnapshotがテープにバックアップされます。

- 読み取り専用ボリュームの場合は、最新のSnapshotを含むすべてのSnapshotがテープにバックアップされます。

  バックアップの開始後に作成された新しいSnapshotはバックアップされません。

増分バックアップ

SMTapeの増分バックアップ処理または差分バックアップ処理では、NDMP準拠のバックアップアプリケーションによってSnapshotが作成および管理されます。

増分バックアップ処理を実行するときは、必ずSnapshotを指定する必要があります。増分バックアップ処理を正常に実行するには、前回のバックアップ処理でバックアップされたSnapshot（ベースラインまたは増分）が、バックアップの実行元のボリュームに作成されている必要があります。バックアップされたSnapshotを確実に使用するには、バックアップポリシーの設定時にこのボリュームに割り当てられているSnapshotポリシーを考慮する必要があります。

SnapMirrorデスティネーションでの**SMTape**バックアップに関する考慮事項

- データ保護ミラー関係では、レプリケーション用のデスティネーションボリュームに一時的なSnapshotが作成されます。

  これらのSnapshotはSMTapeバックアップには使用しないでください。

- データ保護ミラー関係にあるデスティネーションボリュームでSMTapeバックアップ処理を実行しているときに、同じボリュームでSnapMirrorの更新が発生した場合は、SMTapeでバックアップされているSnapshotをソースボリュームから削除しないでください。

  バックアップ処理中、SMTapeはデスティネーションボリューム上のSnapshotをロックします。対応するSnapshotがソースボリューム上で削除されると、以降のSnapMirror更新処理は失敗します。

- 増分バックアップでは、これらのスナップショットを使用しないでください。

ONTAPテープ バックアップおよびリストア操作を最適化する **SMTape** 機能

Snapshotのバックアップ、増分バックアップと差分バックアップ、リストアしたボリュームでの重複排除機能と圧縮機能の維持、テープシーディングなどのSMTape機能は、テープバックアップおよびリストア処理を最適化するのに役立ちます。

SMTapeには次の機能があります。

- ディザスタリカバリ解決策を提供します
- 増分バックアップと差分バックアップをイネーブルにします
- Snapshotをバックアップします。
- 重複排除ボリュームのバックアップとリストアを有効にして、リストアしたボリュームで重複排除機能を維持します
- 圧縮ボリュームをバックアップして、リストアしたボリュームで圧縮機能を維持します
- テープシーディングを有効にします

SMTape では、 4~256KB の範囲で、 4KB の倍数単位でブロック化因数をサポートします。

データをリストアできるのは、 ONTAP の 2 つあとのメジャーリリースで作成したボリュームまでです。

SMTape バックアップおよびリストア セッションの**ONTAP**スケーラビリティ制限

NDMPまたはCLIを使用したSMTapeバックアップおよびリストア処理（テープシーディング）を実行する場合は、システムメモリ容量が異なるストレージシステムで同時に実行できるSMTapeバックアップおよびリストアセッションの最大数に注意する必要があります。この最大数は、ストレージシステムのシステムメモリによって異なります。

SMTapeバックアップおよびリストアセッションのスケーラビリティ制限は、NDMPセッションの制限やダンプセッションの制限とは異なります。

ストレージシステムのシステムメモリ	**SMTape** バックアップおよびリストアセッションの総数
16GB未満	6
16GB以上24GB未満	16
24GB以上	32

コマンド（ノードシェルから利用可能）を使用して、ストレージシステムのシステムメモリを取得できます `sysconfig -a`。の詳細については `sysconfig -a`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- NDMPセッションのスケーラビリティ制限
- ダンプバックアップおよびリストアセッションのスケーラビリティ制限

ONTAPテープ シーディングについて学ぶ

テープシーディングは、データ保護ミラー関係のデスティネーションFlexVol volumeの初期化に役立つSMTape機能です。

テープシーディングを使用すると、低帯域幅接続を介して、ソースシステムとデスティネーションシステムの間にデータ保護ミラー関係を確立できます。

ソースからデスティネーションへのスナップショットの増分ミラーリングは、低帯域幅接続で実行できます。ただし、低帯域幅接続では、ベースSnapshotの最初のミラーリングに時間がかかります。このような場合は、テープへのソースボリュームのSMTapeバックアップを実行し、そのテープを使用して最初のベースSnapshotをデスティネーションに転送できます。その後、低帯域幅接続を使用して、デスティネーションシステムへのSnapMirrorの差分更新を設定できます。

SMTape が**ONTAP**ストレージ フェイルオーバーおよび **ARL** 操作でどのように機能するか

SMTapeバックアップまたはリストア処理を実行する前に、これらの処理とストレージフェイルオーバー（テイクオーバーとギブバック）またはアグリゲートの再配置（ARL）処理との連携について理解しておく必要があります。オプションは `-override-vetoes`、ストレージフェイルオーバーまたはARL処理時のSMTapeエンジンの動作を決定します。

SMTapeバックアップまたはリストア処理が実行中で、オプションがに設定されている `false`場合 `-override-vetoes`は、ユーザが開始したストレージフェイルオーバーまたはARL処理が停止され、バックアップまたはリストア処理が完了します。バックアップアプリケーションでCAB拡張がサポートされている場合は、バックアップポリシーを再設定しなくても、増分SMTapeバックアップおよびリストア処理を引き続き実行できます。ただし、この `–override-vetoes`オプションをに設定する `true`と、ストレージフェイルオーバーまたはARL処理が続行され、SMTapeバックアップまたはリストア処理が中止されます。

関連情報

"ネットワーク管理"

"高可用性"

SMTapeと**ONTAP**ボリューム移動の仕組み

ストレージシステムが最後のカットオーバーフェーズを試行するまで、SMTapeバックアップ処理とボリューム移動処理を並行して実行できます。このフェーズのあとは、移動するボリュームで新しいSMTapeバックアップ処理を実行できません。ただし、現在の処理は完了するまで引き続き実行されます。

ボリューム移動処理では、ボリュームのカットオーバーフェーズを開始する前に、同じボリュームでアクティブなSMTapeバックアップ処理がないかどうかがチェックされます。アクティブなSMTapeバックアップ処理がある場合、ボリューム移動処理はカットオーバー保留状態になり、SMTapeバックアップ処理を完了できます。これらのバックアップ処理が完了したら、ボリューム移動処理を手動で再開する必要があります。

バックアップアプリケーションでCAB拡張がサポートされている場合は、バックアップポリシーを再設定することなく、読み取り/書き込みボリュームおよび読み取り専用ボリュームで増分テープバックアップおよびリストア処理を引き続き実行できます。

ベースラインリストア処理とボリューム移動処理を同時に実行することはできません。ただし、増分リストアはボリューム移動処理と並行して実行できます。この動作は、ボリューム移動処理におけるSMTapeバックアップ処理と同様です。

SMTape が**ONTAP**ボリュームの再ホスト操作でどのように機能するか

ボリュームでボリュームリホスト処理を実行中のときは、SMTape処理を開始できません。ボリュームリホスト処理に関係するボリュームでは、 SMTape セッションを開始しないでください。

ボリュームリホスト処理の実行中は、 SMTape バックアップまたはリストアが失敗します。SMTape バックアップまたはリストアの実行中は、ボリュームリホスト処理が失敗し、該当するエラーメッセージが表示されます。この状況では、 NDMP ベースと CLI ベースの両方のバックアップまたはリストア処理が環境ベースになります。

ADB 実行中に**ONTAP NDMP** バックアップ ポリシーが受ける影響

Automatic Data Balancer （ ADB ；自動データバランサ）が有効な場合、 ADB はアグリゲートの使用状況の統計を分析し、設定されている使用率の上限のしきい値を超えたアグリゲートを特定します。

バランサは、しきい値を超えたアグリゲートを特定すると、クラスタ内の別のノードにあるアグリゲートに移動できるボリュームを特定してそのボリュームの移動を試みます。この状況は、このボリュームに設定されているバックアップポリシーに影響します。 Data Management Application （ DMA ；データ管理アプリケーション）が CAB に対応していない場合、バックアップポリシーを再設定してベースラインバックアップ処理を実行する必要があるためです。

DMA が CAB に対応しており、特定のインターフェイスを使用してバックアップポリシーが設定されている場合は、 ADB に影響しません。

ONTAP MetroCluster構成におけるSMTapeバックアップおよびリストア操作への影響

MetroCluster 構成で SMTape バックアップおよびリストア処理を実行するには、スイッチオーバー処理またはスイッチバック処理の実行時に SMTape 処理が受ける影響について理解しておく必要があります。

SMTape バックアップまたはリストア処理のあとにスイッチオーバーが行われる場合

クラスタ 1 とクラスタ 2 の 2 つのクラスタがあるとします。クラスタ 1 で SMTape バックアップまたはリストア処理を実行しているときに、クラスタ 1 からクラスタ 2 へのスイッチオーバーが開始されると、次のような結果になります。

- このオプションの値がに設定されて `false`いる場合 `–override-vetoes`は、スイッチオーバープロセスが中止され、バックアップまたはリストア処理が続行されます。
- このオプションの値がに設定されている場合 `true`は、SMTapeバックアップまたはリストア処理が中止され、スイッチオーバープロセスが続行されます。

SMTape バックアップまたはリストア処理のあとにスイッチバックが行われる場合

クラスタ 1 からクラスタ 2 へのスイッチオーバーが実行され、クラスタ 2 で SMTape バックアップまたはリストア処理が開始されます。クラスタ 2 にあるボリュームが SMTape 処理によってバックアップまたはリストアされます。この時点で、クラスタ 2 からクラスタ 1 へのスイッチバックが開始されると、次のような結果になります。

- このオプションの値がに設定されて `false`いる場合は `-override-vetoes`、スイッチバックプロセスが中止され、バックアップまたはリストア処理が続行されます。
- このオプションの値がの場合は `true`、バックアップまたはリストア処理が中止され、スイッチバックプロセスが続行されます。

スイッチオーバーまたはスイッチバックの実行中に SMTape バックアップまたはリストア処理が開始された場合

クラスタ 1 からクラスタ 2 へのスイッチオーバープロセスの実行中に、クラスタ 1 で SMTape バックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチオーバーが続行されます。

クラスタ 2 からクラスタ 1 へのスイッチバックプロセスの実行中に、クラスタ 2 で SMTape バックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチバックが続行されます。

FlexVolのテープバックアップおよびリストア処理を監視する

FlexVolボリュームのONTAPテープ バックアップおよびリストア操作を監視します。

イベントログファイルを表示して、テープバックアップおよびリストア処理を監視できます。ONTAPは、発生したバックアップおよびリストアの重大なイベントとその時刻を、コントローラのディレクトリにある `/etc/log/`という名前のログファイルに自動的に記録し `backup`ます。デフォルトでは、イベントロギングはに設定されてい `on`ます。

イベントログファイルを表示する理由には、次のものがあります。

- 夜間バックアップが成功したかどうかを確認しています
- バックアップ処理に関する統計の収集
- 過去のイベントログファイルの情報を使用したバックアップおよびリストア処理に関する問題の診断

イベントログファイルは、週に 1 回ローテーションされます。 `/etc/log/backup`ファイルの名前がに変更され、 `/etc/log/backup.0`ファイルの名前がに `/etc/log/backup.0`変更され `/etc/log/backup.1`ます。ログファイルは最大6週間保存されます。したがって、最大7つのメッセージファイルと現在の `/etc/log/backup`ファイルを保持でき (/etc/log/backup.[0-5]`ます。

テープ バックアップおよびリストア操作の**ONTAP**イベント ログ ファイルにアクセスします

ディレクトリにあるテープバックアップおよびリストア処理用のイベントログファイルには、ノードシェルでコマンドを使用して `rdfile`アクセスできます `/etc/log/`。これらのイベントログファイルを表示して、テープバックアップおよびリストア処理を監視できます。

タスクの内容

Webサービスへのアクセスを許可するアクセス制御ロールや、アクセス方法を使用して設定されたユーザアカウント `http`などの追加の設定では `spi`、Webブラウザを使用してこれらのログファイルにアクセスすることもできます。

手順

1. ノードシェルにアクセスするには、次のコマンドを入力します。

   `node run -node node_name`

   `node_name` はノードの名前です。

2. テープバックアップおよびリストア処理用のイベントログファイルにアクセスするには、次のコマンドを入力します。

   `rdfile /etc/log/backup`

関連情報

"システム管理"

ダンプイベントログメッセージおよびリストアイベントログメッセージの形式とは

ONTAPダンプおよびリストアイベントログメッセージの形式

ダンプイベントおよびリストアイベントごとに、バックアップログファイルにメッセージが書き込まれます。

ダンプイベントログメッセージおよびリストアイベントログメッセージの形式は次のとおりです。

`type timestamp identifier event (event_info)`

次に、イベントログメッセージ形式のフィールドについて説明します。

- 各ログ・メッセージは、次の表に示すいずれかのタイプ・インジケータから始まります。

タイプ	説明
ログ	ロギングイベント
DMP	ダンプイベント
RST	リストアイベント

- `timestamp`イベントの日時が表示されます。
- ダンプイベントのフィールドには、 `identifier`ダンプパスとダンプの一意のIDが表示されます。 `identifier`リストアイベントのフィールドでは、リストア先のパス名のみが一意の識別子として使用されます。ロギング関連のイベントメッセージには、フィールドは含まれません `identifier`。

ONTAPログイベントについて学ぶ

ログで始まるメッセージのeventフィールドは、ロギングの開始または終了を指定します。

次の表に示すいずれかのイベントが含まれます。

イベント	説明
Start_Logging	ロギングの開始、または無効化後にロギングが再びオンになったことを示します。
Stop_Logging	ロギングがオフになっていることを示します。

ONTAPダンプイベントについて学ぶ

ダンプイベントのeventフィールドには、イベントタイプのあとにイベント固有の情報がかっこ内に表示されます。

次の表に、ダンプ処理で記録されるイベント、その説明、および関連するイベント情報を示します。

イベント	説明	イベント情報
開始	NDMPダンプが開始されました	ダンプレベルおよびダンプのタイプ
終了	ダンプが正常に完了しました	処理されたデータの量
中止	処理がキャンセルされました	処理されたデータの量
オプション	指定したオプションが表示されます	NDMPオプションを含む、すべてのオプションとその関連値

イベント	説明	イベント情報
tape_open	テープが読み取り/書き込み用に開いている	新しいテープデバイスの名前
tape_close	テープが読み取り/書き込みのために閉じられている	テープデバイスの名前
フェーズ-変更	ダンプが新しい処理フェーズに入っています	新しいフェーズの名前
エラー	ダンプで予期しないイベントが発生しました	エラーメッセージ
Snapshot	スナップショットが作成または検出された場合	Snapshotの名前と時刻
ベースダンプ	内部メタファイル内にベースダンプエントリが見つかりました	ベースダンプのレベルと時刻（増分ダンプの場合のみ）

ONTAP復元イベントについて学ぶ

リストアイベントのeventフィールドには、イベントタイプのあとにイベント固有の情報がかっこ内に表示されます。

次の表に、リストア処理に関して記録されるイベント、その説明、および関連するイベント情報を示します。

イベント	説明	イベント情報
開始	NDMPリストアが開始されました	リストアレベルとリストアタイプ
終了	リストアが正常に完了した	処理されたファイル数とデータ量
中止	処理がキャンセルされました	処理されたファイル数とデータ量
オプション	指定したオプションが表示されます	NDMPオプションを含む、すべてのオプションとその関連値
tape_open	テープが読み取り/書き込み用に開いている	新しいテープデバイスの名前
tape_close	テープが読み取り/書き込みのために閉じられている	テープデバイスの名前
フェーズ-変更	リストアは新しい処理フェーズに入っています	新しいフェーズの名前

イベント	説明	イベント情報
エラー	リストアで予期しないイベントが発生する	エラーメッセージ

ONTAPテープ バックアップおよびリストア操作のイベント ログの有効化または無効化

イベントロギングのオンとオフを切り替えることができます。

手順

1. イベントロギングを有効または無効にするには、クラスタシェルで次のコマンドを入力します。

   options -*option_name* backup.log.enable -*option-value* {on | off}

   `on`イベントロギングをオンにします。

   `off`イベントロギングをオフにします。

   イベントロギングはデフォルトでオンになっています。

FlexVolのテープバックアップおよびリストアに関するエラーメッセージ

バックアップおよびリストアに関するエラーメッセージ

リソース制限：使用可能なスレッドがありません

- * メッセージ *

  ```
  Resource limitation: no available thread
  ```

- * 原因 *

  アクティブなローカルテープI/Oスレッドの最大数が現在使用されています。最大16台のローカルテープドライブをアクティブにできます。

- * 是正措置 *

  一部のテープジョブが完了するのを待ってから、新しいバックアップジョブまたはリストアジョブを開始します。

テープ予約がプリエンプトされました

- * メッセージ *

  ```
  Tape reservation preempted
  ```

- * 原因 *

  テープドライブが別の処理で使用されているか、テープが途中で閉じられました。

- * 是正措置 *

  テープドライブが別の処理で使用されていないこと、およびDMAアプリケーションがジョブを中止していないことを確認してから再試行してください。

メディアを初期化できませんでした

- * メッセージ *

  ```
  Could not initialize media
  ```

- * 原因 *

  このエラーは、次のいずれかの理由で発生する可能性があります。

  - バックアップに使用するテープドライブが破損しています。
  - テープに完全なバックアップが含まれていないか、テープが破損しています。
  - アクティブなローカルテープI/Oスレッドの最大数が現在使用されています。

    最大16台のローカルテープドライブをアクティブにできます。

- * 是正措置 *
  - テープドライブが破損している場合は、有効なテープドライブを使用して処理を再試行します。
  - テープに完全なバックアップが含まれていないか、テープが破損している場合は、リストア処理を実行できません。
  - テープリソースを使用できない場合は、いくつかのバックアップジョブまたはリストアジョブが完了するのを待ってから、処理を再試行します。

実行中のダンプまたはリストアの最大許容数（セッション制限の最大数）

- * メッセージ *

  ```
  Maximum number of allowed dumps or restores (maximum session limit) in
  progress
  ```

- * 原因 *

  最大数のバックアップジョブまたはリストアジョブがすでに実行されています。

- * 是正措置 *

  現在実行中のジョブがいくつか完了してから、処理を再試行します。

テープ書き込み時のメディアエラー

- * メッセージ *

  ```
  Media error on tape write
  ```

- * 原因 *

  バックアップに使用するテープが破損しています。

- * 是正措置 *

  テープを交換し、バックアップジョブを再試行します。

テープ書き込みに失敗しました

- * メッセージ *

  ```
  Tape write failed
  ```

- * 原因 *

  バックアップに使用するテープが破損しています。

- * 是正措置 *

  テープを交換し、バックアップジョブを再試行します。

テープの書き込みに失敗しました-新しいテープでメディアエラーが発生しました

- * メッセージ *

  ```
  Tape write failed - new tape encountered media error
  ```

- * 原因 *

  バックアップに使用するテープが破損しています。

- * 是正措置 *

  テープを取り替えて、バックアップを再試行します。

tape write failed -新しいテープが壊れているか、書き込み保護されています

- * メッセージ *

  ```
  Tape write failed - new tape is broken or write protected
  ```

- * 原因 *

  バックアップに使用されているテープが破損しているか、書き込み保護されています。

- * 是正措置 *

  テープを取り替えて、バックアップを再試行します。

テープの書き込みに失敗しました-新しいテープがすでにメディアの最後にあります

- * メッセージ *

  ```
  Tape write failed - new tape is already at the end of media
  ```

- * 原因 *

  テープにバックアップを完了するための十分なスペースがありません。

- * 是正措置 *

  テープを取り替えて、バックアップを再試行します。

テープ書き込みエラー

- * メッセージ *

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- * 原因 *

  テープ容量が不足しているため、バックアップデータを格納できません。

- * 是正措置 *

  大容量のテープを使用して、バックアップジョブを再試行します。

テープ読み取り時のメディアエラー

- * メッセージ *

  ```
  Media error on tape read
  ```

- * 原因 *

  データのリストア元のテープが破損しており、完全なバックアップデータが含まれていない可能性があります。

- * 是正措置 *

  テープに完全なバックアップが含まれていることがわかっている場合は、リストア処理を再試行します。テープに完全なバックアップが含まれていなければ、リストア処理は実行できません。

テープ読み取りエラー

- * メッセージ *

  ```
  Tape read error
  ```

- * 原因 *

  テープドライブが破損しているか、テープに完全なバックアップが含まれていません。

- * 是正措置 *

  テープドライブが破損している場合は、別のテープドライブを使用します。テープに完全なバックアップが含まれていない場合は、データをリストアできません。

すでにテープの端にある

- * メッセージ *

  ```
  Already at the end of tape
  ```

- * 原因 *

  テープにデータが含まれていないか、テープを巻き戻す必要があります。

- * 是正措置 *

  テープにデータが含まれていない場合は、バックアップを含むテープを使用して、リストアジョブを再試行します。それ以外の場合は、テープを巻き戻して、リストアジョブを再試行します。

テープレコードサイズが小さすぎます。もっと大きいサイズを試してみてください。

- * メッセージ *

  ```
  Tape record size is too small. Try a larger size.
  ```

- * 原因 *

  バックアップ時に使用されたブロック化因数より小さいブロック化因数がリストア処理に指定されました。

- * 是正措置 *

  バックアップ時に指定したのと同じブロック化因数を使用します。

テープレコードのサイズは、**block_size2**ではなく**block_size1**にする必要があります。

- * メッセージ *

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- * 原因 *

  ローカルリストアに指定されたブロック化因数が正しくありません。

- * 是正措置 *

  をブロック化因数に指定してリストアジョブを再試行し `block_size1`ます。

テープレコードサイズは**4KB~256KB**の範囲で指定する必要があります。

- * メッセージ *

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- * 原因 *

  バックアップまたはリストア処理に指定されたブロック化因数が、許容範囲内に収まっていません。

- * 是正措置 *

  ブロック化因数は4~256KBの範囲で指定します。

NDMPのエラーメッセージ

ネットワーク通信エラー

- * メッセージ *

  ```
  Network communication error
  ```

- * 原因 *

  NDMP 3ウェイ接続でリモートテープとの通信に失敗しました。

- * 是正措置 *

  リモートムーバーへのネットワーク接続を確認します。

リードソケットからのメッセージ: **error_string**

- * メッセージ *

  ```
  Message from Read Socket: error_string
  ```

- * 原因 *

  NDMP 3ウェイ接続のリモートテープからのリストア通信でエラーが発生しました。

- * 是正措置 *

  リモートムーバーへのネットワーク接続を確認します。

書き込み**Dirnet**からのメッセージ: **ERROR_STRING**

- * メッセージ *

  ```
  Message from Write Dirnet: error_string
  ```

- * 原因 *

NDMP 3ウェイ接続でのリモートテープへのバックアップ通信でエラーが発生しました。

- * 是正措置 *

  リモートムーバーへのネットワーク接続を確認します。

リードソケット受信**EOF**

- * メッセージ *

  ```
  Read Socket received EOF
  ```

- * 原因 *

  NDMP 3ウェイ接続でリモートテープとの通信が試行され、ファイル終了マークに達しました。ブロックサイズが大きいバックアップイメージから3ウェイリストアを試行している可能性があります。

- * 是正措置 *

  正しいブロックサイズを指定し、リストア処理を再試行します。

ndmpdのバージョン番号が無効です**: VERSION_NUMBER** ``

- * メッセージ *

  ```
  ndmpd invalid version number: version_number
  ```

- * 原因 *

  指定したNDMPバージョンがストレージシステムでサポートされていません。

- * 是正措置 *

  NDMPバージョン4を指定します。

ndmpdセッション**session_ID**がアクティブでない

- * メッセージ *

  ```
  ndmpd session session_ID not active
  ```

- * 原因 *

  NDMPセッションが存在しない可能性があります。

- * 是正措置 *

  コマンドを使用し `ndmpd status`て、アクティブなNDMPセッションを表示します。

ボリューム**volume_name**の**vol ref**を取得できませんでした

- * メッセージ *

  ```
  Could not obtain vol ref for Volume vol_name
  ```

- * 原因 *

  ボリュームが他の処理で使用されている可能性があるため、ボリューム参照を取得できませんでした。

- * 是正措置 *

  あとで処理を再試行します。

データ接続タイプ**["NDMP4_addr_tcp"|"NDMP4_addr_tcp_ipv6"]**は**["ipv6"|"ipv4"]**制御接続でサポートされません

- * メッセージ *

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- * 原因 *

  ノードを対象としたNDMPモードでは、確立されたNDMPデータ接続のネットワークアドレスタイプ（IPv4またはIPv6）がNDMP制御接続と同じである必要があります。

- * 是正措置 *

  バックアップアプリケーションのベンダーにお問い合わせください。

Data Listen ： **CAB** データ接続の準備前提条件エラー

- * メッセージ *

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- * 原因 *

  バックアップアプリケーションがCAB拡張をNDMPサーバとネゴシエートし、NDMP_CAB_DATA_CONN_PREPAREメッセージとNDMP_DATA_LISTENメッセージの間で指定されたNDMPデータ接続アドレスタイプの不一致を検出すると、NDMPデータリスンが失敗します。

- * 是正措置 *

  バックアップアプリケーションのベンダーにお問い合わせください。

Data connect ： **CAB** データ接続準備前提条件エラー

- * メッセージ *

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- * 原因 *

  バックアップアプリケーションがCAB拡張をNDMPサーバとネゴシエート
  し、NDMP_CAB_DATA_CONN_PREPAREメッセージとNDMP_DATA_CONNECTメッセージの間で指定
  されたNDMPデータ接続アドレスタイプが一致しない場合、NDMPデータ接続は失敗します。

- * 是正措置 *

  バックアップアプリケーションのベンダーにお問い合わせください。

エラー：**show failed**：ユーザ「**<username>**」のパスワードを取得できません

- * メッセージ *

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- * 原因 *

  NDMPのユーザアカウント設定が不完全

- * 是正措置 *

  ユーザアカウントがSSHアクセス方式に関連付けられていること、および認証方式がユーザパスワードで
  あることを確認します。

ダンプに関するエラーメッセージ

デスティネーションボリュームは読み取り専用

- * メッセージ *

  ```
  Destination volume is read-only
  ```

- * 原因 *

  リストア処理の試行先のパスが読み取り専用です。

- * 是正措置 *

  別の場所にデータをリストアしてみてください。

デスティネーション**qtree**は読み取り専用

- * メッセージ *

  ```
  Destination qtree is read-only
  ```

- * 原因 *

  リストアの試行先のqtreeが読み取り専用です。

- * 是正措置 *

  別の場所にデータをリストアしてみてください。

ボリュームでダンプが一時的に無効になりました。再試行してください

- * メッセージ *

  ```
  Dumps temporarily disabled on volume, try again
  ```

- * 原因 *

  処理または `snapmirror resync`処理の一部であるSnapMirrorデスティネーションボリュームでNDMPダンプバックアップが試行されました `snapmirror break`。

- * 是正措置 *

  または `snapmirror resync`処理が終了するのを待って `snapmirror break`から、ダンプ処理を実行します。

  SnapMirrorデスティネーションボリュームの状態が読み取り/書き込みから読み取り専用、または読み取り専用から読み取り/書き込みに変わるたびに、ベースラインバックアップを実行する必要があります。

関連情報

- "スナップミラーの破損"
- "snapmirror resync"

NFSラベルが認識されない

- * メッセージ *

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- * 原因 *

  NFSv4.2が有効になっている場合、ONTAP 9 .9.1以降ではNFSセキュリティラベルがサポートされます。ただし、NFSセキュリティラベルは現在ダンプエンジンで認識されません。ファイル、ディレクトリ、またはダンプ形式の特殊ファイルでNFSセキュリティラベルが検出されると、ダンプは失敗します。

- * 是正措置 *

  NFSセキュリティラベルの付いたファイルやディレクトリがないことを確認します。

ファイルは作成されませんでした

- * メッセージ *

  ```
  No files were created
  ```

- * 原因 *

  拡張DAR機能を有効にせずにディレクトリDARが試行されました。

- * 是正措置 *

  拡張DAR機能を有効にしてから、DARを再試行します。

ファイル **<** ファイル名 **>** のリストアに失敗しました

- * メッセージ *

  ```
  Restore of the file file name failed
  ```

- * 原因 *

  デスティネーションボリューム上のLUNと同じファイル名のファイルのDirect Access Recovery（DAR）が実行されると、DARは失敗します。

- * 是正措置 *

  ファイルのDARを再試行します。

src inode <inode 番号 **> ...**一時的に切り捨てが失敗しました

- * メッセージ *

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  inode.
  ```

- * 原因 *

  ファイルのリストア時に、ファイルのinodeが削除されます。

- * 是正措置 *

  ボリューム上のリストア処理が完了するまで待機してから、そのボリュームを使用します。

ダンプに必要な**Snapshot**をロックできない

- * メッセージ *

  ```
  Unable to lock a snapshot needed by dump
  ```

- * 原因 *

  バックアップに指定したSnapshotを使用できません。

- * 是正措置 *

  別のSnapshotを使用してバックアップを再試行します。

使用可能なSnapshotのリストを表示するには、コマンドを使用し `snap list`ます。

の詳細については `snap list`、を"ONTAPコマンド リファレンス"参照してください。

ビットマップファイルが見つかりません

- * メッセージ *

  `Unable to locate bitmap files`

- * 原因 *

  バックアップ処理に必要なビットマップファイルが削除されている可能性があります。この場合、バックアップを再開できません。

- * 是正措置 *

  バックアップを再度実行します。

ボリュームが一時的な状態にある

- * メッセージ *

  `Volume is temporarily in a transitional state`

- * 原因 *

  バックアップ対象のボリュームが一時的にマウント解除された状態になっています。

- * 是正措置 *

  しばらく待ってから、もう一度バックアップを実行してください。

SMTapeエラーメッセージ

順序が正しくないチャンク

- * メッセージ *

  `Chunks out of order`

- * 原因 *

  バックアップテープが正しい順序でリストアされていません。

- * 是正措置 *

  リストア処理を再試行し、正しい順序でテープを装填します。

チャンク形式はサポートされていません

- * メッセージ *

  ```
  Chunk format not supported
  ```

- * 原因 *

  SMTapeにバックアップイメージが含まれていません。

- * 是正措置 *

  SMTapeにバックアップイメージが含まれていない場合は、SMTapeバックアップを含むテープを使用して処理を再試行します。

メモリの割り当てに失敗しました

- * メッセージ *

  ```
  Failed to allocate memory
  ```

- * 原因 *

  システムのメモリが不足しています。

- * 是正措置 *

  システムがあまりビジー状態でないときに、ジョブを再試行します。

データバッファを取得できませんでした

- * メッセージ *

  ```
  Failed to get data buffer
  ```

- * 原因 *

  ストレージシステムのバッファが不足しています。

- * 是正措置 *

  ストレージシステムの処理がいくつか完了するのを待ってから、ジョブを再試行してください。

Snapshotが見つかりませんでした

- * メッセージ *

  ```
  Failed to find snapshot
  ```

- * 原因 *

  バックアップに指定したSnapshotを使用できません。

- * 是正措置 *

  指定したSnapshotが使用可能かどうかを確認します。そうでない場合は、正しいスナップショットを使用して再試行してください。

Snapshotを作成できませんでした

- * メッセージ *

  ```
  Failed to create snapshot
  ```

- * 原因 *

  ボリュームにはすでに最大数のSnapshotが含まれています。

- * 是正措置 *

  いくつかのSnapshotを削除してから、バックアップ処理を再試行してください。

Snapshotをロックできませんでした

- * メッセージ *

  ```
  Failed to lock snapshot
  ```

- * 原因 *

  Snapshotは使用中か削除されています。

- * 是正措置 *

  Snapshotが別の処理で使用されている場合は、その処理が完了するのを待ってからバックアップを再試行します。Snapshotが削除されている場合は、バックアップを実行できません。

Snapshotを削除できませんでした

- * メッセージ *

  ```
  Failed to delete snapshot
  ```

- * 原因 *

  自動Snapshotは他の処理で使用されているため、削除できませんでした。

- * 是正措置 *

  Snapshotのステータスを確認するには、コマンドを使用し `snap`ます。スナップショットが不要な場合は、手動で削除します。

最新の**Snapshot**を取得できませんでした

- * メッセージ *

  ```
  Failed to get latest snapshot
  ```

- * 原因 *

  ボリュームがSnapMirrorによって初期化されているため、最新のSnapshotが存在しない可能性があります。

- * 是正措置 *

  初期化が完了してから再試行してください。

新しいテープをロードできませんでした

- * メッセージ *

  ```
  Failed to load new tape
  ```

- * 原因 *

  テープドライブまたはメディアでエラーが発生しました。

- * 是正措置 *

  テープを交換して処理を再試行してください。

テープを初期化できませんでした

- * メッセージ *

  ```
  Failed to initialize tape
  ```

- * 原因 *

  このエラーメッセージは、次のいずれかの理由で表示されることがあります。

  - SMTapeにバックアップイメージが含まれていません。
  - 指定したテープブロック化因数が正しくありません。
  - テープが破損しています。
  - リストア用の正しいテープが装填されていません。

- * 是正措置 *

  - SMTape にバックアップイメージが含まれていない場合は、 SMTape バックアップを含むテープを使用して処理を再試行します。
  - ブロック化因数が正しくない場合は、正しいブロック化因数を指定して処理を再試行します。
  - テープが破損している場合は、リストア処理を実行できません。

- 間違ったテープが装填されている場合は、正しいテープを使用して処理を再試行します。

リストアストリームを初期化できませんでした

- * メッセージ *

  ```
  Failed to initialize restore stream
  ```

- * 原因 *

  このエラーメッセージは、次のいずれかの理由で表示されることがあります。

  - SMTapeにバックアップイメージが含まれていません。
  - 指定したテープブロック化因数が正しくありません。
  - テープが破損しています。
  - リストア用の正しいテープが装填されていません。

- * 是正措置 *
  - SMTapeにバックアップイメージが含まれていない場合は、SMTapeバックアップを含むテープを使用して処理を再試行します。
  - ブロック化因数が正しくない場合は、正しいブロック化因数を指定して処理を再試行します。
  - テープが破損している場合は、リストア処理を実行できません。
  - 間違ったテープが装填されている場合は、正しいテープを使用して処理を再試行します。

バックアップイメージの読み取りに失敗しました

- * メッセージ *

  ```
  Failed to read backup image
  ```

- * 原因 *

  テープが破損しています。

- * 是正措置 *

  テープが破損している場合は、リストア処理を実行できません。

イメージヘッダーがないか破損しています

- * メッセージ *

  ```
  Image header missing or corrupted
  ```

- * 原因 *

  テープに有効なSMTapeバックアップが含まれていません。

- * 是正措置 *

有効なバックアップが含まれているテープを使用して再試行します。

内部アサーション

- * メッセージ *

  `Internal assertion`

- * 原因 *

  SMTapeの内部エラーがあります。

- * 是正措置 *

  エラーを報告し、テクニカルサポートにファイルを送信し `etc/log/backup`ます。

無効なバックアップイメージマジック番号

- * メッセージ *

  `Invalid backup image magic number`

- * 原因 *

  SMTapeにバックアップイメージが含まれていません。

- * 是正措置 *

  SMTapeにバックアップイメージが含まれていない場合は、SMTapeバックアップを含むテープを使用して処理を再試行します。

バックアップイメージのチェックサムが無効です

- * メッセージ *

  `Invalid backup image checksum`

- * 原因 *

  テープが破損しています。

- * 是正措置 *

  テープが破損している場合は、リストア処理を実行できません。

無効な入力テープです

- * メッセージ *

  `Invalid input tape`

- * 原因 *

  テープヘッダー内のバックアップイメージのシグネチャが無効です。テープのデータが破損しているか、テープに有効なバックアップイメージが含まれていません。

- * 是正措置 *

  有効なバックアップイメージを使用してリストアジョブを再試行します。

ボリュームパスが無効です

- * メッセージ *

  ```
  Invalid volume path
  ```

- * 原因 *

  バックアップ処理またはリストア処理に指定されたボリュームが見つかりません。

- * 是正措置 *

  有効なボリュームパスとボリューム名を指定してジョブを再試行します。

バックアップセット**ID**の不一致

- * メッセージ *

  ```
  Mismatch in backup set ID
  ```

- * 原因 *

  テープの変更中にロードされたテープが、バックアップセットに含まれていません。

- * 是正措置 *

  正しいテープを装填して、ジョブを再試行します。

バックアップのタイムスタンプが一致しません

- * メッセージ *

  ```
  Mismatch in backup time stamp
  ```

- * 原因 *

  テープの変更中にロードされたテープが、バックアップセットに含まれていません。

- * 是正措置 *

  コマンドを使用し `smtape restore -h`て、テープのヘッダー情報を確認します。

シャットダウンによりジョブが中止されました

- * メッセージ *

  `Job aborted due to shutdown`

- * 原因 *

  ストレージシステムをリブートしています。

- * 是正措置 *

  ストレージシステムのリブート後にジョブを再試行します。

Snapshotの自動削除が原因でジョブが中止されました

- * メッセージ *

  `Job aborted due to snapshot autodelete`

- * 原因 *

  ボリュームに十分なスペースがないため、Snapshotの自動削除が実行されています。

- * 是正措置 *

  ボリューム内のスペースを解放してから、ジョブを再試行してください。

テープは現在他の処理で使用されています

- * メッセージ *

  `Tape is currently in use by other operations`

- * 原因 *

  テープドライブは別のジョブで使用されています。

- * 是正措置 *

  現在アクティブなジョブが完了してから、バックアップを再試行します。

テープが故障しています

- * メッセージ *

  `Tapes out of order`

- * 原因 *

  リストア処理用のテープシーケンスの最初のテープに、イメージヘッダーがありません。

- * 是正措置 *

  イメージヘッダーを含むテープをロードし、ジョブを再試行します。

転送に失敗しました（**MetroCluster**処理が原因で中止されました）

- * メッセージ *

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- * 原因 *

  スイッチオーバーまたはスイッチバック処理が原因で、SMTape処理が中止されます。

- * 是正措置 *

  スイッチオーバー処理またはスイッチバック処理の終了後にSMTape処理を実行します。

Transfer failed (ARL initiated abort)

- * メッセージ *

  ```
  Transfer failed (ARL initiated abort)
  ```

- * 原因 *

  SMTape処理の実行中にアグリゲートの再配置を開始すると、SMTape処理は中止されます。

- * 是正措置 *

  アグリゲートの再配置処理が終了したあとにSMTape処理を実行します。

Transfer failed (CFO initiated abort)

- * メッセージ *

  ```
  Transfer failed (CFO initiated abort)
  ```

- * 原因 *

  CFOアグリゲートのストレージフェイルオーバー（テイクオーバーとギブバック）処理が原因で、SMTape処理が中止されます。

- * 是正措置 *

  CFOアグリゲートのストレージフェイルオーバーが終了したあとにSMTape処理を実行します。

転送に失敗（ **SFO** によって中止が開始されました）

- * メッセージ *

```
Transfer failed (SFO initiated abort)
```

- * 原因 *

  ストレージフェイルオーバー（テイクオーバーとギブバック）処理が原因で、SMTape処理が中止されます。

- * 是正措置 *

  ストレージフェイルオーバー（テイクオーバーとギブバック）処理が終了したあとにSMTape処理を実行します。

移行中の基盤となるアグリゲート

- * メッセージ *

```
Underlying aggregate under migration
```

- * 原因 *

  移行（ストレージフェイルオーバーまたはアグリゲートの再配置）中のアグリゲートでSMTape処理が開始されると、SMTape処理は失敗します。

- * 是正措置 *

  アグリゲートの移行が終了したあとにSMTape処理を実行します。

ボリュームは移行中です

- * メッセージ *

```
Volume is currently under migration
```

- * 原因 *

  ボリューム移行とSMTapeバックアップを同時に実行することはできません。

- * 是正措置 *

  ボリューム移行が完了してから、バックアップジョブを再試行します。

ボリュームはオフライン

- * メッセージ *

```
Volume offline
```

- * 原因 *

  バックアップ対象のボリュームがオフラインです。

- * 是正措置 *

ボリュームをオンラインにしてから、バックアップを再試行します。

ボリュームは制限なし

- * メッセージ *

  `Volume not restricted`

- * 原因 *

  データのリストア先のデスティネーションボリュームが制限されていません。

- * 是正措置 *

  ボリュームを制限して、リストア処理を再試行します。

NDMP構成

ONTAP NDMP構成の詳細

サードパーティ製バックアップアプリケーションを使用してデータをテープに直接バックアップするために、ネットワークデータ管理プロトコル（NDMP）を使用するようにONTAP 9クラスタを簡単に設定できます。

バックアップアプリケーションがCluster Aware Backup（CAB）をサポートしている場合は、SVMを対象としたNDMPまたはノードを対象としたNDMPを設定できます。

- SVMを対象としたクラスタ（管理SVM）レベルでは、クラスタの異なるノードでホストされているすべてのボリュームをバックアップできます。可能な場合は、SVMを対象としたNDMPを推奨します。
- ノードを対象としたNDMPを使用すると、そのノードでホストされているすべてのボリュームをバックアップできます。

バックアップアプリケーションでCABがサポートされていない場合は、ノードを対象としたNDMPを使用する必要があります。

SVMを対象としたNDMPとノードを対象としたNDMPは相互に排他的であり、同じクラスタ上に設定することはできません。

ノードを対象としたNDMPは、ONTAP 9で廃止されました。

詳細については、をご覧ください "クラスタ対応バックアップ（CAB）"。

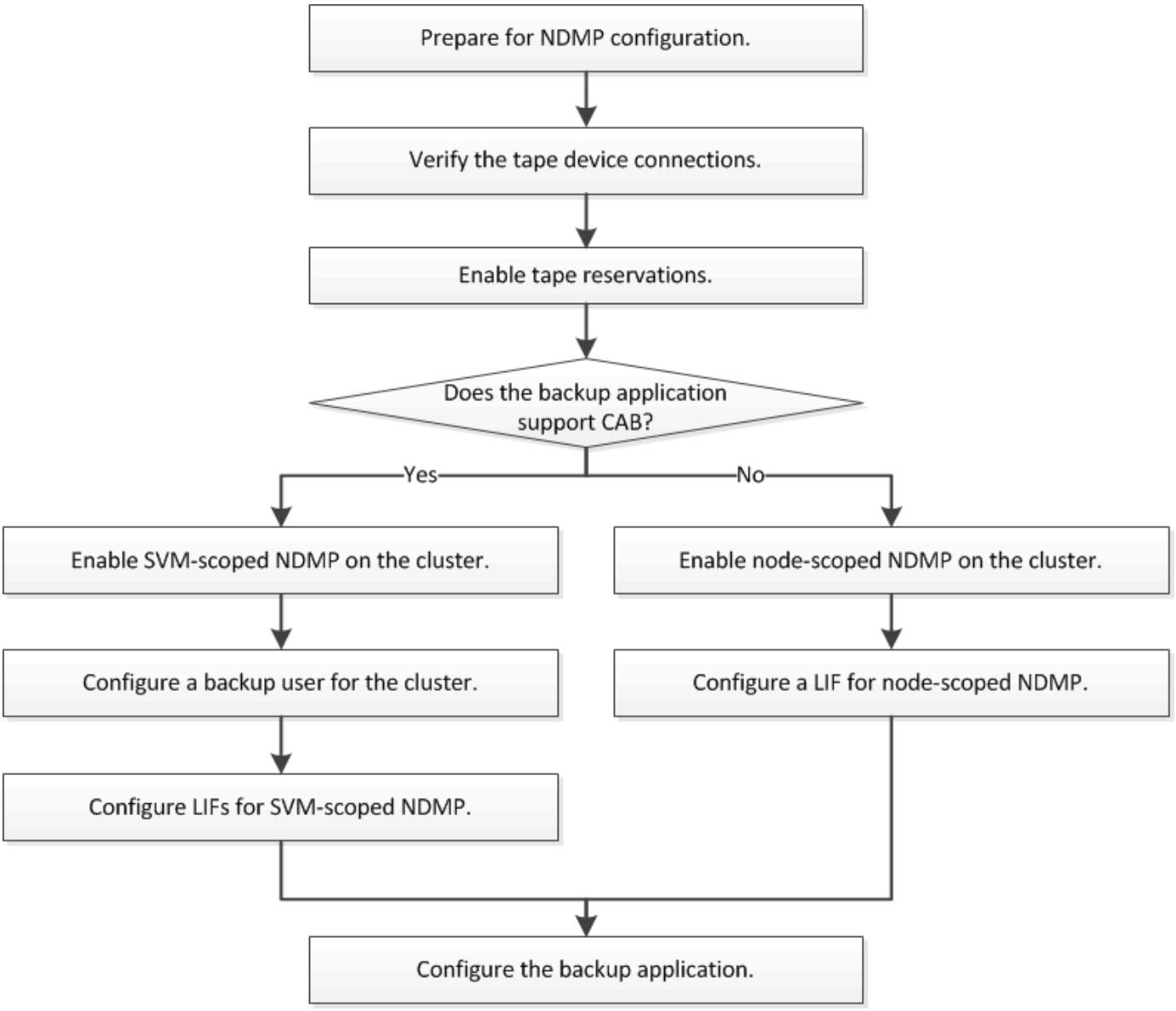
NDMPを設定する前に、次の点を確認してください。

- サードパーティ製バックアップアプリケーション（データ管理アプリケーションまたはDMAとも呼ばれる）がある。
- クラスタ管理者である。
- テープデバイスとオプションのメディアサーバがインストールされている。

- テープデバイスは、Fibre Channel（FC）スイッチを介してクラスタに接続されているか、ローカルに接続されています。
- 少なくとも1つのテープデバイスのLogical Unit Number（LUN；論理ユニット番号）が0である。

ONTAP NDMP構成ワークフローについて学ぶ

NDMP を使用したテープバックアップのセットアップでは、 NDMP 構成の準備、テープデバイスの接続の確認、テープ予約の有効化、 SVM またはノードレベルでの NDMP の設定、クラスタでの NDMP の有効化、バックアップユーザの設定、 LIF の設定、バックアップアプリケーションの設定を行います。



ONTAP NDMP構成を準備する

Network Data Management Protocol（NDMP；ネットワークデータ管理プロトコル）経由のテープバックアップアクセスを設定する前に、計画した構成がサポートされていること、テープドライブが各ノードの認定ドライブとして表示されていること、すべての

ノードにクラスタ間LIFがあること、およびバックアップアプリケーションでCluster Aware Backup（CAB）拡張がサポートされているかどうかを確認する必要があります。

手順

1. ONTAPのサポートについては、バックアップアプリケーションプロバイダの互換性マトリックスを参照してください（NetAppでは、サードパーティ製のバックアップアプリケーションがONTAPまたはNDMPに対応していません）。

   次のNetAppコンポーネントに互換性があることを確認する必要があります。

   - クラスタで実行されている ONTAP 9 のバージョン。
   - バックアップアプリケーションのベンダーとバージョン。Veritas NetBackup 8.2やCommvaultなど。
   - テープデバイスの詳細情報には、テープドライブのメーカー、モデル、インターフェイスなどが含まれます。たとえば、IBM Ultrium 8やHPE StoreEver Ultrium 30750 LTO-8などです。
   - クラスタ内のノードのプラットフォーム。FAS8700やA400など。

   バックアップアプリケーションのレガシーONTAP互換性サポートマトリックスについては、を参照して "NetApp Interoperability Matrix Tool"ください。

2. 各ノードの組み込みのテープ構成ファイルに、テープドライブが認定ドライブとして表示されていることを確認します。

   a. コマンドラインインターフェイスで、コマンドを使用して組み込みのテープ構成ファイルを表示します `storage tape show-supported-status`。

   ```
   cluster1::> storage tape show-supported-status

   Node: cluster1-1
                                    Is
   Tape Drives                      Supported  Support Status
   -------------------------------  ---------
   -------------------------------
   Certance Ultrium 2               true       Dynamically Qualified
   Certance Ultrium 3               true       Dynamically Qualified
   Digital DLT2000                  true       Qualified
   ```

   b. テープドライブを、出力に表示された認定ドライブのリストと比較します。

   出力に表示されるテープデバイスの名前は、デバイスラベルまたはInteroperability Matrixに記載されている名前と多少異なる場合があります。たとえば、Digital DLT2000はDLT2kとも呼ばれます。このような小さな名前の違いは無視してかまいません。

   c. デバイスがInteroperability Matrixで認定されているにもかかわらず、出力に認定デバイスとして表示されない場合は、NetAppサポートサイトの手順に従って、デバイスの更新された構成ファイルをダウンロードしてインストールします。

   "NetAppのダウンロード:テープデバイス構成ファイル"

ノードの出荷後にテープデバイスが認定されていた場合、認定デバイスが組み込みのテープ構成ファイルにリストされていないことがあります。

3. クラスタ内のすべてのノードにクラスタ間LIFがあることを確認します。

   a. コマンドを使用して、ノードのクラスタ間LIFを表示します `network interface show -role intercluster`。

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

   b. クラスタ間LIFがいずれのノードにも存在しない場合は、コマンドを使用してクラスタ間LIFを作成し`network interface create`ます。

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   の詳細については `network interface create`、を"ONTAPコマンド リファレンス"参照してくだ

さい。

"ネットワーク管理"

4. バックアップアプリケーションに付属のドキュメントを参照して、バックアップアプリケーションがCluster Aware Backup（CAB）をサポートしているかどうかを確認します。

   キャブのサポートは、実行可能なバックアップのタイプを決定する重要な要素です。

関連情報

- "ストレージテープショー"
- "ストレージテープサポートステータスの表示"

ONTAP NDMPテープデバイスの接続を確認する

すべてのドライブとメディアチェンジャが ONTAP でデバイスとして認識されていることを確認する必要があります。

手順

1. コマンドを使用して、すべてのドライブとメディアチェンジャに関する情報を表示します `storage tape show`。

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                 Device Type     Description
Status
------------------------  --------------  ------------------------------
--------
sw4:10.11                 tape drive      HP LTO-3
normal
0b.125L1                  media changer   HP MSL G3 Series
normal
0d.4                      tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                    media changer   IBM 3573-TL
normal
...
```

2. テープドライブが表示されない場合は、問題のトラブルシューティングを行います。
3. メディアチェンジャが表示されない場合は、コマンドを使用してメディアチェンジャに関する情報を表示し `storage tape show-media-changer`、問題のトラブルシューティングを行います。

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

関連情報

- "ストレージテープショーメディアチェンジャー"

ONTAP NDMPバックアップ操作のテープ予約を有効にする

NDMP バックアップ処理のために、バックアップアプリケーションで使用するテープドライブが予約されていることを確認する必要があります。

タスクの内容

予約の設定はバックアップアプリケーションによって異なります。これらの設定は、バックアップアプリケーションおよび同じドライブを使用するノードまたはサーバと一致する必要があります。正しい予約設定については、バックアップアプリケーションのベンダーのドキュメントを参照してください。

手順

1. コマンドを使用して予約を有効にし `options -option-name tape.reservations -option-value persistent`ます。

   次のコマンドは、という値で予約を有効にし `persistent`ます。

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. コマンドを使用してすべてのノードで予約が有効になっていることを確認し `options tape.reservations`、出力を確認します。

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                 persistent

cluster1-2
    tape.reservations                 persistent
2 entries were displayed.
```

SVMを対象としたNDMPの設定

ONTAPクラスタでSVMスコープのNDMPを有効にする

DMAがCluster Aware Backup（CAB）拡張をサポートしている場合は、SVMを対象としたNDMPを有効にし、クラスタ（管理SVM）でNDMPサービスを有効にし、データ接続と制御接続用のLIFを設定することで、クラスタの異なるノードでホストされているすべてのボリュームをバックアップできます。

開始する前に

CAB拡張はDMAでサポートされている必要があります。

タスクの内容

ノードを対象としたNDMPモードをオフにすると、クラスタでSVMを対象としたNDMPモードが有効になります。

手順

1. SVMを対象としたNDMPモードを有効にします。

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   SVMを対象としたNDMPモードが有効になります。

2. 管理SVMでNDMPサービスを有効にします。

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   認証タイプはデフォルトでに設定され `challenge`、プレーンテキスト認証は無効になっています。

   セキュアな通信のために、プレーンテキスト認証は無効にしておく必要があります。

3. NDMPサービスが有効になっていることを確認します。

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

ONTAP NDMP認証のバックアップユーザーを有効にする

バックアップアプリケーションからSVMを対象としたNDMPを認証するには、十分なPrivilegesとNDMPパスワードを持つ管理ユーザが必要です。

タスクの内容

バックアップ管理者ユーザ用のNDMPパスワードを生成する必要があります。バックアップ管理ユーザはクラスタレベルまたはSVMレベルで有効にすることができ、必要に応じて新しいユーザを作成することもできます。デフォルトでは、次のロールのユーザがNDMPバックアップを認証できます。

- クラスタ全体： `admin`または `backup`
- 個 々 のSVM： `vsadmin`または `vsadmin-backup`

NISまたはLDAPユーザを使用する場合は、そのユーザがそれぞれのサーバ上に存在している必要があります。Active Directoryユーザは使用できません。

手順

1. 現在の管理者ユーザと権限を表示します。

   ```
   security login show
   ```

   の詳細については `security login show`、を"ONTAPコマンド リファレンス"参照してください。

2. 必要に応じて、コマンドと、クラスタ全体または個 々 のSVM Privilegesに適したロールを使用して、新しいNDMPバックアップユーザを作成し `security login create`ます。

   パラメータには、ローカルバックアップユーザの名前、またはNISまたはLDAPユーザの名前を指定できます `-user-or-group-name`。

   次のコマンドでは、ロールが割り当てられた `backup`バックアップユーザがクラスタ全体に対して作成され `backup_admin1`ます。

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   次のコマンドを実行すると、個 々 のSVMにロールが割り当てられた `vsadmin-backup`バックアップユーザが作成され `vsbackup_admin1`ます。

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   ```

`-application ssh -authmethod password -role vsadmin-backup`

新しいユーザのパスワードを入力し、確認のためにもう一度入力します。

の詳細については `security login create`、を"ONTAPコマンド リファレンス"参照してください。

3. コマンドを使用して、管理SVMのパスワードを生成します `vserver services ndmp generate password`。

   生成されたパスワードは、バックアップアプリケーションによるNDMP接続の認証に使用する必要があります。

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

SVM スコープの **NDMP** 用に **ONTAP LIF** を構成する

データリソースとテープリソースの間のデータ接続、および管理SVMとバックアップアプリケーションの間の制御接続の確立に使用されるLIFを特定する必要があります。LIFを特定したら、サービスポリシーとフェイルオーバーポリシーが設定されていることを確認する必要があります。

ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "サポートされるトラフィックの管理"。

ONTAP 9 .10.1以降

手順

1. コマンドでパラメータを指定して `-service-policy`、ノードでホストされているクラスタ間LIFを特定します `network interface show`。

   ```
   network interface show -service-policy default-intercluster
   ```

   の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドでパラメータを指定して `-service-policy`、ノードでホストされている管理LIFを特定します `network interface show`。

   ```
   network interface show -service-policy default-management
   ```

3. クラスタ間LIFにサービスが含まれていることを確認し `backup-ndmp-control`ます。

   ```
   network interface service-policy show
   ```

   の詳細については `network interface service-policy show`、を"ONTAPコマンド リファレンス"参照してください。

4. すべてのLIFのフェイルオーバーポリシーが適切に設定されていることを確認します。

   a. コマンドを使用して、 `network interface show -failover`クラスタ管理LIFのフェイルオーバーポリシーがに設定されていること、およびクラスタ間LIFとノード管理LIFのポリシーがに設定され `local-only`ていることを確認し `broadcast-domain-wide`ます。

      次のコマンドは、クラスタ管理LIF、クラスタ間LIF、およびノード管理LIFのフェイルオーバーポリシーを表示します。

```
cluster1::> network interface show -failover

           Logical          Home             Failover    Failover
Vserver    Interface        Node:Port        Policy      Group
-------    --------------   --------------   ----------  --------
cluster    cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                         Failover
Targets:
                                                         .......
cluster1   cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                         Failover
Targets:
                                                         .......
           IC1              cluster1-1:e0a   local-only  Default
                                                         Failover
Targets:
           IC2              cluster1-1:e0b   local-only  Default
                                                         Failover
Targets:
                                                         .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
```

a. フェイルオーバーポリシーが適切に設定されていない場合は、コマンドでパラメータを指定し `-failover-policy`てフェイルオーバーポリシーを変更します `network interface modify`。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

5. コマンドでパラメータを指定し `preferred-interface-role`て、データ接続に必要なLIFを指定し `vserver services ndmp modify`ます。

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. コマンドを使用して、クラスタに優先インターフェイスロールが設定されていることを確認します `vserver services ndmp show`。

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9 .9以前

手順

1. コマンドでパラメータを指定して `-role`、クラスタ間LIF、クラスタ管理LIF、およびノード管理LIFを特定します `network interface show`。

   次のコマンドは、クラスタ間LIFを表示します。

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   次のコマンドは、クラスタ管理LIFを表示します。

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

次のコマンドは、ノード管理LIFを表示します。

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

の詳細については `network interface show`、を"ONTAPコマンド リファレンス"参照してください。

2. クラスタ間(`node-mgmt`LIF、クラスタ管理`LIF(`cluster-mgmt`、およびノード管理LIFでNDMPに対してファイアウォールポリシーが有効になっていることを確認します。

   a. コマンドを使用して、NDMPに対してファイアウォールポリシーが有効になっていることを確認します `system services firewall policy show`。

      次のコマンドは、クラスタ管理LIFのファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

次のコマンドは、クラスタ間LIFのファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

次のコマンドは、ノード管理LIFのファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. ファイアウォールポリシーが有効になっていない場合は、コマンドでパラメータを指定して `-service`、ファイアウォールポリシーを有効にします `system services firewall policy modify`。

次のコマンドは、クラスタ間LIFのファイアウォールポリシーを有効にします。

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. すべてのLIFのフェイルオーバーポリシーが適切に設定されていることを確認します。

a. コマンドを使用して、 `network interface show -failover`クラスタ管理LIFのフェイルオーバーポリシーがに設定されていること、およびクラスタ間LIFとノード管理LIFのポリシーがに設定され `local-only`ていることを確認し `broadcast-domain-wide`ます。

次のコマンドは、クラスタ管理LIF、クラスタ間LIF、およびノード管理LIFのフェイルオーバーポリシーを表示します。

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ------------------ --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1   cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
           IC1                 cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
           IC2                 cluster1-1:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
```

a. フェイルオーバーポリシーが適切に設定されていない場合は、コマンドでパラメータを指定し `-failover-policy`てフェイルオーバーポリシーを変更します `network interface modify`。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

4. コマンドでパラメータを指定し `preferred-interface-role`て、データ接続に必要なLIFを指定し `vserver services ndmp modify`ます。

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. コマンドを使用して、クラスタに優先インターフェイスロールが設定されていることを確認します `vserver services ndmp show`。

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

ノードを対象とした**NDMP**の設定

ONTAPクラスタでノードスコープ**NDMP**を有効にする

単一のノードでホストされているボリュームをバックアップするには、ノードを対象としたNDMPを有効にし、NDMPサービスを有効にし、データ接続と制御接続用のLIFを設定します。この処理は、クラスタのすべてのノードに対して実行できます。

ノードを対象としたNDMPは、ONTAP 9で廃止されました。

タスクの内容

ノードスコープモードでNDMPを使用する場合は、ノード単位で認証を設定する必要があります。詳細については、を参照してください "サポート技術情報の記事「ノードスコープモードでNDMP認証を構成する方法」"。

手順

1. ノードを対象としたNDMPモードを有効にします。

```
cluster1::> system services ndmp node-scope-mode on
```

NDMPのnode-scope-modeが有効になります。

2. クラスタ内のすべてのノードでNDMPサービスを有効にします。

   ワイルドカード「*」を使用すると、すべてのノードで NDMP サービスが同時に有効になります。

   バックアップアプリケーションによるNDMP接続の認証用のパスワードを指定する必要があります。

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. NDMPパスワードのセキュアな通信のためのオプションを無効にし `-clear-text`ます。

   すべてのノードで同時にワイルドカード"`オプションを使用する*" disables the `-clear-text。

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. NDMPサービスが有効になっていて、オプションが無効になっていることを確認し `-clear-text`ます。

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

ノードスコープの**NDMP**用に**ONTAP LIF**を構成する

ノードとバックアップアプリケーションの間のデータ接続および制御接続の確立に使用されるLIFを特定する必要があります。LIFを特定したら、そのLIFに対してファイアウォールポリシーとフェイルオーバーポリシーが設定されていることを確認する必要があります。

ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "サポートされるトラフィックの管理"。

ONTAP 9 .10.1以降

手順

1. コマンドでパラメータを指定して `-service-policy`、ノードでホストされているクラスタ間LIFを特定します `network interface show`。

```
network interface show -service-policy default-intercluster
```

2. クラスタ間LIFにサービスが含まれていることを確認し `backup-ndmp-control`ます。

```
network interface service-policy show
```

3. クラスタ間LIFのフェイルオーバーポリシーが適切に設定されていることを確認します。

   a. コマンドを使用して、 `network interface show -failover`クラスタ間LIFのフェイルオーバーポリシーがに設定されていることを確認します `local-only`。

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. フェイルオーバーポリシーが適切に設定されていない場合は、コマンドでパラメータを指定し `-failover-policy`てフェイルオーバーポリシーを変更します `network interface modify`。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

`network interface service-policy show`、および `network interface modify`の詳細について `network interface show`
は、をlink:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface["ONTAPコマンド リファレンス"^]参照してください。

ONTAP 9 .9以前

手順

1. コマンドでパラメータを指定して `-role`、ノードでホストされているクラスタ間LIFを特定します `network interface show`。

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. クラスタ間LIFでNDMPに対してファイアウォールポリシーが有効になっていることを確認します。

   a. コマンドを使用して、NDMPに対してファイアウォールポリシーが有効になっていることを確認します `system services firewall policy show`。

      次のコマンドは、クラスタ間LIFのファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

b. ファイアウォールポリシーが有効になっていない場合は、コマンドでパラメータを指定して `-service`、ファイアウォールポリシーを有効にします `system services firewall policy modify`。

次のコマンドは、クラスタ間LIFのファイアウォールポリシーを有効にします。

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. クラスタ間LIFのフェイルオーバーポリシーが適切に設定されていることを確認します。

a. コマンドを使用して、 `network interface show -failover`クラスタ間LIFのフェイルオーバーポリシーがに設定されていることを確認します `local-only`。

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

b. フェイルオーバーポリシーが適切に設定されていない場合は、コマンドでパラメータを指定し `-failover-policy`てフェイルオーバーポリシーを変更します `network interface modify。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

および `network interface modify`の詳細については `network interface show、を"ONTAPコマンド リファレンス"参照してください。

ONTAP NDMP構成用のバックアップアプリケーションを構成する

クラスタで NDMP アクセスを設定したら、クラスタ構成から情報を収集し、バックアップアプリケーションで残りのバックアッププロセスを設定する必要があります。

手順

1. ONTAP で前に設定した次の情報を収集します。
   - バックアップアプリケーションで NDMP 接続を作成するために必要なユーザ名とパスワード
   - バックアップアプリケーションからクラスタに接続するために必要なクラスタ間 LIF の IP アドレス
2. ONTAPで、コマンドを使用して、ONTAPが各デバイスに割り当てたエイリアスを表示します `storage`

`tape alias show`。

エイリアスを確認しておくと、バックアップアプリケーションの設定で役立つことがよくあります。

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                          Alias     Mapping
----------------------------- --------- --------------------------------
stsw-3220-4a-4b-02            st2       SN[HU19497WVR]
...
```

3. バックアップアプリケーションで、バックアップアプリケーションのドキュメントに従って残りのバックアッププロセスを設定します。

終了後

ボリューム移動や LIF 移行などのデータ移動イベントが発生した場合に備えて、中断されたバックアップ処理を再初期化できるように準備しておく必要があります。

関連情報

- "ストレージテープエイリアス表示"

NetApp ElementソフトウェアとONTAP間のレプリケーションの概要

SnapMirrorを使用してElementボリュームのSnapshotをONTAPデスティネーションにレプリケートすることで、Elementシステムのビジネス継続性を確保できます。これにより、 Element サイトで災害が発生した場合でも、 ONTAP システムからクライアントに引き続きデータを提供し、サービスのリストア後に Element システムを再アクティブ化することができます。

ONTAP 9.4以降では、ONTAPノードで作成したLUNのSnapshotをElementシステムにレプリケートして戻すことができます。たとえば、Elementサイトの停止中にLUNを作成した場合や、LUNを使用してONTAPからElementソフトウェアにデータを移行する場合などです。

"NetApp ElementソフトウェアとONTAPのレプリケーションの設定"です。

イベント、パフォーマンス、健全性の監視

System Managerを使用したクラスタパフォーマンスの監視

ONTAP System Managerを使用してクラスタのパフォーマンスを監視する

このセクションのトピックでは、ONTAP 9 .7以降のリリースでSystem Managerを使用してクラスタの健全性とパフォーマンスを管理する方法について説明します。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"クラスタのパフォーマンスを監視します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

System Managerのダッシュボードでシステムに関する情報を確認することで、クラスタのパフォーマンスを監視できます。ダッシュボードには、重要なアラートと通知、ストレージ階層とボリュームの効率性と容量、クラスタで使用可能なノード、HAペアを構成するノードのステータス、最もアクティブなアプリケーションとオブジェクト、クラスタやノードのパフォーマンス指標に関する情報が表示されます。

ダッシュボードでは、次の情報を確認できます。

- 健全性：クラスタの健全性
- 容量：クラスタで使用可能な容量を教えてください。
- パフォーマンス：レイテンシ、IOPS、スループットを基準に、クラスタのパフォーマンスはどれくらいですか？
- ネットワーク：ホストとストレージオブジェクト（ポート、インターフェイス、Storage VMなど）のネットワークはどのように設定されていますか？

健全性と容量の概要でをクリックすると、追加情報を表示したり、タスクを実行したりできます →。

パフォーマンスの概要では、時間、日、週、月、または年に基づいて指標を表示できます。

ネットワークの概要には、ネットワーク内の各オブジェクトの数が表示されます（例：「8 NVMe/FCポート」）。数字をクリックすると、各ネットワークオブジェクトの詳細が表示されます。

ONTAP System Managerダッシュボードでクラスタを表示する方法について学習します

System Managerダッシュボードを使用すると、ONTAPクラスタを1つの場所からすばやく包括的に把握できます。

System Managerダッシュボードを使用すると、重要なアラートと通知、ストレージ階層とボリュームの効率性と容量、クラスタで使用可能なノード、ハイアベイラビリティ（HA）ペアを構成するノードのステータス、最もアクティブなアプリケーションとオブジェクト、クラスタやノードのパフォーマンス指標に関する情報を一目で確認できます。

ダッシュボードは次の4つのパネルで構成されています。

健全性

[健全性]ビューには、クラスタ内の検出可能なすべてのノードの全体的な健常性に関する情報が表示されます。

[健全性]ビューには、クラスタレベルのエラーと警告（未設定のノードの詳細など）も表示され、クラスタのパフォーマンスを向上させるために変更できる特性が示されます。

をクリック → して[健全性]ビューを展開すると、クラスタの名前、バージョン、クラスタの作成日時など、クラスタの概要が表示されます。クラスタに関連付けられているノードの健常性に関連する統計を監視することもできます。タグを管理して、環境内のリソースをグループ化したり識別したりできます。[Insights]セクションでは、システムの容量、セキュリティコンプライアンス、構成を最適化できます。

容量

[容量]ビューには、クラスタのストレージスペースが表示されます。使用済み論理スペースの合計、使用済み物理スペースの合計、および使用可能なディスクスペースを確認できます。

Active IQに登録してクラスタの履歴データを表示することもできます。クリックし → て[容量]ビューを展開すると、クラスタに関連付けられている階層の概要が表示されます。各階層の容量情報（合計スペース、使用済みスペース、使用可能スペース）を確認できます。スループット、IOPS、およびレイテンシの詳細が表示されます。"容量の測定値の詳細については、System Managerを参照してください。"です。

[容量]ビューを使用して、ローカル階層とクラウド階層のどちらを追加するかを選択できます。詳細については、を参照してください "クラスタの容量を表示する"。

ネットワーク

[ネットワーク]ビューには、ネットワークの一部である物理ポート、ネットワークインターフェイス、およびStorage VMが表示されます。

[ネットワーク]ビューには、ネットワークに接続されているクライアントのタイプが表示されます。ネットワークに接続されたこれらのクライアントはそれぞれ番号で表されます（「NVMe/FC 16」など）。番号を選択すると、これらの各ネットワーク要素の詳細が表示されます。

をクリックすると、ネットワークの全ページにわたる包括的なビューが表示されます。このビューには、 → ネットワーク上のポート、ネットワークインターフェイス、Storage VM、ホストが含まれます。

パフォーマンス

[パフォーマンス]ビューには、ONTAPクラスタの健常性と効率の監視に役立つパフォーマンス統計が表示されます。統計には、レイテンシ、スループット、IOPSなどの主要なクラスタパフォーマンス指標がグラフで表示されます。

[Performance]ビューには、日、時間、週、または年ごとに異なる時間間隔でパフォーマンス統計が表示されます。各種グラフを使用してクラスタのパフォーマンスを簡単に分析し、最適化が必要な特性を特定できます。このクイック分析は、ワークロードをどのように追加または移動するかを決定するのに役立ちます。使用量のピーク時間を確認して、潜在的な変化に備えて計画することもできます。

パフォーマンスビューには、レイテンシ、スループット、IOPSに関連するパフォーマンス指標の合計が表示されます。

9.15.1以降では、パフォーマンスビューが強化され、レイテンシ、スループット、IOPSに関連する読み取

り、書き込み、その他、合計のパフォーマンス指標のグラフが表示されるようになりました。その他の指標には、読み取りまたは書き込み以外の処理が含まれます。

パフォーマンス値は3秒ごとに更新され、パフォーマンスグラフは15秒ごとに更新されます。クラスタのパフォーマンスに関する情報がない場合、グラフは表示されません。

クリックする と、時間、日、週、月、年ごとのパフォーマンス指標の全ページビューが表示されます。ローカルシステムのパフォーマンス指標のレポートをダウンロードすることもできます。

ONTAP System Managerでホットボリュームやその他のオブジェクトを識別する

アクセス頻度の高いボリューム（ホットボリューム）やデータ（ホットオブジェクト）を特定して、クラスタパフォーマンスを高速化できます。

ONTAP 9.10.1以降では、ファイルシステム分析のアクティビティ追跡機能を使用してボリューム内のホットオブジェクトを監視できます。

手順

1. [ストレージ]>[ボリューム]*をクリックします。
2. IOPS、レイテンシ、およびスループットの列をフィルタして、アクセス頻度の高いボリュームやデータを表示します。

ONTAP System ManagerでQoSを変更する

ONTAP 9 8以降では、ストレージのプロビジョニング時にがサービス品質（QoS）デフォルトで有効になります。プロビジョニングプロセスでは、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。ストレージのプロビジョニングが完了したあとにQoSを変更することもできます。

手順

1. System Managerで、**[ストレージ]***を選択し、[ボリューム]*を選択します。
2. QoSを変更するボリュームの横にある*[編集]*を選択します 。

ONTAP System Managerでリスクを監視する

ONTAP 9 .10.0以降では、System Managerを使用して、Active IQデジタルアドバイザ（デジタルアドバイザ）によって報告されるリスクを監視できます。ONTAP 9 .10.1以降では、System Managerを使用してリスクを承認することもできます。

NetAppデジタルアドバイザは、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を報告します。System Managerを使用すると、Digital Advisorによって報告されるリスクを確認し、ストレージ管理、可用性の向上、セキュリティの強化、ストレージパフォーマンスの向上に役立つ実用的な情報を受け取ることができます。

Digital Advisorアカウントへのリンク

Digital Advisorからリスクに関する情報を受け取るには、最初にSystem ManagerからDigital Advisorアカウン

トにリンクする必要があります。

手順

1. System Manager で、 * Cluster > Settings * の順にクリックします。
2. [**Active IQ Registration**](登録 *) で '[*Register] (登録 *) をクリックします
3. Digital Advisorのクレデンシャルを入力します。
4. クレデンシャルの認証が完了したら、「 * 確認」をクリックして Active IQ と System Manager * をリンクします。

リスク数を表示する

ONTAP 9 .10.0以降では、Digital Advisorによって報告されたリスクの数をSystem Managerのダッシュボードで確認できます。

開始する前に

System ManagerからDigital Advisorアカウントへの接続を確立する必要があります。を参照してください Digital Advisorアカウントへのリンク。

手順

1. System Manager で、 * ダッシュボード * をクリックします。
2. * Health * セクションで、報告されたリスクの数を確認します。

> リスクの数を示すメッセージをクリックすると、各リスクの詳細情報を確認できます。を参照して リスクの詳細を表示

リスクの詳細を表示

ONTAP 9 .10.0以降では、Digital Advisorから報告されるリスクが影響範囲別に分類される仕組みをSystem Managerで確認できます。また、報告された各リスク、システムへの潜在的な影響、および対処方法に関する詳細情報も表示できます。

開始する前に

System ManagerからDigital Advisorアカウントへの接続を確立する必要があります。を参照してください Digital Advisorアカウントへのリンク。

手順

1. [* イベント]>[すべてのイベント *] をクリックします。
2. 概要 * セクションの * Active IQ 提案 * で、各インパクトエリアカテゴリのリスク数を表示します。リスクカテゴリには次のものがあります。
   - パフォーマンスと効率性
   - 可用性と保護
   - 容量
   - 構成
   - セキュリティ

3. Active IQ Suggestions * （リスク提案 * ）タブをクリックして、以下を含む各リスクに関する情報を表示します。
    - システムへの影響のレベル
    - リスクのカテゴリ
    - 影響を受けるノード
    - 必要な緩和策のタイプ
    - 対処方法

リスクを承認

ONTAP 9 .10.1以降では、System Managerを使用して未解決のリスクを承認できます。

手順

1. System Managerで、の手順を実行してリスクのリストを表示しますリスクの詳細を表示。
2. 承認する未完了のリスクの名前をクリックします。
3. 次のフィールドに情報を入力します。
    - リマインダー（日付）
    - 位置合わせ
    - コメント
4. [* Acknowledge （確認）] をクリックし

> リスクを承認してから、Digital Advisorの提案リストに変更が反映されるまでに数分かかります。

リスクの承認を取り消し

ONTAP 9 .10.1以降では、以前に承認したリスクの承認を取り消すことができます。

手順

1. System Managerで、の手順を実行してリスクのリストを表示しますリスクの詳細を表示。
2. 承認を取り消す承認済みリスクの名前をクリックします。
3. 次のフィールドに情報を入力します。
    - 位置合わせ
    - コメント
4. [承認の取り消し *] をクリックします。

> リスクの承認を取り消してから、Digital Advisorの提案リストに変更が反映されるまでに数分かかります。

ONTAP System Managerの分析情報でシステムを最適化

System Managerでは、システムの最適化に役立つ分析情報を確認できます。

タスクの内容

この手順は、FAS、AFF、および ASA システムに適用されます。ASAASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をお持ちの場合は、 "以下の手順を実行します"システムの最適化に役立つ洞察を表示します。ASAr2 システムは、SAN のみのお客様向けに簡素化された ONTAP エクスペリエンスを提供します。

ONTAP 9.11.1 以降では、システムの容量、セキュリティ コンプライアンス、および構成を最適化するのに役立つ分析情報を System Manager で表示できます。

> 拡張機能をブロックすると、予期しない結果になる可能性があります。.11.1以降では、System Managerを使用して、Storage VMのネイティブONTAP 9を有効にすることができます。Storage VMを推奨するSystem Manager Insightメッセージが表示される場合があります"ネイティブFPolicyの設定"。
>
> FPolicyネイティブモードでは、特定のファイル拡張子を許可または禁止できます。System Managerでは、過去にランサムウェア攻撃で使用されたファイル拡張子が3、000を超えることを推奨しています。これらの拡張子の一部は、環境内の正規のファイルによって使用されている可能性があり、ブロックすると、予期しない問題が発生する可能性があります。
>
> したがって、環境のニーズに合わせて拡張子のリストを変更することを強くお勧めします。を参照してください "System Managerを使用してポリシーを再作成するためにSystem Managerで作成されたネイティブFPolicyの設定からファイル拡張子を削除する方法"。
>
> ネイティブFPolicyの詳細については、を参照してください"FPolicy設定タイプ"。

これらの分析情報はベストプラクティスに基づいて1つのページに表示され、すぐにシステムを最適化するためのアクションを開始できます。詳細については、を参照してください "System Managerの分析情報"。

最適化に関するインサイトを表示

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。

   [* Insights （インサイト）] ページには、インサイトのグループが表示されます各インサイトグループには、1つ以上のインサイトが含まれている場合があります。次のグループが表示されます。

   - Needs your attention
   - リスクの修正
   - ストレージを最適化

2. （オプション）ページの右上隅にある次のボタンをクリックして、表示されるインサイトを絞り込みます。

   - セキュリティ関連のインサイトを表示します。
   - 容量関連の分析情報が表示されます。

- 構成関連のインサイトを表示します。
- すべてのインサイトが表示されます。

分析情報に対応してシステムを最適化

System Managerでは、分析情報を却下するか、問題のさまざまな解決方法を探るか、問題を修正するプロセスを開始することで、分析情報に対応できます。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. インサイトにカーソルを合わせると、次の操作を実行するためのボタンが表示されます。
   - * Dismiss * ：ビューからインサイトを削除します。洞察を非表示にするには、 [customize-settings-insights] 。
   - * Explore * ：洞察に言及されている問題を解決するさまざまな方法を見つけます。このボタンは、修正方法が複数ある場合にのみ表示されます。
   - * 修正 *: インサイトで説明されている問題を修正するプロセスを開始します。修正を適用するために必要なアクションを実行するかどうかを確認するメッセージが表示されます。

これらの処理の一部は System Manager の他のページから開始できますが、 * Insights * ページではこの 1 ページから実行できるため、日常業務を合理化できます。

インサイトの設定をカスタマイズする

System Managerで通知を受け取るインサイトをカスタマイズできます。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. ページの右上隅にあるをクリックし、*[設定]*を選択します。
3. [* 設定 *] ページで、通知を受けるインサイトの横にチェックボックスがあることを確認します。以前にインサイトを却下した場合は、チェックボックスにチェックが入っていることを確認することで却下を解除できます。
4. [保存（ Save ）] をクリックします。

インサイトを**PDF**ファイルとしてエクスポートする

該当するすべてのインサイトをPDFファイルとしてエクスポートできます。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. ページの右上隅にあるをクリックし、*エクスポート*を選択します。

ONTAP System Managerでネイティブ**FPolicy**を設定する

開始する前に

System Manager Insightsにアクセスすると、*[ベストプラクティスの適用]*で、ネイティブのFPolicyが設定されていないことを示すメッセージが表示されることがあります。

FPolicy設定タイプの詳細については、を参照してください"FPolicy設定タイプ"。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. で、[ネイティブFPolicyは設定されていません]*を探します。
3. アクションを実行する前に、次のメッセージをお読みください。

> 拡張機能をブロックすると、予期しない結果になる可能性があります。.11.1以降では、System Managerを使用して、Storage VMのネイティブONTAP 9を有効にすることができます。FPolicyネイティブモードでは、特定のファイル拡張子を許可または禁止できます。System Managerでは、過去にランサムウェア攻撃で使用されたファイル拡張子が3、000を超えることを推奨しています。これらの拡張子の一部は、環境内の正規のファイルによって使用されている可能性があり、ブロックすると、予期しない問題が発生する可能性があります。
>
> したがって、環境のニーズに合わせて拡張子のリストを変更することを強くお勧めします。を参照してください "System Managerを使用してポリシーを再作成するためにSystem Managerで作成されたネイティブFPolicyの設定からファイル拡張子を削除する方法"。

4. [修正]*をクリックします。
5. ネイティブFPolicyを適用するStorage VMを選択します。
6. Storage VMごとに、ネイティブFPolicyを受け取るボリュームを選択します。
7. [**Configure**] をクリックします。

CLIを使用したクラスタパフォーマンスの監視と管理

ONTAP Active IQ Unified Managerのパフォーマンス監視と管理について学ぶ

基本的なパフォーマンスの監視と管理タスクを設定し、一般的なパフォーマンスの問題を特定して解決できます。

次の前提条件に該当する場合は、これらの手順を使用してクラスタのパフォーマンスを監視および管理できます。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- ONTAP コマンドラインインターフェイスに加え、 Active IQ Unified Manager （旧 OnCommand Unified Manager ）を使用して、システムのステータスとアラートを表示し、クラスタのパフォーマンスを監視し、根本原因分析を実施する。
- ONTAPコマンドラインインターフェイスを使用してストレージQuality of Service（QoS；サービス品質）を設定している。また、次の方法でQoSを利用することもできます。

    - System Manager
    - ONTAP REST API
    - ONTAP tools for VMware vSphere
    - NetAppサービスレベルマネージャ（NSLM）
    - OnCommand Workflow Automation（WFA）
- Linux または Windows ベースのインストールではなく、仮想アプライアンスを使用してActive IQ Unified Managerをインストールします。
- DHCPではなく静的な設定を使用してソフトウェアをインストールします。
- ONTAPコマンドにはadvanced権限レベルでアクセスできます。
- 「admin」ロールを持つクラスタ管理者である。

関連情報

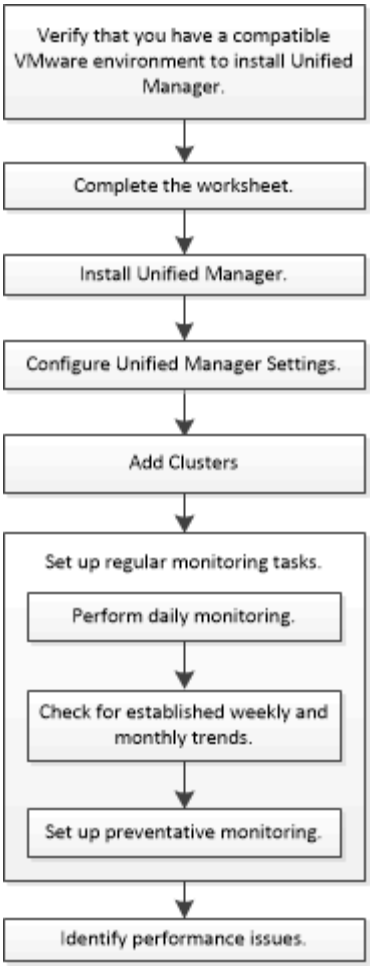
上記の想定条件に該当しない場合は、次の資料を参照してください。

- "Active IQ Unified Manager 9.8のインストール"
- "システム管理"

パフォーマンスの監視

ONTAP Active IQ Unified Managerのパフォーマンス監視とメンテナンスのワークフローについて学ぶ

クラスタパフォーマンスの監視と保守では、Active IQ Unified Manager ソフトウェアをインストールし、基本的な監視タスクを設定し、パフォーマンスの問題を特定し、必要に応じて調整を行います。



ONTAP Active IQ Unified Managerの VMware 環境要件を確認する

Active IQ Unified Managerをインストールするには、VMware環境が必要な要件を満たしていることを確認する必要があります。

手順

1. VMwareインフラがUnified Managerのインストールに必要なサイジング要件を満たしていることを確認します。
2. に移動し "Interoperability Matrix"て、次のコンポーネントについて、サポートされている組み合わせであることを確認します。
   - ONTAPのバージョン
   - ESXiオペレーティングシステムのバージョン
   - VMware vCenter Server のバージョン
   - VMware Tools のバージョン
   - ブラウザのタイプとバージョン

   Unified Managerでサポートされる構成はInteroperability Matrixで確認できます。
3. 選択した構成の構成名をクリックします。

その構成の詳細が[Configuration Details]ウィンドウに表示されます。

4. 次のタブの情報を確認します。
   - 脚注

     に、構成に固有の重要なアラートと情報を示します。

   - ポリシーとガイドライン

     すべての構成に関する一般的なガイドラインが表示されます。

ONTAP Active IQ Unified Managerワークシート

Active IQ Unified Managerをインストール、設定、接続する前に、環境に関する特定の情報を確認しておく必要があります。ワークシートに情報を記録できます。

Unified Managerのインストール情報

ソフトウェアが導入されている仮想マシン	あなたの価値
ESXiサーバのIPアドレス	
ホストの完全修飾ドメイン名	
ホストIPアドレス	
ネットワークマスク	
ゲートウェイのIPアドレス	
プライマリDNSアドレス	
セカンダリDNSアドレス	
検索ドメイン	
メンテナンスユーザの名前	
メンテナンスユウサノハスワアト	

Unified Managerの設定情報

設定	あなたの価値
メンテナンスユーザのEメールアドレス	

NTPサーバ	
SMTPサーバのホスト名またはIPアドレス	
SMTPのユーザ名	
SMTPパスワード	
SMTPのデフォルトポート	25（デフォルト値）
アラート通知の送信元Eメール	
LDAPのバインド識別名	
LDAPのバインドパスワード	
Active Directory管理者名	
Active Directoryのパスワード	
認証サーバのベース識別名	
認証サーバのホスト名またはIPアドレス	

クラスタ情報

Unified Managerで各クラスタについて次の情報を確認します。

クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理IPアドレス	
ONTAP管理者のユーザ名 管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP管理者のパスワード	
プロトコル（HTTPまたはHTTPS）	

関連情報

"カンリシヤニンシヨウトRBAC"

Active IQ Unified Managerのインストール

ONTAP Active IQ Unified Managerをダウンロードして導入する

ソフトウェアをインストールするには、仮想アプライアンス（VA）インストールファイルをダウンロードし、VMware vSphere Clientを使用してVMware ESXiサーバに導入する必要があります。VAはOVAファイルで使用できます。

手順

1. NetApp Support Siteソフトウェアのダウンロード * ページにアクセスし、 Active IQ Unified Manager を探します。

   https://mysupport.netapp.com/products/index.html

2. [Select Platform* （プラットフォームの選択）] ドロップダウンメニューで [* VMware vSphere* （ VMware vSphere * ）] を選択し、 [* Go!* （実行）] をクリックします
3. 「OVA」ファイルを、VMware vSphere Clientからアクセス可能なローカルまたはネットワーク上の場所に保存します。
4. VMware vSphere Client で、 * File * > * Deploy OVF Template * をクリックします。
5. 「OVA」ファイルを探し、ウィザードを使用してESXiサーバに仮想アプライアンスを導入します。

   ウィザードの * Properties * タブを使用して、静的な構成情報を入力できます。

6. VMの電源をオンにします。
7. 最初の起動プロセスを表示するには、 * Console * タブをクリックします。
8. プロンプトに従って、VMにVMware Toolsをインストールします。
9. タイムゾーンを設定します。
10. メンテナンスユーザの名前とパスワードを入力します。
11. VMコンソールに表示されるURLに移動します。

ONTAP Active IQ Unified Managerの初期設定を構成する

Web UI への初回アクセス時に Active IQ Unified Manager の初期セットアップダイアログボックスが表示されます。このダイアログボックスでは、いくつかの初期設定を行ったり、クラスタを追加したりできます。

手順

1. デフォルトのAutoSupport Enabled設定をそのまま使用します。
2. NTP サーバの詳細、メンテナンスユーザの E メールアドレス、 SMTP サーバのホスト名、およびその他の SMTP オプションを入力し、 * Save * をクリックします。

終了後

初期セットアップが完了すると、クラスタデータソースページが表示され、クラスタの詳細を確認できます。

Active IQ Unified Managerで監視するONTAPクラスタを指定します

クラスタを監視対象に含め、クラスタの検出ステータスを確認したり、クラスタのパフォーマンスを監視したりするには、クラスタを Active IQ Unified Manager サーバに追加する必要があります。

開始する前に

- 次の情報が必要です。
  - ホスト名またはクラスタ管理IPアドレス

    ホスト名は、 Unified Manager がクラスタへの接続に使用する完全修飾ドメイン名（ FQDN ）または短縮名です。このホスト名は、クラスタ管理IPアドレスに解決される必要があります。

  クラスタ管理IPアドレスは、管理用Storage Virtual Machine（SVM）のクラスタ管理LIFである必要があります。ノード管理LIFを使用すると処理に失敗します。

  - ONTAP管理者のユーザ名とパスワード
  - クラスタおよびクラスタのポート番号で設定できるプロトコルのタイプ（ HTTP または HTTPS ）
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- ONTAP管理者にONTAPIとSSHの管理者ロールが割り当てられている必要があります。
- Unified Manager の FQDN を使用して、 ONTAP に ping を実行できる必要があります。

  これは、ONTAPコマンドを使用して確認できます `ping -node node_name -destination Unified_Manager_FQDN`。

タスクの内容

MetroCluster構成の場合は、ローカルクラスタとリモートクラスタの両方を追加し、クラスタを正しく設定する必要があります。

手順

1. [* Configuration * > * Cluster Data Sources *] をクリックします。
2. [クラスタ] ページで、 [* 追加] をクリックします。
3. Add Cluster * （クラスタの追加）ダイアログボックスで、クラスタのホスト名または IP アドレス（ IPv4 または IPv6 ）、ユーザ名、パスワード、通信プロトコル、ポート番号など、必要な値を指定します。

   デフォルトでは、HTTPSプロトコルが選択されています。

   クラスタ管理IPアドレスは、IPv6からIPv4またはIPv4からIPv6に変更できます。次の監視サイクルが完了すると、新しいIPアドレスがクラスタグリッドとクラスタ設定ページに反映されます。
4. [追加]*をクリックします。
5. [HTTPS]が選択されている場合は、次の手順を実行します。
   a. [* Authorize Host * （ホストの認証 * ）] ダイアログボックスで、 [* View Certificate * （証明書の表示 ）] をクリックしてクラスタに関する証明書情報を表示します。

b. 「 * はい * 」をクリックします。

Unified Manager で証明書がチェックされるのはクラスタを最初に追加したときだけですが、 ONTAP に対する API 呼び出しごとに確認されるわけではありません。

証明書の期限が切れているクラスタは追加できません。SSL証明書を更新してからクラスタを追加する必要があります。

6. * オプション * ：クラスタ検出ステータスを表示します。

a. クラスタセットアップ * ページでクラスタ検出ステータスを確認します。

デフォルトの監視間隔である約 15 分後に、 Unified Manager データベースにクラスタが追加されます。

基本的な監視タスクの設定

ONTAP Active IQ Unified Managerの毎日の監視を実行する

監視を毎日実行して、注意が必要なパフォーマンスの問題がすぐに発生しないようにすることができます。

手順

1. Active IQ Unified Manager UI から * Event Inventory * ページに移動して、現在のイベントと廃止状態のイベントをすべて表示します。
2. [表示]*オプションからを選択し `Active Performance Events`、必要な操作を決定します。

ONTAP Active IQ Unified Manager の週次および月次パフォーマンス傾向を使用して、パフォーマンスの問題を特定します。

パフォーマンスの傾向を特定すると、ボリュームレイテンシを分析して、クラスタの使用率が高すぎるか低すぎるかを特定するのに役立ちます。同様の手順を使用して、CPU、ネットワーク、またはその他のシステムのボトルネックを特定できます。

手順

1. 使用率が高すぎるか低すぎる疑いがあるボリュームを探します。
2. [ボリュームの詳細 **]** タブで、 **[*30 d]** をクリックして履歴データを表示します。
3. [データのブレークダウンの条件] ドロップダウンメニューで、 [**Latency**] を選択し、 [**Submit**] をクリックします。
4. クラスタコンポーネント比較グラフで「 * Aggregate 」を選択解除し、クラスタのレイテンシをボリュームレイテンシグラフと比較します。
5. アグリゲートを選択し、クラスタコンポーネント比較チャート内の他のすべてのコンポーネントの選択を解除して、アグリゲートのレイテンシをボリュームレイテンシチャートと比較します。
6. [読み取り/書き込みレイテンシ]グラフをボリュームレイテンシのグラフと比較します。
7. クライアントアプリケーションの負荷が原因でワークロードの競合が発生していないかどうかを確認し、必要に応じてワークロードをリバランシングします。
8. アグリゲートの使用率が高すぎて競合を引き起こしていないかどうかを確認し、必要に応じてワークロードをリバランシングします。

ONTAP Active IQ Unified Managerのパフォーマンスしきい値を使用してイベント通知を生成する

イベントは、事前に定義された状況が発生したとき、またはパフォーマンスカウンタの値がしきい値を超えたときに、 Active IQ Unified Manager で自動的に生成される通知です。イベントによって、監視しているクラスタ内のパフォーマンスの問題を特定できます。特定の重大度タイプのイベントが発生したときに自動的に E メール通知を送信するアラートを設定できます。

ONTAPパフォーマンスしきい値を設定する

パフォーマンスしきい値を設定して、重大なパフォーマンスの問題を監視することができます。ユーザ定義のしきい値は、システムが定義されたしきい値に近づいたとき、または超えたときに警告または重大イベントの通知をトリガーします。

手順

1. 警告イベントと重大イベントのしきい値を作成します。
   a. [* Configuration * > * Performance Thresholds *] を選択します。
   b. [作成（ Create ）] をクリックします。
   c. オブジェクトタイプを選択し、ポリシーの名前と説明を指定します。
   d. オブジェクトカウンタの条件を選択し、警告イベントと重大イベントの制限値を指定します。
   e. イベントを送信するために制限値に違反する必要がある期間を選択し、 [保存] をクリックします。
2. しきい値ポリシーをストレージオブジェクトに割り当てます。
   a. 以前に選択したクラスタオブジェクトタイプのインベントリページに移動し、 View オプションから * Performance * を選択します。
   b. しきい値ポリシーを割り当てるオブジェクトを選択し、 * しきい値ポリシーの割り当て * をクリックします。
   c. 前の手順で作成したポリシーを選択し、 * ポリシーの割り当て * をクリックします。

例

重大なパフォーマンスの問題を特定するためにユーザ定義のしきい値を設定することができます。たとえば、ボリュームのレイテンシが20ミリ秒を超えるとMicrosoft Exchange Serverがクラッシュすることがわかっている場合は、警告しきい値を12ミリ秒、重大しきい値を15ミリ秒のように設定できます。このしきい値の設定を使用して、ボリュームのレイテンシが制限を超えたときに通知を受け取ることができます。

ONTAP Active IQ Unified Managerアラートを追加する

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

開始する前に

- イベント生成時に Active IQ Unified Manager サーバからユーザに通知を送信できるように、通知に使用するユーザの E メールアドレス、 SMTP サーバ、 SNMP トラップホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名またはEメールアドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、[スクリプト]ページを使用してUnified Managerにスクリプトを追加しておく必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

タスクの内容

ここで説明するように、[Alert Setup]ページからアラートを作成するだけでなく、イベントを受信したあとに[Event Details]ページから直接アラートを作成することもできます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [* Alert Setup*] ページで、 [* Add] をクリックします。
3. [* アラートの追加 *] ダイアログボックスで、 [* 名前 *] をクリックし、アラートの名前と概要を入力します。
4. [* リソース] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

   [* 次を含む名前（ * Name Contains ）] フィールドでテキスト文字列を指定してフィルタを設定し、リソースのグループを選択できます。指定したテキスト文字列に基づいて、フィルタルールに一致するリソースのみが使用可能なリソースのリストに表示されます。指定するテキスト文字列では、大文字と小文字が区別されます。

   あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。

5. [*Events] をクリックし、アラートをトリガーするイベント名またはイベントの重大度タイプに基づいてイベントを選択します。

   複数のイベントを選択するには、Ctrlキーを押しながら選択します。

6. [*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、 SNMP トラップをトラップレシーバに送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。

   ユーザに指定したEメールアドレスを変更し、アラートを編集用に再度開くと、変更したEメールアドレスが以前に選択したユーザにマッピングされなくなるため、[Name]フィールドには何も表示されません。また、[ユーザ]ページで選択したユーザのEメールアドレスを変更しても、変更したEメールアドレスは更新されません。

   SNMPトラップを使用してユーザに通知することもできます。

7. [保存（ Save ）] をクリックします。

アラートの追加例

次の例は、次の要件を満たすアラートを作成する方法を示しています。

- アラート名： HealthTest
- リソース：名前に「abc」を含むすべてのボリュームを対象にし、名前に「xyz」を含むすべてのボリュームを除外します。
- イベント：健全性に関するすべての重大イベントを含む
- アクション：「sample@domain.com」、「テスト」スクリプトが含まれており、15分ごとにユーザに通知する必要があります。

[Add Alert]ダイアログボックスで、次の手順を実行します。

1. をクリックし、[アラート名]*フィールドにと入力します `HealthTest`。
2. [* リソース] をクリックし、 [含める] タブで、ドロップダウン・リストから [* ボリューム] を選択します。
   a. [名前に次の文字を含む]フィールドにと入力し `abc`、名前に「abc」を含むボリュームを表示します。
   b. [Available Resources]領域で*+*を選択し[All Volumes whose name contains 'abc']、[Selected Resources]領域に移動します。
   c. をクリックし、[名前に次の文字を含む]フィールドにと入力し **`xyz`**、[追加]*をクリックします。
3. [* イベント **]** をクリックし、 **[** イベントの重要度 **]** フィールドから **[** クリティカル *] を選択します。
4. [Matching Events] 領域から [*All Critical Events] を選択し、 [Selected Events] 領域に移動します。
5. [Actions]*をクリックし、[Alert These Users]フィールドにと入力します `sample@domain.com`。
6. 15 分ごとにユーザに通知するには、「 * 15 分ごとに通知する」を選択します。

   指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。
7. 実行するスクリプトの選択メニューで、 * テスト * スクリプトを選択します。
8. [保存（ Save ）] をクリックします。

ONTAP Active IQ Unified Managerのアラート設定を構成する

アラートについて、アラートをトリガーする Active IQ Unified Manager のイベント、アラートを受け取る E メール受信者、およびアラートの頻度を指定することができます。

開始する前に

アプリケーション管理者のロールが必要です。

タスクの内容

次のタイプのパフォーマンスイベントに対して固有のアラートを設定できます。

- 重大イベント：ユーザ定義のしきい値に違反したときにトリガーされる
- 警告イベント：ユーザ定義のしきい値、システム定義のしきい値、または動的なしきい値に違反したときにトリガーされる

デフォルトでは、すべての新しいイベントについて、 Unified Manager の管理者ユーザに E メールアラート

が送信されます。Eメールアラートを他のユーザに送信するには、そのユーザのEメールアドレスを追加します。

特定のタイプのイベントに関するアラートの送信を無効にするには、イベントカテゴリのすべてのチェックボックスをオフにする必要があります。この操作によって、ユーザインターフェイスにイベントが表示されなくなることはありません。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * を選択します。

   [Alert Setup]ページが表示されます。

2. [* 追加] をクリックし、各イベントタイプに適切な設定を行います。

   Eメールアラートを複数のユーザに送信するには、各Eメールアドレスをカンマで区切って入力します。

3. [保存（ Save ）] をクリックします。

ONTAP Active IQ Unified Managerのパフォーマンスの問題を特定する

パフォーマンスイベントが発生した場合は、 Active IQ Unified Manager で問題のソースを特定し、他のツールを使用して修正することができます。イベントのEメール通知を受信したり、日 々 の監視中にイベントに気付いたりすることがあります。

手順

1. Eメール通知内のリンクをクリックすると、パフォーマンスイベントが発生しているストレージオブジェクトに直接移動できます。

状況	そしたら…。
イベントのEメール通知を受信する	リンクをクリックしてイベントの詳細ページに直接移動します。
[Event Inventory]ページを分析中にイベントに注目してください。	イベントを選択してイベントの詳細ページに直接移動します。

2. システム定義のしきい値を超えたイベントの場合は、UIに表示される推奨される対処方法に従って問題をトラブルシューティングします。
3. ユーザ定義のしきい値を超えたイベントの場合は、イベントを分析して対処が必要かどうかを判断します。
4. 問題が解決しない場合は、次の設定を確認します。
   - ストレージシステムのプロトコル設定
   - イーサネットスイッチまたはファブリックスイッチのネットワーク設定
   - ストレージシステムのネットワーク設定
   - ストレージシステムのディスクレイアウトとアグリゲートの指標を表示します
5. 問題が解決しない場合は、テクニカルサポートにお問い合わせください。

ONTAP Active IQ Digital Advisorを使用してシステムパフォーマンスを表示します

AutoSupportの計測データをNetAppに送信するONTAPシステムについて、パフォーマンスと容量に関する広範なデータを表示できます。Digital Advisorでは、System Managerよりも長い期間のシステムパフォーマンスが表示されます。

CPU利用率、レイテンシ、IOPS、プロトコル別のIOPS、およびネットワークスループットのグラフを表示できます。このデータを.csv形式でダウンロードして、他のツールで分析することもできます。

このパフォーマンスデータに加えて、Digital Advisorではワークロード別のストレージ効率を表示し、そのタイプのワークロードで想定される効率と比較できます。容量のトレンドを表示して、特定の期間に追加が必要になる可能性のあるストレージの見積もりを確認できます。

- Storage Efficiencyは、お客様レベル、クラスタレベル、ノードレベルで、メインのダッシュボードの左側に表示されます。
- パフォーマンスは、メインダッシュボードの左側にクラスタレベルおよびノードレベルで表示されます。

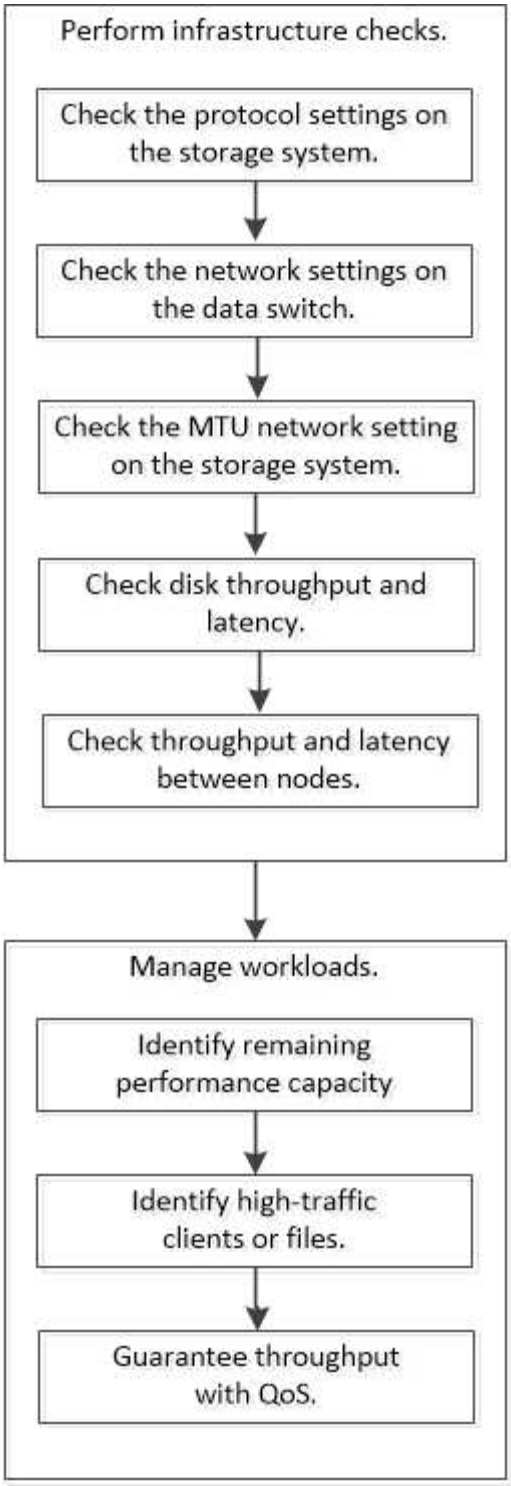
関連情報

- "Digital Advisorのドキュメント"
- "Digital Advisorのビデオプレイリスト"
- "Digital Advisor Webポータル"

パフォーマンスの問題の管理

ONTAPパフォーマンス管理ワークフロー

パフォーマンスの問題を特定したら、インフラのいくつかの基本的な診断チェックを実行して、明らかな構成エラーを排除できます。問題が特定されない場合は、ワークロード管理の問題に目を向けることができます。



基本的なインフラチェックの実行

ストレージシステムのプロトコル設定を確認

ONTAP NFS TCP最大転送サイズを確認する

NFS の場合、読み取りと書き込みの TCP 最大転送サイズがパフォーマンス問題の原因になっていないかどうかを確認することができます。このサイズが原因でパフォーマンスが低下している可能性がある場合は、サイズを大きくして対処できます。

開始する前に

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- このタスクを実行するには、advanced権限レベルのコマンドを使用する必要があります。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. TCP 最大転送サイズを確認します。

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. TCP 最大転送サイズが小さすぎる場合は、サイズを大きくします。

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. 管理者権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、のTCP最大転送サイズを1048576に変更し `SVM1`ます。

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

ONTAP iSCSI TCP読み取り/書き込みサイズを確認する

iSCSI の場合、 TCP 読み取り / 書き込みサイズを確認して、サイズ設定がパフォーマンス問題を作成中であるかどうかを判断できます。サイズが問題のソースである場合は、サイズを変更して対処できます。

開始する前に

このタスクを実行するには、advanced権限レベルのコマンドが必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. TCP ウィンドウサイズの設定を確認します。

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. TCP ウィンドウサイズの設定を変更します。

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. admin権限に戻ります。

   ```
   set -privilege admin
   ```

例

次に、のTCPウィンドウサイズを131、400バイトに変更する例を示し `SVM1`ます。

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

ONTAP CIFS/SMBマルチプレックス設定を確認する

CIFSネットワークのパフォーマンスが低下してパフォーマンスの問題が発生した場合は、多重化設定を変更して問題を改善および修正できます。

手順

1. CIFS多重化設定を確認します。

   ```
   vserver cifs options show -vserver -vserver_name -instance
   ```

2. CIFS多重化設定を変更します。

   ```
   vserver cifs options modify -vserver -vserver_name -max-mpx integer
   ```

例

次に、の最大多重化カウントを255に変更する例を示し `SVM1`ます。

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

ONTAP FCアダプタのポート速度を確認する

パフォーマンスを最適化するには、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにします。ポートに自動ネゴシエーションが設定されている場合、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

開始する前に

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

手順

1. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

   の詳細については `network fcp adapter modify`、を"ONTAPコマンド リファレンス"参照してください。

2. ポートアダプタの最大速度を確認します。

   `fcp adapter show -instance`

   の詳細については `fcp adapter show`、を"ONTAPコマンド リファレンス"参照してください。

3. 必要に応じてポート速度を変更します。

   `network fcp adapter modify -node` *`nodename`* `-adapter` *`adapter`* `-speed {1|2|4|8|10|16|auto}`

4. アダプタをオンラインにします。

   `network fcp adapter modify -node` *`nodename`* `-adapter` *`adapter`* `-state up`

5. アダプタのすべてのLIFをオンラインにします。

   `network interface modify -vserver * -lif * { -home-node node1 -home-port e0c } -status-admin up`

   の詳細については `network interface modify`、を"ONTAPコマンド リファレンス"参照してください。

例

次に、の `node1`アダプタのポート速度を2Gbpsに変更する例を示し `0d`ます。

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

データスイッチの**ONTAP**ネットワーク設定を確認する

クライアント、サーバ、およびストレージシステム（ネットワークエンドポイント）では同じMTU設定を維持する必要がありますが、パフォーマンスに影響が及ばないように、NICやスイッチなどの中間ネットワークデバイスは最大MTU値に設定する必要があります。

最高のパフォーマンスを得るには、ネットワーク内のすべてのコンポーネントがジャンボフレーム（IP 9000バイト、イーサネットを含む9022バイト）を転送できる必要があります。データスイッチは少なくとも9022バイトに設定する必要がありますが、ほとんどのスイッチでは標準値9216を使用できます。

手順

1. データスイッチの場合は、MTUサイズが9022以上に設定されていることを確認します。

詳細については、スイッチベンダーのドキュメントを参照してください。

ストレージシステムの**ONTAP MTU**ネットワーク設定を確認します

ストレージシステムのネットワーク設定がクライアントまたは他のネットワークエンドポイントと同じでない場合は、設定を変更できます。管理ネットワークのMTU設定

は1500に設定されていますが、データネットワークのMTUサイズは9000にする必要があります。

タスクの内容

ブロードキャストドメイン内のポートのMTUサイズはすべて同じですが、管理トラフィックを処理するe0Mポートは例外です。ポートがブロードキャストドメインに属している場合は、コマンドを使用して `broadcast-domain modify`、変更したブロードキャストドメイン内のすべてのポートのMTUを変更します。

NICやデータスイッチなどの中間ネットワークデバイスは、ネットワークエンドポイントよりも大きなMTUサイズに設定できます。詳細については、を参照してください "データスイッチのネットワーク設定を確認する"。

手順

1. ストレージシステムのMTUポート設定を確認します。

   ```
   network port show -instance
   ```

   の詳細については `network port show`、を"ONTAPコマンド リファレンス"参照してください。

2. ポートで使用するブロードキャストドメインのMTUを変更します。

   ```
   network port broadcast-domain modify -ipspace ipspace -broadcast-domain
   broadcast_domain -mtu new _mtu
   ```

例

次の例は、MTUポート設定を9000に変更します。

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

ONTAPディスクのスループットとレイテンシを確認する

ディスクのスループットとレイテンシの指標を確認すると、クラスタノードのトラブルシューティングに役立ちます。

タスクの内容

このタスクを実行するには、advanced権限レベルのコマンドが必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. ディスクのスループットとレイテンシの指標を確認します。

```
statistics disk show -sort-key latency
```

例

次の例は、に対する `cluster1`各ユーザの読み取り処理または書き込み処理の合計を表示します `node2。

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                     Busy Total Read  Write  Read    Write   *Latency
  Disk       Node    (%)   Ops   Ops   Ops   (Bps)    (Bps)      (us)
------------ ----    ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

関連情報

- "statistics disk show"

ONTAPのスループットとノード間のレイテンシを確認する

コマンドを使用すると、ネットワークのボトルネックを特定したり、ノード間のネットワークパスを事前に確認したりできます `network test-path`。このコマンドは、クラスタ間ノード間でもクラスタ内ノード間でも実行できます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには、advanced権限レベルのコマンドが必要です。
- クラスタ間パスの場合は、ソースクラスタとデスティネーションクラスタのピア関係が確立されている必要があります。

タスクの内容

場合によっては、ノード間のネットワークパフォーマンスがパス構成の想定どおりにならないことがあります。たとえば、SnapMirrorレプリケーション処理で発生する大量のデータ転送では、ソースクラスタとデスティネーションクラスタ間のリンクが10GbEの場合と一致しない場合があります。

コマンドを使用すると、ノード間のスループットとレイテンシを測定できます `network test-path`。このコマンドは、クラスタ間ノード間でもクラスタ内ノード間でも実行できます。

このテストではネットワークパスがデータでいっぱいになるため、システムがビジーでないときやノード間のネットワークトラフィックが過剰でないときにコマンドを実行してください。テストは10秒後にタイムアウトします。このコマンドは、ONTAP 9ノード間でのみ実行できます。

オプションは `session-type`、ネットワークパスで実行する処理のタイプを識別します。たとえば、リモートデスティネーションへのSnapMirrorレプリケーションの場合は「AsyncMirrorRemote」と指定します。タイプによって、テストで使用されるデータの量が決まります。次の表に、セッションタイプを示します。

セッションタイプ（ Session Type ）	説明
AsyncMirrorLocal です	SnapMirrorによって同じクラスタ内のノード間で使用される設定
AsyncMirrorRemote	異なるクラスタのノード間のSnapMirrorで使用される設定（デフォルトタイプ）
RemoteDataTransfer	ONTAP が同じクラスタ内のノード間のリモートデータアクセスに使用する設定（たとえば、別のノードのボリュームに格納されたファイルを取得するためのノードへのNFS要求）

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. ノード間のスループットとレイテンシを測定します。

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   ソースノードはローカルクラスタ内に存在する必要があります。デスティネーションノードは、ローカルクラスタまたはピアクラスタに配置できます。の値が「local」の `-source-node`場合は、コマンドを実行するノードを指定します。

   次のコマンドは、ローカルクラスタ上のと `node3`の `cluster2`間のSnapMirrorタイプのレプリケーション処理のスループットとレイテンシを測定し `node1`ます。

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   ```

   出力例は次のとおりです（出力の詳細は、ONTAPのバージョンによって異なります）。

```
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms:  2301.47
```

の詳細については `network test-path`、を"ONTAPコマンド リファレンス"参照してください。

3. admin権限に戻ります。

   ```
   set -privilege admin
   ```

終了後

パス構成に対して期待される値を得られない場合は、ノードのパフォーマンス統計の確認、ツールを使用したネットワークの問題の切り分け、スイッチ設定の確認などを行います。

ワークロードの管理

ONTAPで残りのパフォーマンス容量を特定

パフォーマンス容量（ *headroom* ）は、リソースのワークロードのパフォーマンスにレイテンシの影響を受ける前にノードまたはアグリゲートに配置できる作業量を測定します。クラスタで利用可能なパフォーマンス容量を把握しておくと、ワークロードのプロビジョニングと分散に役立ちます。

開始する前に

このタスクを実行するには、advanced権限レベルのコマンドが必要です。

タスクの内容

オプションでは、次の値を使用してヘッドルームの統計を収集および表示できます `-object`。

- CPUの場合は、 `resource_headroom_cpu`。
- アグリゲートの場合は、 `resource_headroom_aggr`。

このタスクは、System ManagerとActive IQ Unified Managerを使用して実行することもできます。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. リアルタイムのヘッドルーム統計の収集を開始します。

   ```
   statistics start -object resource_headroom_cpu|aggr
   ```

   の詳細については `statistics start`、を"ONTAPコマンド リファレンス"参照してください。

3. リアルタイムのヘッドルーム統計情報を表示します。

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

4. admin権限に戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、クラスタノードの1時間あたりの平均ヘッドルーム統計を表示します。

ノードの使用可能なパフォーマンス容量は、カウンタからカウンタを `optimal_point_utilization`引いて計算できます `current_utilization`。この例では、の利用率 `CPU_sti2520-213`は-14%（72%~86%）であることから、CPUの過去1時間の平均利用率が高すぎることがわかります。

または `ewma_weekly`を指定すると `ewma_monthly`、同じ情報を長期間にわたって平均化できます `ewma_daily`。

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                    -
                         current_ops                            4376
                     current_latency                           37719
                 current_utilization                              86
                   optimal_point_ops                            2573
               optimal_point_latency                            3589
          optimal_point_utilization                              72
     optimal_point_confidence_factor                              1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                    -
                         current_ops                               0
                     current_latency                               0
                 current_utilization                               0
                   optimal_point_ops                               0
               optimal_point_latency                               0
          optimal_point_utilization                               71
     optimal_point_confidence_factor                              1
2 entries were displayed.
```

の詳細については `statistics show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPでトラフィックの多いクライアントやファイルを特定する

ONTAP の Active Objects テクノロジを使用すると、クラスタのトラフィック量を著しく増大させているクライアントやファイルを特定することができます。これらの「上位」

のクライアントまたはファイルを特定したら、クラスタのワークロードをリバランシングするか、その他の手順を実行して問題を解決できます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタに最もアクセスする上位のクライアントを表示します。

   `statistics top client show -node node_name -sort-key sort_column -interval seconds_between_updates -iterations iterations -max number_of_instances`

   次のコマンドは、アクセス頻度の高い上位のクライアントを表示し `cluster1`ます。

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                                  *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

   の詳細については `statistics top client show`、を"ONTAPコマンド リファレンス"参照してください。

2. クラスタで最も多くアクセスされる上位のファイルを表示します。

   `statistics top file show -node node_name -sort-key sort_column -interval seconds_between_updates -iterations iterations -max number_of_instances`

   次のコマンドは、でアクセスされる上位のファイルを表示し `cluster1`ます。

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

の詳細については `statistics top file show`、を"ONTAPコマンド リファレンス"参照してください。

QoSでスループットを保証

ONTAPの**QoS**概要でスループットを保証

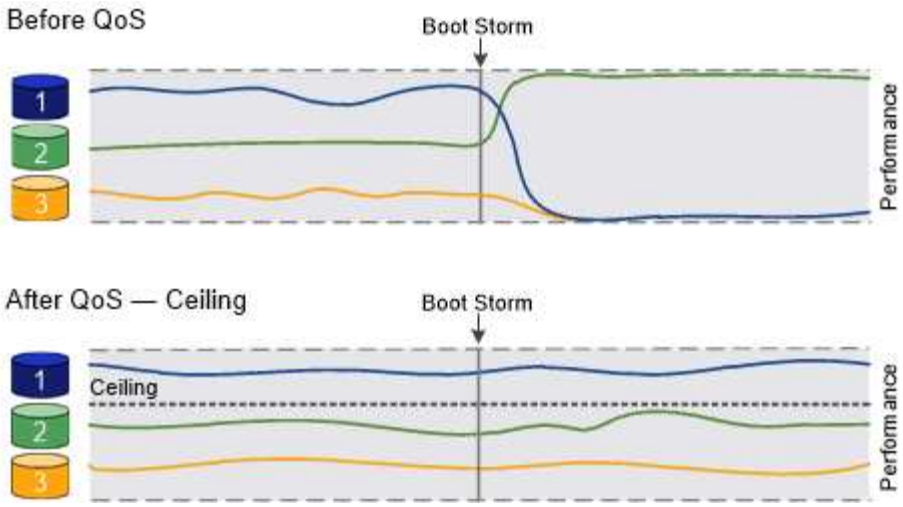
ストレージQuality of Service（QoS；サービス品質）を使用して、重要なワークロードのパフォーマンスが競合するワークロードによって低下しないようにすることができます。競合するワークロードに Throughput Ceil天 を設定して、システムリソースへの影響を制限したり、重要なワークロードに Throughput Floor_ を設定したりすることで、競合するワークロードによる要求に関係なく最小のスループットターゲットを満たすことができます。同じワークロードに対して上限と下限を設定することもできます。

スループットの上限（最大**QoS**）

スループットの上限は、ワークロードのスループットを最大IOPS、最大MBps、またはIOPSとMBpsに制限します。次の図では、ワークロード2のスループットの上限により、ワークロード1と3の「Bully」にならないようになっています。

a_policy group_ は、 1 つ以上のワークロードに対するスループットの上限を定義します。ワークロードとは、 a_storage オブジェクト： _a ボリューム、ファイル、 qtree 、または LUN 、あるいは SVM 内のすべてのボリューム、ファイル、 qtree 、または LUN の I/O 処理のことです。上限はポリシーグループの作成時に指定することも、ワークロードを監視してから指定することもできます。

ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を10%までは超えることができます。バーストに対処するために、上限を50%まで超過することがあります。バーストは、トークンが最大150%蓄積すると、シングルノードで発生します。



スループットの下限（最小**QoS**）

スループットの下限は、ワークロードのスループットが最小IOPS、最小MBps、またはIOPSとMBpsを下回らないことを保証します。次の図では、ワークロード1とワークロード3のスループットの下限が設定されているため、ワークロード2からの要求に関係なく、必要な最小スループットが確保されています。

これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

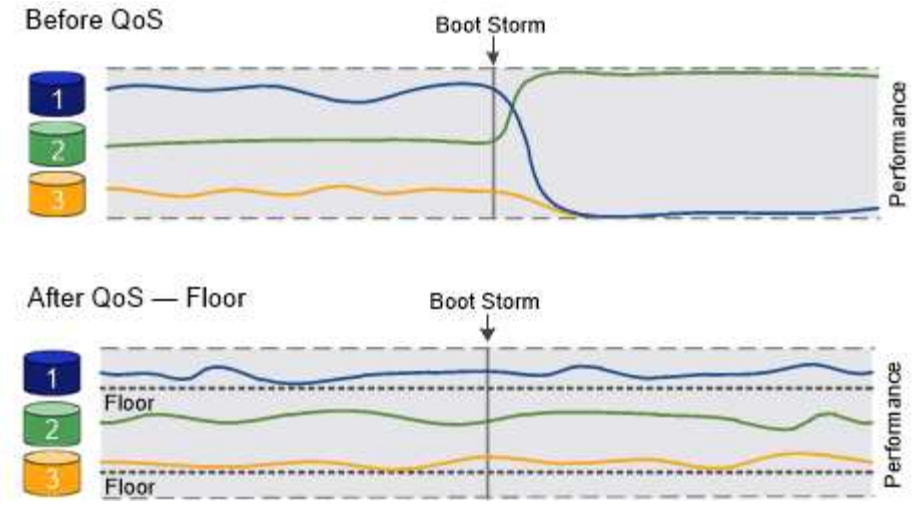
下限はポリシーグループの作成時に指定できます。また、ワークロードを監視したあとで指定することもできます。

ONTAP 9.13.1以降では、を使用してSVMスコープでスループットの下限を設定でき[adaptive-qos-templates]ます。ONTAP 9.13.1より前のリリースでは、スループットの下限を定義するポリシーグループはSVMに適用できません。

ONTAP 9 .7より前のリリースでは、十分なパフォーマンス容量がある場合にスループットの下限が保証されます。

ONTAP 9 .7以降では、十分なパフォーマンス容量がない場合でもスループットの下限が保証されます。この新しい下限の動作は、下限v2と呼ばれます。下限v2では、この保証を満たすために、スループットの下限がないワークロードや下限の設定を超える作業でレイテンシが高くなる可能性があります。下限v2は、QoSとアダプティブQoSの両方に適用されます。

ONTAP 9.7P6以降では、下限v2の新しい動作を有効または無効にするオプションを使用できます。などの重要な処理の実行中は、ワークロードが指定された下限を下回ることがあります `volume move trigger-cutover`。利用可能な容量が十分にあり、重要な処理を実行していない場合でも、ワークロードのスループットが指定された下限を最大5%下回ることがあります。下限がオーバープロビジョニングされていてパフォーマンス容量がない場合、一部のワークロードが指定された下限を下回ることがあります。



共有および非共有の**QoS**ポリシーグループ

ONTAP 9.4 以降では、 _non-shared_QoS ポリシーグループを使用して、定義されたスループットの上限または下限の環境を各メンバーのワークロードごとに指定できます。_shared_policy グループの動作は ' ポリシー・タイプによって異なります

- スループットの上限については、共有ポリシーグループに割り当てられたワークロードの合計スループットが指定した上限を超えることはできません。
- スループットの下限の場合、共有ポリシーグループは単一のワークロードにのみ適用できます。

アダプティブ**QoS**

通常、ストレージオブジェクトに割り当てるポリシーグループの値は固定値です。ストレージオブジェクトのサイズが変わった場合は、値を手動で変更する必要があります。たとえば、ボリュームの使用スペースが増えた場合、通常は指定されているスループットの上限も増やす必要があります。

アダプティブ QoS _ ワークロードのサイズの変更に合わせてポリシーグループの値が自動的に調整され、 TB または GB あたりの IOPS が一定に維持されます。これは、数百、数千のワークロードを管理する大規模な環境では大きなメリットです。

アダプティブQoSは、主にスループットの上限の調整に使用しますが、下限の管理（ワークロードサイズが増加した場合）にも使用できます。ワークロードのサイズは、ストレージオブジェクトに割り当てられたスペースまたはストレージオブジェクトで使用されているスペースのいずれかで表されます。

ONTAP 9 .5以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9 .4以前のスループットの下限ではサポートされません。

- 割り当て済みスペースのポリシーでは、ストレージオブジェクトの公称サイズを基準に IOPS と TB / GB の比率が維持されます。比率が100 IOPS/GBの場合、150GBのボリュームのスループットの上限は、ボリュームのサイズが変わらないかぎり15、000 IOPSです。ボリュームのサイズが300GBに変更されると、アダプティブQoSによってスループットの上限が30、000 IOPSに調整されます。
- a_used space-policy （デフォルト）は、ストレージ効率化前に格納されている実際のデータの量に基づいて、 IOPS/TB|GB の比率を維持します。比率が100 IOPS/GBの場合、100GBのデータが格納されている150GBのボリュームのスループットの上限は10、000 IOPSです。使用済みスペースの量が変わると、アダプティブQoSによって比率に応じてスループットの上限が調整されます。

ONTAP 9 5以降では、アプリケーションのI/Oブロックサイズを指定して、スループット制限をIOPSとMBpsの両方で表すことができます。MBps制限は、ブロックサイズにIOPS制限を掛けて計算されます。たとえば、32KのI/OブロックサイズでIOPSの制限が6144IOPS/TBの場合、MBpsの制限は192MBpsになります。

スループットの上限と下限の両方について、次の動作が想定されます。

- アダプティブQoSポリシーグループにワークロードを割り当てると、上限または下限がただちに更新されます。
- アダプティブQoSポリシーグループに含まれるワークロードのサイズを変更すると、上限または下限が約5分で更新されます。

更新を実行するには、スループットが少なくとも10 IOPS増加する必要があります。

アダプティブQoSポリシーグループは常に非共有です。定義されているスループットの上限または下限は、各メンバーワークロードに個別に適用されます。

ONTAP 9.6以降では、SSDを使用するONTAP Select Premiumでスループットの下限がサポートされます。

アダプティブポリシーグループテンプレート

ONTAP 9.13.1以降では、アダプティブQoSテンプレートをSVMに設定できます。アダプティブポリシーグループテンプレートを使用すると、SVM内のすべてのボリュームにスループットの下限と上限を設定できます。

アダプティブポリシーグループテンプレートは、SVMの作成後にのみ設定できます。 `vserver modify`コマンドでパラメータを指定し `-qos-adaptive-policy-group-template`て、ポリシーを設定します。

アダプティブポリシーグループテンプレートを設定すると、ポリシーの設定後に作成または移行されたボリュームには自動的にポリシーが継承されます。ポリシーテンプレートを割り当てても、SVM上の既存のボリュームには影響しません。SVMでポリシーを無効にすると、以降SVMに移行または作成されたボリュームにポリシーは適用されません。アダプティブポリシーグループテンプレートを無効にしても、ポリシーテンプレートが保持されるため、そのポリシーテンプレートを継承したボリュームには影響しません。

詳細については、を参照してください アダプティブポリシーグループテンプレートの設定。

一般的なサポート

次の表に、スループットの上限、スループットの下限、およびアダプティブQoSのサポートの違いを示します。

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 **v2**	アダプティブ**QoS**
ONTAP 9バージョン	すべて	9.2以降	9.7以降	9.3以降
プラットフォーム	すべて	• AFF • C190[1] • SSDを使用したONTAP Select Premium [1]	• AFF • C190 • SSDを使用したONTAP Select Premium	すべて

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 **v2**	アダプティブ**QoS**
プロトコル	すべて	すべて	すべて	すべて
FabricPool	○	○（階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合）	○（階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合）	いいえ
SnapMirror Synchronous	○	いいえ	いいえ	○

[1]C190とONTAP SelectのサポートはONTAP 9.6リリースから開始されました。

スループットの上限がサポートされるワークロード

次の表に、スループットの上限でサポートされるワークロードをONTAP 9のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロードのサポート	**ONTAP 9.8**以降	**ONTAP 9.7** から **9.4**	**ONTAP 9.3**以前
ボリューム	はい	はい	はい
ファイル	はい	はい	はい
LUN	はい	はい	はい
SVM	はい	はい	はい
FlexGroupボリューム	はい	はい	○（ONTAP 9.3のみ）
qtree [1]	はい	いいえ	いいえ
ポリシーグループごとに複数のワークロード	はい	はい	はい
非共有ポリシーグループ	はい	はい	いいえ

[1] ONTAP 9.9.1 以降では、SMB が有効になっているFlexVolおよびFlexGroupボリュームの qtree でも SMB アクセスがサポートされます。ONTAP 9.8以降では、NFSが有効なFlexVolおよびFlexGroupボリュームのqtreeでNFSアクセスがサポートされます。

スループットの下限がサポートされるワークロード

次の表に、スループットの下限がサポートされるワークロードをONTAP 9のバージョン別に示します。ルー

トボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロードのサポート	**ONTAP 9.3**	**ONTAP 9.4~9.7**	**ONTAP 9.8** から **9.13.0**	**ONTAP 9.13.1**以降
ボリューム	はい	はい	はい	はい
ファイル	はい	はい	はい	はい
LUN	はい	はい	はい	はい
SVM	いいえ	いいえ	いいえ	はい
FlexGroupボリューム	いいえ	はい	はい	はい
qtree [1]	いいえ	いいえ	はい	はい
ポリシーグループごとに複数のワークロード	いいえ	はい	はい	はい
非共有ポリシーグループ	いいえ	はい	はい	はい

[1] ONTAP 9.8以降では、NFSが有効なFlexVolおよびFlexGroupボリュームのqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVolおよびFlexGroupボリュームのqtreeでもSMBアクセスがサポートされます。

アダプティブ**QoS**がサポートされるワークロード

次の表に、アダプティブQoSがサポートされるワークロードをONTAP 9のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロードのサポート	**ONTAP 9.3**	**ONTAP 9.4** から **9.13.0**	**ONTAP 9.13.1**以降
ボリューム	はい	はい	はい
ファイル	いいえ	はい	はい
LUN	いいえ	はい	はい
SVM	いいえ	いいえ	はい
FlexGroupボリューム	いいえ	はい	はい
ポリシーグループごとに複数のワークロード	はい	はい	はい
非共有ポリシーグループ	はい	はい	はい

ワークロードとポリシーグループの最大数

次の表に、ワークロードとポリシーグループの最大数をONTAP 9のバージョン別に示します。

ワークロードのサポート	**ONTAP 9.3**以前	**ONTAP 9.4**以降
クラスタあたりの最大ワークロード	12,000	40,000
ノードあたりの最大ワークロード	12,000	40,000
ポリシーグループの最大数	12,000	12,000

ONTAPスループットフロア **v2** を有効または無効にする

AFFでスループットの下限v2を有効または無効にすることができます。デフォルトは有効です。下限v2を有効にすると、コントローラの使用率が高く、他のワークロードのレイテンシが高くなることを犠牲にして、スループットの下限を満たすことができます。下限v2は、QoSとアダプティブQoSの両方に適用されます。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のいずれかのコマンドを入力します。

状況	使用するコマンド
下限v2を無効にする	`qos settings throughput-floors-v2 -enable false`
下限v2を有効にする	`qos settings throughput-floors-v2 -enable true`

> MetroClusterクラスタでスループットの下限v2を無効にするには、
>
> `qos settings throughput-floors-v2 -enable false`
>
> ソースクラスタとデスティネーションクラスタの両方でコマンドを実行します。

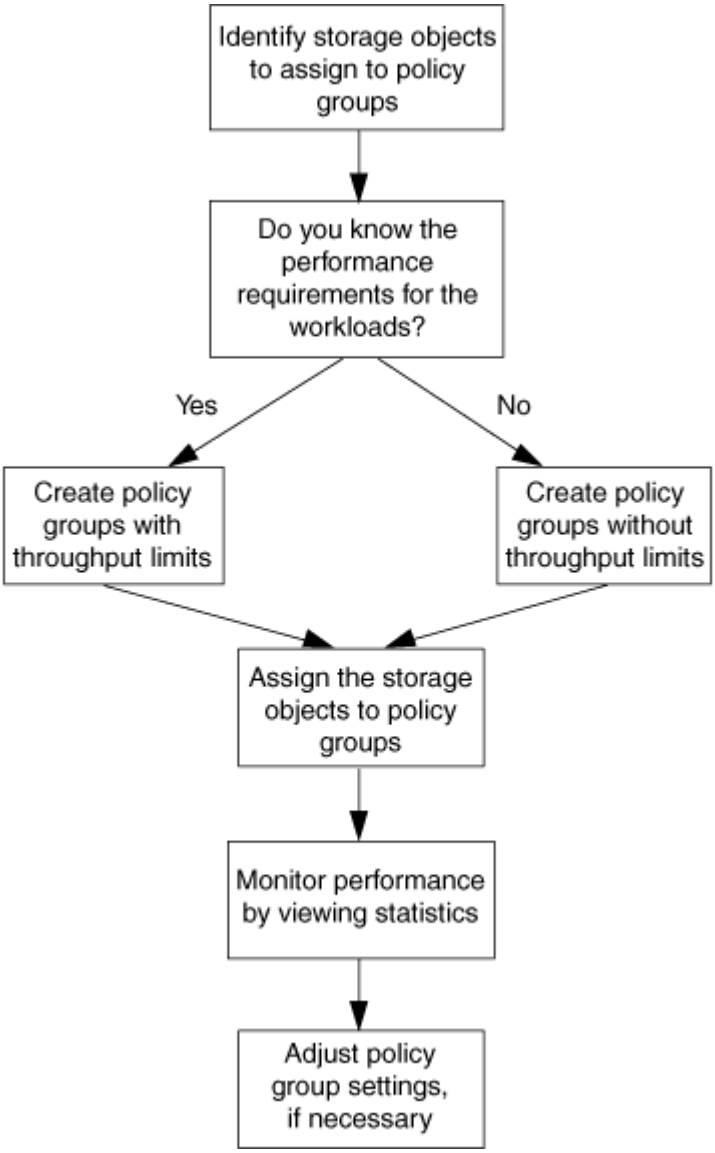
```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

の詳細については `qos settings throughput-floors-v2`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPストレージ **QoS** ワークフロー

QoS で管理するワークロードのパフォーマンス要件がすでにわかっている場合は、ポリ

シーグループを作成するときにスループットの制限を指定できます。それ以外の場合は、ワークロードを監視したうえで指定することができます。



ONTAPで**QoS**を使用したスループットの上限の設定

ポリシーグループのフィールドを使用して、ストレージオブジェクトのワークロードのスループットの上限（最大QoS）を定義できます `max-throughput`。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。

開始する前に

- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ポリシーグループをSVMに適用するには、クラスタ管理者である必要があります。

タスクの内容

- ONTAP 9.4 以降では、 _non-shared_QoS ポリシーグループを使用して、定義されたスループットの上限環境を各メンバーのワークロードごとに指定できます。ポリシーグループが _shared ：ポリシーグループに割り当てられているワークロードの合計スループットが指定した上限を超えることはできません。

共有されていないポリシーグループを指定するには、コマンドに `qos policy-group create`を設定します `-is-shared=false`。

- スループットの上限は、IOPS、MB/秒、またはIOPS、MB/秒で指定できます。IOPSとMBpsの両方を指定した場合は、先に上限に達した方が適用されます。

> ⓘ 同じワークロードに対して上限と下限を設定する場合は、スループット制限はIOPS単位でのみ指定できます。

- QoS制限の対象となるストレージオブジェクトは、ポリシーグループが属するSVMに含める必要があります。同じSVMに複数のポリシーグループを含めることができます。
- そのストレージオブジェクトまたは子オブジェクトがポリシーグループに属している場合、そのストレージオブジェクトをポリシーグループに割り当てることはできません。
- QoSのベストプラクティスとして、同じタイプのストレージオブジェクトにポリシーグループを適用することを推奨します。

手順

1. ポリシーグループを作成します。

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   の詳細については `qos policy-group create`、を"ONTAPコマンド リファレンス"参照してください。

   スループットの上限は、コマンドを使用して調整できます `qos policy-group modify`。

   次のコマンドは、最大スループットが5、000 IOPSの共有ポリシーグループを作成し `pg-vs1`ます。

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   次のコマンドは、最大スループットが100 IOPS、400KB/秒の非共有ポリシーグループを作成し `pg-vs3`ます。

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   次のコマンドは、スループットの制限がない非共有ポリシーグループを作成し `pg-vs4`ます。

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

   の詳細については `qos policy-group modify`、を"ONTAPコマンド リファレンス"参照してください。

2. ポリシーグループをSVM、ファイル、ボリューム、またはLUNに適用します。

   storage_object create -vserver *SVM* -qos-policy-group *policy_group*

   この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。コマンドを使用すると、ストレージオブジェクトに別のポリシーグループを適用できます *storage_object* modify。

   次のコマンドは、ポリシーグループをSVM `vs1`に適用し `pg-vs1`ます。

   ```
   cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
   ```

   次のコマンドは、ボリューム `app1`およびに `app2`ポリシーグループを適用し `pg-app`ます。

   ```
   cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
   -qos-policy-group pg-app
   ```

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app
   ```

3. ポリシーグループのパフォーマンスを監視します。

   qos statistics performance show

   の詳細については qos statistics performance show、を"ONTAPコマンド リファレンス"参照してください。

   > パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

   次のコマンドは、ポリシーグループのパフォーマンスを表示します。

   ```
   cluster1::> qos statistics performance show
   Policy Group           IOPS      Throughput   Latency
   -------------------- -------- --------------- ----------
   -total-                 12316       47.76MB/s  1264.00us
   pg_vs1                   5008       19.56MB/s     2.45ms
   _System-Best-Effort        62       13.36KB/s     4.13ms
   _System-Background         30           0KB/s        0ms
   ```

4. ワークロードのパフォーマンスを監視します。

   qos statistics workload performance show

パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
---------------- ------ -------- ---------------- ----------
-total-               -    12320        47.84MB/s  1215.00us
app1-wid7967       7967     7219        28.20MB/s   319.00us
vs1-wid12279      12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS      14       55        10.92KB/s   236.00us
_Scan_Backgro..    5688       20            0KB/s         0ms
```

の詳細については `qos statistics workload performance show`、を"ONTAPコマンド リファレンス"参照してください。

QoSワークロードの詳細なレイテンシ統計を表示するには、コマンドを使用し `qos statistics workload latency show`ます。の詳細については `qos statistics workload latency show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPで**QoS**を使用してスループットの下限を設定

ポリシーグループのフィールドを使用して、ストレージオブジェクトのワークロードのスループットの下限（最小QoS）を定義できます `min-throughput`。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。ONTAP 9 8以降では、スループットの下限をIOPS、MBps、またはIOPS/MBpsで指定できます。

開始する前に

- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ONTAP 9.13.1以降では、を使用してSVMレベルでスループットの下限を適用できますアダプティブポリシーグループテンプレート。QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。

タスクの内容

- ONTAP 9.4 以降では、 _non-shared_qos ポリシーグループを使用して、定義したスループットの下限を各メンバーワークロードに個別に適用するように指定できます。これは、スループットの下限が設定されたポリシーグループを複数のワークロードに適用できる唯一の条件です。

  共有されていないポリシーグループを指定するには、コマンドに `qos policy-group create`を設定します `-is-shared=false`。

- ノードまたはアグリゲートに十分なパフォーマンス容量（ヘッドルーム）がない場合、ワークロードのスループットが指定された下限を下回ることがあります。
- QoS制限の対象となるストレージオブジェクトは、ポリシーグループが属するSVMに含める必要があります。同じSVMに複数のポリシーグループを含めることができます。

- QoSのベストプラクティスとして、同じタイプのストレージオブジェクトにポリシーグループを適用することを推奨します。
- スループットの下限が定義されたポリシーグループは、SVMには適用できません。

手順

1. の説明に従って、ノードまたはアグリゲートに十分なパフォーマンス容量があることを確認します。
2. ポリシーグループを作成します。

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   の詳細については `qos policy-group create`、を"ONTAPコマンド リファレンス"参照してください。

3. スループットの下限を調整するには、コマンドを使用し `qos policy-group modify`ます。

   次のコマンドは、最小スループットが1、000 IOPSの共有ポリシーグループを作成し `pg-vs2`ます。

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   次のコマンドは、スループットの制限がない非共有ポリシーグループを作成し `pg-vs4`ます。

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

   の詳細については `qos policy-group modify`、を"ONTAPコマンド リファレンス"参照してください。

4. ポリシーグループをボリュームまたはLUNに適用します。

   `*storage_object* create -vserver *SVM* -qos-policy-group *policy_group*`使用することができます `_storage_object_modify`ストレージ オブジェクトに別のポリシー グループを適用するコマンド。

   次のコマンドは、ポリシーグループをボリューム `app2`に適用し `pg-app2`ます。

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

   この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

5. ポリシーグループのパフォーマンスを監視します。

   `qos statistics performance show`

パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

の詳細については `qos statistics performance show`、を"ONTAPコマンド リファレンス"参照してください。

6. ワークロードのパフォーマンスを監視します。

`qos statistics workload performance show`

パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

の詳細については `qos statistics workload performance show`、を"ONTAPコマンド リファレンス"参照してください。

QoSワークロードの詳細なレイテンシ統計を表示するには、コマンドを使用し `qos statistics workload latency show`ます。の詳細については `qos statistics workload latency show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPでアダプティブ**QoS**ポリシーグループを使用する

アダプティブ QoS ポリシーグループを使用すると、ボリュームサイズの変更に合わせてスループットの上限や下限を自動的に調整し、 TB または GB あたりの IOPS を一定に

保つことができます。これは、数百、数千のワークロードを管理する大規模な環境では大きなメリットです。

開始する前に

- ONTAP 9.3以降が実行されている必要があります。アダプティブQoSポリシーグループは、ONTAP 9以降で使用できます。3.
- ポリシーグループを作成するには、クラスタ管理者である必要があります。

タスクの内容

ストレージオブジェクトはアダプティブポリシーグループまたは非アダプティブポリシーグループのメンバーにすることはできますが、両方のメンバーにすることはできません。SVMはストレージオブジェクトとポリシーで同じである必要があります。ストレージオブジェクトはオンラインである必要があります。

アダプティブQoSポリシーグループは常に非共有です。定義されているスループットの上限または下限は、各メンバーワークロードに個別に適用されます。

ストレージオブジェクトサイズに対するスループット制限の比率は、次のフィールドの組み合わせによって決まります。

- `expected-iops`は、割り当て済み（TB / GB）あたりの最小想定IOPSです。

> `expected-iops`は、AFFプラットフォームでのみ保証されます。`expected-iops`FabricPoolについては、階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合にのみ保証されます。`expected-iops`は、SnapMirror同期関係にないボリュームに対して保証されます。

- `peak-iops`は、割り当て済みまたは使用済み（TB / GB）あたりの最大IOPSです。
- `expected-iops-allocation`expected-iopsに割り当てスペース（デフォルト）と使用スペースのどちらを使用するかを示します。

> `expected-iops-allocation`ONTAP 9 .5以降で使用できます。ONTAP 9 .4以前ではサポートされていません。

- peak-iops-allocation`に割り当てスペースと使用済みスペース（デフォルト）のどちらを使用するかを示します `peak-iops。
- absolute-min-iops`は、絶対最小IOPSです。このフィールドは、非常に小さいストレージオブジェクトで使用できます。が計算値より大きい場合は `absolute-min-iops、および/または `expected-iops`の両方が `expected-iops`上書きされ `peak-iops`ます。

  たとえば、TBあたり1、000 IOPS/TBに設定した場合、ボリュームサイズが1GB未満の場合は expected-iops、フラクショナルIOPが計算され `expected-iops`ます。計算された割合は `peak-iops`さらに小さい割合になります。これを回避するには、を現実的な値に設定し `absolute-min-iops`ます。

- `block-size`アプリケーションI/Oブロックサイズを指定します。デフォルトは32Kです。有効な値は、8K、16K、32K、64K、ANYです。anyは、ブロックサイズが適用されないことを意味します。

次の表に示す3つのデフォルトのアダプティブQoSポリシーグループがあります。これらのポリシーグループはボリュームに直接適用できます。

デフォルトのポリシーグループ	想定IOPS/TB	最大IOPS/TB	絶対最小 IOPS
`extreme`	6,144	12,288	1000
`performance`	2,048	4,096	500
`value`	128	512	75

そのストレージオブジェクトまたは子オブジェクトがポリシーグループに属している場合、そのストレージオブジェクトをポリシーグループに割り当てることはできません。次の表に、制限事項を示します。

割り当て内容	割り当てることができない項目
SVM	SVM に含まれているストレージオブジェクトのポリシーグループへの割り当て
ボリューム	そのボリュームを含むSVMまたは子LUN
LUN	そのLUNを含むボリュームまたはSVM
ファイル	そのファイルを含むボリュームまたはSVM

手順

1. アダプティブQoSポリシーグループを作成します。

   ```
   qos adaptive-policy-group create -policy group policy_group -vserver SVM
   -expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
   -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
   space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
   ```

   の詳細については `qos adaptive-policy-group create`、を"ONTAPコマンド リファレンス"参照してください。

   > ℹ `-expected-iops-allocation`および `-block-size`は、ONTAP 9 .5以降で使用できます。これらのオプションは、ONTAP 9 .4以前ではサポートされていません。

   次のコマンドは、300 IOPS/TB `-peak-iops`、1、000 IOPS/TB、、 `used-space`および `-absolute-min-iops`50 IOPSに設定され `-peak-iops-allocation`た `-expected-iops`アダプティブQoSポリシーグループを作成し `adpg-app1`ます。

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. アダプティブQoSポリシーグループをボリュームに適用します。

   `volume create -vserver SVM -volume volume -aggregate aggregate -size number_of TB|GB -qos-adaptive-policy-group policy_group`

   の詳細については `volume create`、を"ONTAPコマンド リファレンス"参照してください。

   次のコマンドは、アダプティブQoSポリシーグループをボリューム `app1`に適用し `adpg-app1`ます。

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

   次のコマンドは、デフォルトのアダプティブQoSポリシーグループを新しい `app4`ボリュームと既存のボリューム `app5`に適用し `extreme`ます。ポリシーグループに対して定義されたスループットの上限は、ボリュームに `app5`個別に適用され `app4`ます。

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

ONTAPでアダプティブポリシーグループテンプレートを設定する

ONTAP 9.13.1以降では、アダプティブポリシーグループテンプレートを使用して、SVMレベルでスループットの下限と上限を適用できます。

タスクの内容

- アダプティブポリシーグループテンプレートはデフォルトポリシーです `apg1`。ポリシーはいつでも変更できます。CLIまたはONTAP REST APIでのみ設定でき、既存のSVMにのみ適用できます。
- アダプティブポリシーグループテンプレートは、ポリシーの設定後にSVMで作成またはSVMに移行されるボリュームにのみ影響します。SVM上の既存のボリュームのステータスは維持されます。

  アダプティブポリシーグループテンプレートを無効にした場合、SVM上のボリュームの既存のポリシーは保持されます。無効化の影響を受けるのは、あとでSVMに作成または移行されたボリュームだけです。

- QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。
- アダプティブポリシーグループテンプレートは、AFFプラットフォーム向けに設計されています。アダプ

ティブポリシーグループテンプレートは他のプラットフォームでも設定できますが、ポリシーによって最小スループットが適用されない場合があります。同様に、FabricPoolアグリゲートまたは最小スループットをサポートしないアグリゲート内のSVMにアダプティブポリシーグループテンプレートを追加することもできますが、スループットの下限は適用されません。

- SVMがMetroCluster構成またはSnapMirror関係に含まれている場合は、ミラーされたSVMにアダプティブポリシーグループテンプレートが適用されます。

手順

1. SVMを変更してアダプティブポリシーグループテンプレートを適用します。
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. ポリシーが設定されたことを確認します。
   `vserver show -fields qos-adaptive-policy-group`

ONTAP Unified Managerでクラスタのパフォーマンスを監視する

Active IQ Unified Managerを使用すると、可用性を最大限に高め、NetApp AFFおよびFASのストレージインフラの制御を維持して、拡張性、サポート性、パフォーマンス、セキュリティを向上させることができます。

Active IQ Unified Managerはシステムの健全性を継続的に監視してアラートを送信するため、ITスタッフのリソースを解放できます。単一のダッシュボードからストレージのステータスを瞬時に確認し、推奨される対処方法に従って問題に迅速に対処できます。

検出と監視を行い、通知を受け取ることで、ストレージをプロアクティブに管理して迅速に問題を解決できるため、データ管理が簡易化されます。ペタバイト規模のデータを単一のダッシュボードから監視し、大規模なデータを管理できるため、管理効率が向上します。

Active IQ Unified Managerを使用すると、パフォーマンスデータと高度な分析を使用してパフォーマンスを最適化し、変動するビジネスニーズに対応できます。レポート機能を使用すると、標準のレポートにアクセスしたり、ビジネス固有のニーズに合わせてカスタムの運用レポートを作成したりできます。

関連リンク：

- "Active IQ Unified Managerの詳細はこちら"
- "Active IQ Unified Manager for VMwareの利用を開始する"
- "Active IQ Unified Manager for Linusの使用を開始する"
- "Active IQ Unified Manager for Windowsの使用を開始する"

ONTAP Data Infrastructure Insightsでクラスタのパフォーマンスを監視する

NetApp Data Infrastructure Insightsは、インフラ全体を可視化する監視ツールです。パブリッククラウドやプライベートデータセンターを含むすべてのリソースを監視、トラブルシューティング、最適化できます。

すべてのリソースを監視、トラブルシューティング、最適化

Data Infrastructure Insightsは、問題解決にかかる時間を大幅に短縮し、エンドユーザーへの影響を未然に防ぎます。また、クラウドインフラストラクチャのコスト削減にも役立ちます。実用的なインテリジェンスでデータを保護することで、内部脅威への露出を軽減します。

Data Infrastructure Insightsは、パブリッククラウドからデータセンターまで、ハイブリッドインフラストラクチャ全体を一元的に可視化します。特定のニーズに合わせてカスタマイズ可能なダッシュボードを瞬時に作成できます。また、組織のニーズに具体的かつ関連性の高い、ターゲットを絞った条件付きアラートも作成できます。

高度な異常検出機能により、問題が発生する前にプロアクティブに解決できます。リソースの競合や利用率の低下が自動的に表示されるため、影響を受けているワークロードをすばやくリストアできます。環境内のさまざまなコンポーネントの関係が自動的に階層化されて可視化されるため、迅速なトラブルシューティングが可能です。

環境全体から未使用のリソースや放置されたリソースを洗い出し、インフラの規模を適切に調整して全体的な支出を最適化する方法を探ることができます。

Data Infrastructure Insightsは、システムトポロジを視覚化し、Kubernetesアーキテクチャの理解を深めます。Kubernetesクラスターの健全性（問題のあるノードなど）を監視し、問題が見つかった場合は拡大表示できます。

Data Infrastructure Insights は、内部脅威に関する実用的な情報を提供する高度な機械学習と異常検出を通じて、悪意のあるユーザーや侵害を受けたユーザーによる組織のデータの悪用から保護するのに役立ちます。

Data Infrastructure InsightsはKubernetesメトリクスを可視化し、ポッド、ノード、クラスター間の関係を完全に把握するのに役立ちます。クラスターや稼働中のポッドの健全性、そして現在処理中の負荷を評価できるため、K8Sクラスターを自在に制御し、デプロイメントの健全性とコストの両方をコントロールできます。

関連リンク

- "データインフラストラクチャインサイトを使い始める"

監査ロギング

ONTAP監査ログ実装の詳細

監査ログに記録された管理アクティビティは標準のAutoSupportレポートに、特定のログアクティビティはEMSメッセージに含まれています。指定した宛先に監査ログを転送したり、 ONTAP CLI または Web ブラウザを使用して監査ログ ファイルを表示したりすることもできます。

ONTAP 9.11.1以降では、System Managerを使用して監査ログの内容を表示できます。

ONTAP 9.12.1以降には、監査ログの改ざんアラートが用意されています。audit.logファイルの改ざんをチェックするためのバックグラウンド ジョブが毎日実行され、変更または改ざんされたログ ファイルが見つかるとEMSアラートが送信されます。

ONTAP9.17.1以降、およびONTAP9.16.1 P4以降の9.16.1パッチリリース、 "クラスタ間操作を使用してピアクラスタから開始されたリモート管理アクティビティも記録できます。"。ユーザー主導の操作と、別のクラスターから発生する内部操作が含まれます。

ONTAPに記録された管理アクティビティ

ONTAP は、発行された要求、要求をトリガーしたユーザー、ユーザーのアクセス方法、要求の時刻など、クラスターで実行された管理アクティビティをログに記録します。

管理アクティビティは次のいずれかの種類になります。

- **SET**リクエスト:
  - これらの要求は通常、非表示のコマンドまたは操作に適用されます。
  - これらの要求は、 `modify` `delete`などのコマンドを実行したときに発行され `create`ます。
  - SET リクエストはデフォルトでログに記録されます。
- **GET**リクエスト:
  - これらのリクエストは情報を取得し、管理インターフェースに表示します。
  - これらの要求は、たとえばコマンドの実行時に発行され `show`ます。
  - GET要求はデフォルトではログに記録されませんが、 ONTAP CLIから送信されたGET要求をログに記録するかどうかを制御できます。 (`-cliget` ）、 ONTAP APIから(`-ontapiget` ）、またはONTAP REST APIから(`-httpget`) がファイルに記録されます。

監査ログの記録とローテーション

ONTAPの記録管理アクティビティ `/mroot/etc/log/mlog/audit.log`ノードのファイル。CLIコマンド用の3つのシェル（クラスタシェル、ノードシェル、非対話型システムシェル）からのコマンドとAPIコマンドがここに記録されます。対話型システムシェルのコマンドは記録されません。監査ログには、クラスタ内のすべてのノードが同期されているかどうかを示すタイムスタンプが含まれます。

> `audit.log`ファイルは、`AutoSupport`ツールによって指定された受信者に送信されます。また、`Splunk`や`syslog`サーバなど、指定した外部の送信先にコンテンツを安全に転送することもできます。

> `audit.log`ファイルは`1`日単位でローテーションされます。サイズが`100MB`に達したときにもローテーションが実行され、以前の`48`個のコピーが保持されます（最大合計ファイル数は`49`）。監査ファイルのローテーションが`1`日単位で実行される場合、`EMS`メッセージは生成されません。監査ファイルのサイズ制限を超えたためにローテーションが実行された場合は、`EMS`メッセージが生成されます。

GET監査を有効にする際は、急速なログローテーションによるデータ損失を防ぐため、ログ転送の設定を検討してください。詳細については、以下のナレッジベースの記事をご覧ください。 "監査ログ転送を有効にする" 。

ONTAP監査ログの変更について

ONTAP 9以降では `command-history.log`、ファイルがに置き換えられ `audit.log`、`mgwd.log`ファイルには監査情報が含まれなくなります。ONTAP 9にアップグレードする場合は、従来のファイルとその内容を参照するスクリプトやツールを確認する必要があります。

ONTAP 9へのアップグレード後も、既存の `command-history.log`ファイルは保持されます。新しいファイルがローテーションされる（作成される）と同時にローテーションアウト（削除）され `audit.log`ます。

アップグレード時にからへの `audit.log`ソフトリンクが作成されるため、ファイルをチェックするツールやスクリプトが `command-history.log`引き続き機能する場合があります `command-history.log`。ただし、ファイルには監査情報が含まれなくなるため、ファイルをチェックするツールやスクリプト `mgwd.log`は失敗します。

また、ONTAP 9以降の監査ログでは、次のエントリは有用ではないとみなされ、不要なロギングアクティビティの原因となるため、記録されなくなりました。

- ONTAPによって実行される内部コマンド（username=root）
- コマンドのエイリアス（元のコマンドとは別に）

ONTAP 9以降では、TCPプロトコルおよびTLSプロトコルを使用して、監査ログを外部の宛先に安全に送信できます。

ONTAP監査ログの内容を表示します。

ONTAP CLI、System Manager、またはWebブラウザを使用して、クラスタのファイルの内容を表示できます `/mroot/etc/log/mlog/audit.log`。

クラスタのログファイルのエントリは次のとおりです。

時間
: ログエントリのタイムスタンプ。

アプリケーション
: クラスタへの接続に使用するアプリケーション。指定可能な値の例は `internal`、、 `console` `ssh` `http` `ontapi`、、、 `snmp`、 `rsh` `telnet`、、および `service-processor`。

ユーザ
: リモートユーザのユーザ名。

都道府県
: 監査要求の現在の状態。、 `pending`、、のいずれ `error`かです `success`。

メッセージ
: コマンドのステータスに関するエラーまたは追加情報 を含むオプションのフィールド。

セッション**ID**
: 要求を受信したセッションID。各SSH_SESSION_ISにはセッションIDが割り当てられ、各HTTP、ONTAPI、またはSNMP_REQUESTには一意のセッションIDが割り当てられます。

Storage VM
: ユーザの接続に使用するSVM。

適用範囲

要求がデータStorage VM上にある場合に表示され `svm`、それ以外の場合はと表示されます。 `cluster`

コマンド**ID**

CLIセッションで受信した各コマンドのID。これにより、要求と応答を関連付けることができます。ZAPI、HTTP、SNMPの各要求にはコマンドIDはありません。

クラスタのログエントリは、ONTAP CLIとWebブラウザを使用して表示できます。また、.11.1以降ではONTAP 9からも表示できます。

System Manager

- インベントリを表示するには、[* Events & Jobs]>[Audit Logs]を選択します。+各列には、カテゴリのフィルタ、ソート、検索、表示、およびインベントリを行うためのコントロールがあります。インベントリの詳細はExcelブックとしてダウンロードできます。
- フィルターを設定するには、右上の*フィルター*ボタンをクリックして、目的のフィールドを選択します。+セッションIDリンクをクリックして、失敗が発生したセッションで実行されたすべてのコマンドを表示することもできます。

CLI

クラスタ内の複数のノードからマージされた監査エントリを表示するには、次のように入力します。+ `security audit log show <[parameters]>`

コマンドを使用すると、個 々 のノードの監査エントリを表示したり、クラスタ内の複数のノードの監査エントリをマージしたりできます `security audit log show`。Webブラウザを使用して、単一のノードのディレクトリの内容を表示することもできます `/mroot/etc/log/mlog`。の詳細については `security audit log show`、を"ONTAPコマンド リファレンス"参照してください。

Webブラウザ

Webブラウザを使用して、単一のノードのディレクトリの内容を表示できます `/mroot/etc/log/mlog`。"Webブラウザを使用してノードのログファイル、コアダンプファイル、およびMIBファイルにアクセスする方法について説明します。"です。

ONTAP監査GET要求設定を管理します。

set要求はデフォルトで記録されますが、get要求は記録されません。ただし、ONTAP HTML(`-httpget`）、ONTAP CLI(`-cliget`）、またはONTAP APIから送信されたGET要求(`-ontapiget`をファイルに記録するかどうかは制御できます。

監査ログの設定は、ONTAP CLI（ONTAP 9 .11.1以降）から変更できます。

System Manager

1. [* Events & Jobs]>[Audit Logs]を選択します。
2. 右上のをクリックし ⚙ 、追加または削除するリクエストを選択します。

CLI

- デフォルトのset要求に加えて、ONTAP CLIまたはAPIからのget要求を監査ログ（audit.logファイル）に記録するように指定するには、次のように入力します。+
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- 現在の設定を表示するには、次のように入力します。+
  `security audit show`

の詳細については `security audit show`、を"ONTAPコマンド リファレンス"参照してください。

ONTAPクラスタ間監査を有効にする

ONTAP 9.17.1以降、およびONTAP 9.16.1 P4以降の9.16.1パッチリリースでは、ONTAPでクラスタ間監査を有効にして、ピアクラスタから開始された操作をログに記録できます。このリモート監査は、複数のONTAPクラスタが相互に連携する環境で特に有用であり、リモートアクションの追跡可能性とアカウンタビリティを実現します。

クラスタ間監査では、ユーザーが開始したGET（読み取り）操作とSET（作成／変更／削除）操作を区別できます。デフォルトでは、宛先クラスタではユーザーが開始したSET操作のみが監査されます。GETやSETなどのデータ読み取りリクエストは、 `show` CLI のコマンドは、リクエストがクロス クラスタであるかどうかに関係なく、デフォルトでは監査されません。

開始する前に

- あなたは持っている必要があります `advanced`レベルの権限
- クラスタは別のクラスタとピアリングされている必要があり、両方のクラスタでONTAP 9.16.1 P4 以降が実行されている必要があります。

> ⓘ 一部のノードのみがONTAP 9.16.1 P4以降にアップグレードされている環境では、アップグレードされたバージョンを実行しているノードでのみ監査ログが記録されます。監査動作の一貫性を確保するため、すべてのノードをサポート対象バージョンにアップグレードすることをお勧めします。

クラスタ間監査を有効または無効にする

手順

1. クラスタ上でクラスタ間監査を有効（または無効）にするには、 `cluster-peer`パラメータを `on`または `off` ：

```
security audit modify -cluster-peer {on|off}
```

2. 現在の監査状態を確認して、クラスタ ピア設定が有効になっているか無効になっているかを確認します。

```
security audit show
```

応答：

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

GET監査を有効にした場合の効果

ONTAP 9.17.1以降では、 "CLI、HTTP、ONTAPI GET監査を有効にする"ピアクラスタでGET監査を有効にすると、クラスタ間のユーザ開始GET要求の監査も有効になります。以前のONTAPバージョンでは、GET監査はローカルクラスタの要求にのみ適用されていました。ONTAPONTAPでは、 `cluster-peer`オプション設定 `on`ローカル クラスター要求とクラスター間要求の両方が監査されます。

ONTAP監査ログのデスティネーションを管理します。

監査ログは最大で10箇所に転送できます。たとえば、Splunkやsyslogサーバにログを転送して、監視、分析、バックアップなどの目的で使用できます。

タスクの内容

転送を設定するには、syslogホストまたはSplunkホストのIPアドレス、ポート番号、転送プロトコル、転送ログに使用するsyslogファシリティを指定する必要があります。 "syslogファシリティについて説明します"です。

`-protocol`パラメータを使用して、次のいずれかの送信値を選択できます。

UDP暗号化なし
: セキュリティなしのUser Datagram Protocol（デフォルト）

TCP暗号化なし
: セキュリティなしの伝送制御プロトコル

TCP暗号化
: Transmission Control Protocol with Transport Layer Security（TLS）+ A * Verify server *オプションは、TCP暗号化プロトコルが選択されている場合に使用できます。

デフォルトのポートはUDPの場合は514、TCPの場合は6514ですが、ネットワークのニーズを満たす任意のポートを指定できます。

`-message-format`コマンドを使用すると、次のいずれかのメッセージ形式を選択できます。

レガシー**- NetApp**
RFC-3164 Syslog形式のバリエーション（形式：<PRIVAL> timestamp hostname：MSG）

RFC-5424
RFC-5424に基づくsyslog形式（形式：<PRIVAL> version timestamp hostname：MSG）

監査ログは、ONTAP CLIから転送できます。ONTAP 9 .11.1以降では、System Managerから転送できます。

System Manager

- 監査ログの送信先を表示するには、* Cluster > Settings *の順に選択します。+ログ送信先の数が*通知管理タイル*に表示されます。クリックする ⋮ と詳細が表示されます。
- 監査ログの送信先を追加、変更、または削除するには、[**Events & Jobs]>[Audit Logs]**を選択し、画面右上の**[*Manage Audit Destinations**]をクリックします。+をクリックする + Add か、*[ホストアドレス]*列内をクリックし ⋮ て、エントリを編集または削除します。

CLI

1. 監査ログの転送先ごとに、送信先のIPアドレスまたはホスト名、およびセキュリティオプションを指定します。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

   - コマンドがデスティネーションホストにpingを送信して接続を確認できない場合、 `cluster log-forwarding create`コマンドはエラーで失敗します。推奨されませんが、 `-force`パラメータを指定してコマンドを実行すると接続の検証が省略されます。
   - パラメータをに `true`設定する `-verify-server`と、ログの転送先の証明書を検証することでIDが検証されます。この値をに設定できる `true`のは、フィールドで値を `-protocol`選択した場合だけ `tcp-encrypted`です。

2. コマンドを使用して、送信先レコードが正しいことを確認し `cluster log-forwarding show`ます。

```
cluster1::> cluster log-forwarding show

                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

関連情報

- "cluster log-forwarding showの各コマンドを使用します"
- "cluster log-forwarding create"

AutoSupport

AutoSupportの詳細

ONTAP AutoSupportの詳細

AutoSupportは、システムヘルスをプロアクティブに監視し、NetAppテクニカルサポート、社内のサポート部門、およびサポートパートナーにメッセージを自動的に送信するメカニズムです。テクニカルサポートへのAutoSupportメッセージの送信はデフォルトで有効になりますが、メッセージを社内のサポート部門に送信するには、適切なオプションを設定し、有効なメールホストを指定する必要があります。

AutoSupport管理を実行できるのはクラスタ管理者だけです。Storage Virtual Machine（SVM）管理者にはAutoSupportへのアクセス権はありません。

AutoSupportは、ストレージシステムの初回設定時にデフォルトで有効になります。AutoSupportは、AutoSupportが有効になってから24時間後にテクニカルサポートへのメッセージ送信を開始します。この24時間を短縮するには、システムをアップグレードまたはリバートするか、AutoSupport設定を変更するか、システム時間を24時間以外に変更します。

> AutoSupportはいつでも無効にできますが、有効のままにしておく必要があります。AutoSupportを有効にすると、ストレージシステムに問題が発生した場合に、迅速に原因を特定して解決することができます。デフォルトでは、AutoSupportを無効にした場合でも、AutoSupportの情報が収集されてローカルに格納されます。

AutoSupportの詳細については、NetAppサポートサイトを参照してください。

関連情報

- "NetAppのサポート"
- "ONTAPコマンド リファレンス"

Digital AdvisorとONTAP AutoSupportの詳細

ONTAPのAutoSupportコンポーネントはテレメトリを収集し、分析用に送信します。Digital Advisorは、AutoSupportからのデータを分析し、プロアクティブなサポートと最適化を提供します。Digital Advisorは、人工知能を使用して潜在的な問題を特定し、ビジネスに影響が及ぶ前に問題を解決できるよう支援します。

Digital Advisorは、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体にわたってデータインフラを最適化します。SupportEdgeと有効な契約を結んでいるNetAppのすべてのお客様が、デジタルアドバイザによるデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Digital Advisorでできることは次のとおりです。

- アップグレードを計画する。Digital Advisorは、新しいバージョンのONTAPにアップグレードすることで解決できる環境内の問題を特定し、Upgrade Advisorコンポーネントがアップグレードの計画を支援します。

- システムの健全性を表示します。デジタルアドバイザのダッシュボードが健全性に関する問題を報告し、問題の修正を支援します。システム容量を監視して、ストレージスペースが不足しないようにします。システムのサポートケースを表示します。
- パフォーマンスの管理Digital Advisorでは、System Managerよりも長い期間のシステムパフォーマンスが表示されます。パフォーマンスに影響している構成やシステムの問題を特定します。
- 効率を最大化Storage Efficiencyの指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定できます。
- インベントリと構成を表示します。Digital Advisorは、完全なインベントリおよびソフトウェアとハードウェアの構成情報を表示します。サービス契約の有効期限を確認し、サポートを継続できるように更新してください。

関連情報

"NetAppのドキュメント：デジタルアドバイザ"

"Digital Advisorを起動"

"SupportEdgeサービス"

ONTAP AutoSupportメッセージが送信されるタイミングと場所を確認する

AutoSupport は、メッセージの種類に応じた宛先にメッセージを送信します。AutoSupportがメッセージを送信するタイミングと場所を把握しておくと、電子メールで受信するメッセージやデジタルアドバイザWebサイトに表示されるメッセージを理解するのに役立ちます。

特に指定がないかぎり、次の表に示す設定はコマンドのパラメータです `system node autosupport modify`。

イベントトリガー型メッセージ

対処が必要なシステムでイベントが発生すると、AutoSupportはイベントトリガー型メッセージを自動的に送信します。

メッセージが送信されたとき	メッセージの送信先
AutoSupportがEMSのトリガーイベントに応答する	および `-noteto`で指定されたアドレス `-to`。（送信されるのはサービスに影響する重要なイベントのみ）。 で指定されたアドレス `-partner-address` テクニカルサポート（がに設定されている `enable`場合） `-support`

スケジュールされたメッセージ

AutoSupport は、定期的に複数のメッセージを自動的に送信します。

メッセージが送信されたとき	メッセージの送信先
毎日（デフォルトでは、午前12時から午前1時の間にログメッセージとして送信されます）	で指定されたアドレス `-partner-address` テクニカルサポート（がに設定されている `enable` 場合） `-support`
Daily（デフォルトでは、パフォーマンスメッセージとして午前12：00から午前1：00の間に送信されます）（パラメータがに設定されて `true`いる場合） `-perf`	partner-address で指定されているアドレス テクニカルサポート（がに設定されている `enable` 場合） `-support`
毎週（デフォルトでは、日曜日の午前12時から午前1時まで送信されます）	で指定されたアドレス `-partner-address` テクニカルサポート（がに設定されている `enable` 場合） `-support`

手動でトリガーされるメッセージ

AutoSupportメッセージは、手動で開始または再送信できます。

メッセージが送信されたとき	メッセージの送信先
コマンドを使用して、手動でメッセージを送信したとき `system node autosupport invoke`	コマンドでパラメータを `system node autosupport invoke`使用してURIを指定する `-uri`と、そのURIにメッセージが送信されます。 `-uri`を省略すると、および `-partner-address`で指定したアドレスにメッセージが送信され `-to`ます。をに設定し `enable`た場合は、テクニカルサポートにもメッセージが送信され `-support`ます。

メッセージが送信されたとき	メッセージの送信先
コマンドを使用して、手動でメッセージを送信したとき `system node autosupport invoke-core-upload`	コマンドでパラメータ `system node autosupport invoke-core-upload`を使用してURIを指定する `-uri` と、そのURIにメッセージが送信され、コアダンプファイルがアップロードされます。 `-uri`コマンドでを省略する `system node autosupport invoke-core-upload`と、テクニカルサポートにメッセージが送信され、テクニカルサポートサイトにコアダンプファイルがアップロードされます。 どちらのシナリオでも、がに設定され `enable`、`-transport`がまたはに `http`設定されている `https`必要があります `-support`。 コアダンプファイルはサイズが大きいため、パラメータおよび `-partner-addresses`パラメータで指定したアドレスにメッセージが送信されません `-to`。
コマンドを使用して、手動でメッセージを送信したとき `system node autosupport invoke-performance-archive`	コマンドでパラメータを `system node autosupport invoke-performance-archive`使用してURIを指定する `-uri`と、そのURIにメッセージが送信され、パフォーマンスアーカイブファイルがアップロードされます。 `-uri`でを省略する `system node autosupport invoke-performance-archive`と、テクニカルサポートにメッセージが送信され、テクニカルサポートサイトにパフォーマンスアーカイブファイルがアップロードされます。 どちらのシナリオでも、がに設定され `enable`、`-transport`がまたはに `http`設定されている `https`必要があります `-support`。 パフォーマンスアーカイブファイルはサイズが大きいため、パラメータと `-partner-addresses`パラメータで指定したアドレスにメッセージが送信されません `-to`。

メッセージが送信されたとき	メッセージの送信先
コマンドを使用して、過去のメッセージを手動で再送信した場合 `system node autosupport history retransmit`	コマンドのパラメータ `system node autosupport history retransmit`で指定したURIのみに送信されます。 `-uri`

テクニカルサポートによってトリガーされるメッセージです

テクニカルサポートは、 AutoSupport OnDemand 機能を使用して、 AutoSupport からのメッセージを要求できます。

メッセージが送信されたとき	メッセージの送信先
AutoSupport が新しい AutoSupport メッセージを生成するという送信指示を取得したとき	で指定されたアドレス `-partner-address` テクニカルサポート（がに設定され、がに設定 `enable`されて `-transport`いる `https`場合） `-support`
過去の AutoSupport メッセージを再送信するという送信指示を AutoSupport が受け取ったとき	テクニカルサポート（がに設定され、がに設定 `enable`されて `-transport`いる `https`場合） `-support`
コアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードする新しい AutoSupport メッセージを生成するという送信指示を AutoSupport が受け取ったとき	がに設定され、がに設定 `enable`され `https`て `-transport`いる場合は、テクニカルサポート `-support`。テクニカルサポートサイトにコアダンプファイルまたはパフォーマンスアーカイブファイルがアップロードされます。

ONTAP AutoSupportイベントトリガー型メッセージの詳細

AutoSupportは、EMSがトリガーイベントを処理するとイベントトリガー型AutoSupportメッセージを作成します。イベントトリガー型AutoSupportメッセージは、対処が必要な問題について受信者にアラートを送信します。このメッセージには、問題に関連する情報のみが含まれています。含めるコンテンツとメッセージの受信者をカスタマイズできます。

AutoSupportでは、次のプロセスを使用してイベントトリガー型AutoSupportメッセージを作成し、送信します。

1. EMSがトリガーイベントを処理すると、EMSはAutoSupportに要求を送信します。

   トリガーイベントは、AutoSupportのデスティネーションとプレフィックスで始まる名前を含むEMSイベントです `callhome.`。

2. AutoSupportがイベントトリガー型AutoSupportメッセージを作成します。

   AutoSupportは、トリガーに関連付けられているサブシステムから基本情報とトラブルシューティング情報を収集して、トリガーイベントに関連する情報のみを含むメッセージを作成します。

各トリガーには、デフォルトのサブシステムのセットが関連付けられています。ただし、コマンドを使用して、追加のサブシステムをトリガーに関連付けることもできます `system node autosupport trigger modify`。

3. AutoSupportは `-noteto`、、 `-partner-address`、および `-support`パラメータを指定してコマンド `-to`で定義した受信者にイベントトリガー型AutoSupportメッセージを送信します `system node autosupport modify`。

   コマンドでパラメータと `-noteto`パラメータを指定する `-to`と、特定のトリガーに対するAutoSupportメッセージの配信を有効または無効にできます `system node autosupport trigger modify`。

特定のイベントについて送信されるデータの例

EMSイベントは、 `storage shelf PSU failed`必須、ログファイル、ストレージ、RAID、HA、プラットフォーム、およびネットワークサブシステムの基本データと、必須、ログファイル、およびストレージサブシステムのトラブルシューティングデータを含むメッセージをトリガーします。

今後のイベントへの応答として送信するAutoSupportメッセージにNFSに関するデータを含めることを決定します `storage shelf PSU failed`。イベントのNFSに関するトラブルシューティングレベルのデータを有効にするには、次のコマンドを入力し `callhome.shlf.ps.fault`ます。

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

`callhome.`プレフィックスは、コマンドを使用する場合、またはCLIのAutoSupportイベントやEMSイベントで参照される場合にイベント `system node autosupport trigger`から削除され `callhome.shlf.ps.fault`ます。

ONTAP AutoSupportメッセージの種類とその内容

AutoSupport メッセージには、サポートされているサブシステムに関するステータス情報が含まれていAutoSupportメッセージの内容を把握しておくと、電子メールで受信したメッセージやデジタルアドバイザWebサイトに表示されたメッセージを解釈したり、応答したりするのに役立ちます。

メッセージのタイプ	メッセージに含まれるデータのタイプ
イベントトリガー型	イベントが発生した特定のサブシステムに関するコンテキスト依存データが含まれるファイル
毎日	ログファイル
パフォーマンス	過去 24 時間以内にサンプリングされたパフォーマンスデータ

メッセージのタイプ	メッセージに含まれるデータのタイプ
毎週	設定データとステータスデータ
コマンドによるトリガー `system node autosupport invoke`	パラメータで指定した値によって異なり `-type`ます。 • `test`いくつかの基本データを含むユーザトリガー型メッセージを送信します。 また、オプションを使用すると、テクニカルサポートからの自動応答Eメールが指定したEメールアドレス宛てに送信される `-to`ため、AutoSupportメッセージが受信されていることを確認できます。 • `performance`パフォーマンスデータを送信します。 • `all`各サブシステムのトラブルシューティングデータを含む、週次メッセージと同様の一連のデータを含むユーザトリガー型メッセージを送信します。 通常、テクニカルサポートはこのメッセージを要求します。
コマンドによるトリガー `system node autosupport invoke-core-upload`	ノードのコアダンプファイル
コマンドによるトリガー `system node autosupport invoke-performance-archive`	指定された期間のパフォーマンスアーカイブファイル
AutoSupport OnDemand によってトリガーされます	AutoSupport OnDemand では、新しいメッセージまたは過去のメッセージを要求できます。 • 新しいメッセージは、AutoSupport収集のタイプに応じて、、 `all`または `performance`になります `test`。 • 過去のメッセージは、再送信されるメッセージの種類によって異なります。 AutoSupport OnDemandでは、次のファイルをNetAppサポートサイトにアップロードする新しいメッセージを要求できます "mysupport.netapp.com"。 • コアダンプ • パフォーマンスアーカイブ

ONTAP AutoSupportサブシステムの表示

各サブシステムは、AutoSupportがメッセージに使用する基本情報とトラブルシューティング情報を提供します。各サブシステムは、トリガーイベントに関連する情報のみをAutoSupportがサブシステムから収集できるトリガーイベントにも関連付けられています。

AutoSupportは状況に応じたコンテンツを収集します。

手順

1. サブシステムおよびトリガーイベントに関する情報を表示します。

```
system node autosupport trigger show
```

ONTAP AutoSupportのサイズ割当量と時間割当量について

AutoSupportは、サブシステム別に編成された情報を収集し、各サブシステムのコンテンツにサイズと時間の予算を適用します。ストレージシステムが拡大すると、AutoSupport予算によってAutoSupportペイロードが制御され、拡張性に優れたAutoSupportデータの配信が可能になります。

サブシステムのコンテンツがサイズまたは時間割当量を超えた場合、AutoSupportは情報の収集を停止し、AutoSupportコンテンツを切り捨てます。コンテンツを簡単に切り捨てることができない場合（バイナリファイルなど）、AutoSupportはコンテンツを省略します。

デフォルトのサイズ割当量と時間割当量の変更は、NetAppサポートから指示があった場合にのみ行ってください。コマンドを使用して、サブシステムのデフォルトのサイズ割当量と時間割当量を確認することもできます `autosupport manifest show`。

イベントトリガー型ONTAP AutoSupportメッセージで送信されるファイルに関する情報

イベントトリガー型AutoSupportメッセージには、AutoSupportがメッセージを生成する原因となったイベントに関連付けられたサブシステムからの基本情報とトラブルシューティング情報のみが含まれています。特定のデータは、NetAppサポートおよびサポートパートナーが問題のトラブルシューティングを行う際に役立ちます。

AutoSupportでは、イベントトリガー型AutoSupportメッセージの内容を制御するために、次の基準を使用します。

- 含まれているサブシステム

  データは、ログファイルなどの共通サブシステムや、RAIDなどの特定のサブシステムなどのサブシステムにグループ化されます。各イベントは、特定のサブシステムのデータのみを含むメッセージをトリガーします。

- 含まれている各サブシステムの詳細レベル

  含まれている各サブシステムのデータは、基本レベルまたはトラブルシューティングレベルで提供されま

す。

コマンドでパラメータを指定する `-instance`と、考えられるすべてのイベントを表示し、各イベントに関するメッセージにどのサブシステムが含まれているかを確認できます `system node autosupport trigger show`。

各イベントにデフォルトで含まれるサブシステムのほかに、コマンドを使用して、基本レベルまたはトラブルシューティングレベルでサブシステムを追加できます。 `system node autosupport trigger modify`

AutoSupportメッセージで送信されるログファイル

AutoSupportメッセージには、テクニカルサポート担当者が最近のシステムアクティビティを確認できるように、複数の主要ログファイルを含めることができます。

ログファイルサブシステムが有効になっている場合は、すべてのタイプの AutoSupport メッセージに次のログファイルが含まれる可能性があります。

ログファイル	ファイルから含まれているデータの量
• ディレクトリのログファイル `/mroot/etc/log/mlog/` • messagesログファイル	最後のAutoSupportメッセージ以降にログに追加された、指定された最大数までの新しい行のみ。これにより、AutoSupportメッセージには重複しない固有の関連データが含まれます。 （パートナーからのログファイルは例外です。パートナーの場合は、最大許容データが含まれます）。
• ディレクトリのログファイル `/mroot/etc/log/shelflog/` • ディレクトリのログファイル `/mroot/etc/log/acp/` • Event Management System （ EMS ；イベント管理システム）ログデータ	指定された最大値までの最新のデータ行。

AutoSupport メッセージの内容は、 ONTAP のリリースによって変わる場合があります。

週単位の**AutoSupport**メッセージで送信されるファイル

週単位のAutoSupportメッセージには、追加の設定データやステータスデータが含まれており、時間の経過に伴うシステム内の変更の追跡に役立ちます。

週単位のAutoSupportメッセージでは、次の情報が送信されます。

- 各サブシステムに関する基本情報
- 選択したディレクトリファイルの内容 `/mroot/etc`
- ログファイル
- システム情報を提供するコマンドの出力

- レプリケートされたデータベース（RDB）情報、サービス統計情報などの追加情報

ONTAP AutoSupport OnDemandがテクニカルサポートから配信指示を取得する方法を確認する

AutoSupport OnDemandは、定期的にテクニカルサポートとの通信を行い、AutoSupportメッセージの送信、再送信、拒否、および大容量ファイルのNetAppサポートサイトへのアップロードに関する送信指示を受け取ります。AutoSupport OnDemandを使用すると、週単位のAutoSupportジョブの実行を待たずに、AutoSupportメッセージをオンデマンドで送信できます。

AutoSupport OnDemandは、次のコンポーネントで構成されています。

- 各ノードで実行されるAutoSupport OnDemandクライアント
- テクニカルサポートで稼働するAutoSupport OnDemandサービス

AutoSupport OnDemandクライアントは、AutoSupport OnDemandサービスを定期的にポーリングし、テクニカルサポートから配信指示を取得します。たとえば、テクニカルサポートは、AutoSupport OnDemandサービスを使用して、新しいAutoSupportメッセージの生成を要求できます。AutoSupport OnDemandクライアントがAutoSupport OnDemandサービスをポーリングすると、クライアントは配信指示を取得し、要求に応じて新しいAutoSupportメッセージをオンデマンドで送信します。

AutoSupport OnDemandはデフォルトで有効になっています。ただし、AutoSupport OnDemandがテクニカルサポートとの通信を継続するには、一部のAutoSupport設定が必要です。AutoSupport OnDemandは、次の要件が満たされると、自動的にテクニカルサポートと通信します。

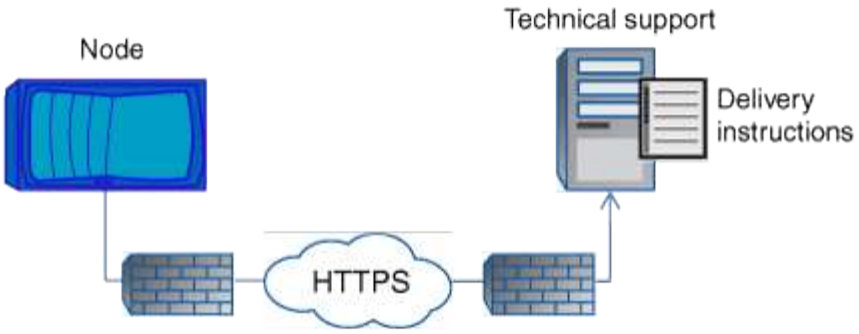
- AutoSupportが有効になっています。
- AutoSupportは、テクニカルサポートにメッセージを送信するように設定されています。
- HTTPS転送プロトコルを使用するようにAutoSupportが設定されている。

AutoSupport OnDemandクライアントは、AutoSupportメッセージの送信先と同じ場所のテクニカルサポートにHTTPS要求を送信します。AutoSupport OnDemandクライアントは、着信接続を受け入れません。

AutoSupport OnDemand は、「 AutoSupport 」ユーザーアカウントを使用してテクニカルサポートと通信します。ONTAPでは、このアカウントを削除できません。

AutoSupport OnDemandを無効にし、AutoSupportは有効なままにする場合は、コマンドを使用し `system node autosupport modify -ondemand-state disable`ます。の詳細については `system node autosupport modify -ondemand-state disable`、を"ONTAPコマンド リファレンス"参照してください。

次の図は、AutoSupport OnDemandがテクニカルサポートにHTTPS要求を送信して配信指示を取得する方法を示しています。



配信指示には、次のことを行うAutoSupportへの要求を含めることができます。

- 新しいAutoSupportメッセージを生成します。

  テクニカルサポートから、問題の優先順位付けに役立つ新しいAutoSupportメッセージが要求される場合があります。

- コアダンプファイルまたはパフォーマンスアーカイブファイルをNetAppサポートサイトにアップロードする新しいAutoSupportメッセージを生成します。

  問題の優先順位付けを支援するために、テクニカルサポートからコアダンプファイルやパフォーマンスアーカイブファイルを要求されることがあります。

- 以前に生成されたAutoSupportメッセージを再送信します。

  この要求は、配信エラーが原因でメッセージが受信されなかった場合に自動的に発生します。

- 特定のトリガーイベントに対するAutoSupportメッセージの配信を無効にします。

  テクニカルサポートによって、使用されていないデータの配信が無効になる場合があります。

Eメールで送信される**ONTAP AutoSupport**メッセージの構造について説明します。

AutoSupport メッセージを E メールで送信すると、メッセージには標準的な件名、簡単な本文、およびデータが含まれた 7z ファイル形式の大きな添付ファイルが含められます。

プライベートデータを非表示にするように AutoSupport が設定されている場合は、ヘッダー、件名、本文、添付ファイル内のホスト名などの特定の情報が省略されるか、マスクされます。

件名

AutoSupport メカニズムによって送信されたメッセージの件名行には、通知の理由を特定するテキスト文字列が含まれています。件名行の形式は次のとおりです。

HA グループ通知の送信元 _ システム _ 名前 _ （ _ メッセージ _ ） _ 重大度 _

- *System_Name* は、 AutoSupport の設定に応じてホスト名またはシステム ID です

本文

AutoSupport メッセージの本文には、次の情報が含まれます。

- メッセージの日付とタイムスタンプ
- メッセージを生成したノード上のONTAPのバージョン
- メッセージを生成したノードのシステムID、シリアル番号、およびホスト名
- AutoSupportシーケンス番号
- SNMP の連絡先名と場所（指定されている場合）
- HAパートナーノードのシステムIDとホスト名

添付ファイル

AutoSupportメッセージの重要な情報は、という名前の7zファイルに圧縮され、メッセージに添付されたファイルに含まれてい `body.7z`ます。

添付ファイルに含まれるファイルは、 AutoSupport メッセージのタイプに固有です。

ONTAP AutoSupportの重大度タイプについて

AutoSupportメッセージには、各メッセージの目的を理解するのに役立つ重大度タイプがあります。たとえば、緊急の問題にすぐに対処するためのメッセージや、情報提供のみを目的としたメッセージなどです。

メッセージには次のいずれかの重大度が設定されます。

- * 警告 * ：アラートメッセージは、何らかの処置を行わないと、より高いレベルのイベントが発生する可能性があることを示します。

  アラートメッセージに対しては、 24 時間以内に対処を行う必要があります。

- * 緊急 * ：システム停止が発生すると、緊急メッセージが表示されます。

  緊急メッセージに対しては、すぐに対処する必要があります。

- * エラー * ：エラー状態は、無視した場合に発生する可能性がある問題を示します。
- * 通知 * ：通常の状態だが重要な状態。
- * 情報 * ：情報メッセージは、問題に関する詳細情報を提供しますが、これは無視してかまいません。
- * デバッグ *: デバッグレベルのメッセージには、実行する必要がある手順が記載されています。

社内のサポート部門が AutoSupport メッセージを E メールで受信する場合、重大度は E メールメッセージの件名に表示されます。

ONTAP AutoSupportメッセージの説明を取得する

受信したAutoSupportメッセージの説明は、ONTAP Syslog Translatorで確認できます。

手順

1. に進みます"Syslog Translator"。
2. [リリース]フィールドに、使用しているONTAP のバージョンを入力します。検索文字列フィールドに「callhome」と入力します。[*平行移動（Translate）]を選択し
3. Syslog Translatorには、入力したメッセージ文字列に一致するすべてのイベントがアルファベット順に一覧表示されます。

ONTAP AutoSupportの管理用コマンド

AutoSupportの設定を変更または表示したり、以前のAutoSupportメッセージに関する情報を表示したり、AutoSupportメッセージを送信、再送信、またはキャンセルしたりするには、コマンドを使用し `system node autosupport`ます。

AutoSupportの設定

状況	使用するコマンド
AutoSupportメッセージを送信するかどうかを制御する	`system node autosupport modify`パラメータを指定した場合 `-state`
AutoSupportメッセージをテクニカルサポートに送信するかどうかを制御する	`system node autosupport modify`パラメータを指定した場合 `-support`
AutoSupportのセットアップまたはAutoSupportの設定の変更	`system node autosupport modify`
個 々 のトリガーイベントについて社内のサポート部門へのAutoSupportメッセージの有効化と無効化、および個 々 のトリガーイベントに応答して送信されるメッセージに含める追加のサブシステムレポートの指定	`system node autosupport trigger modify`

AutoSupport設定に関する情報を表示する

状況	使用するコマンド
AutoSupport設定を表示します。	`system node autosupport show`パラメータを指定した場合 `-node`
AutoSupportメッセージを受信するすべてのアドレスとURLの要約を表示する	`system node autosupport destinations show`
個 々 のトリガーイベントについて社内のサポート部門に送信されるAutoSupportメッセージを表示する	`system node autosupport trigger show`
AutoSupportの設定およびさまざまな宛先への配信のステータスを表示する	`system node autosupport check show`

状況	使用するコマンド
AutoSupportの設定およびさまざまな宛先への配信の詳細なステータスを表示する	`system node autosupport check show-details`

過去の**AutoSupport**メッセージに関する情報を表示する

状況	使用するコマンド
最新の50件のAutoSupportメッセージのうち1つ以上に関する情報を表示する	`system node autosupport history show`
テクニカルサポートサイトまたは指定したにコアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードするために生成された最新のAutoSupportメッセージに関する情報を表示する	`system node autosupport history show-upload-details`
AutoSupportメッセージ内の情報（メッセージ用に収集された各ファイルの名前とサイズ、エラーなど）を表示する	`system node autosupport manifest show`

AutoSupportメッセージの送信、再送信、またはキャンセル

状況	使用するコマンド
ローカルに保存されたAutoSupportメッセージを再送信します。このメッセージは、AutoSupportシーケンス番号で識別されます。 AutoSupportメッセージを再送信し、サポートがすでにそのメッセージを受信している場合、サポートシステムは重複するケースを作成しません。一方、サポートがそのメッセージを受信しなかった場合、AutoSupportシステムはメッセージを分析し、必要に応じてケースを作成します。	`system node autosupport history retransmit`
テストなどの目的で、AutoSupportメッセージを生成して送信します。 AutoSupportが無効になっている場合でも、パラメータを使用して `-force`メッセージを送信します。設定した送信先ではなく、指定した送信先にメッセージを送信するには、パラメータを使用し `-uri`ます。	`system node autosupport invoke`
AutoSupportメッセージをキャンセルする	`system node autosupport history cancel`

の詳細については `system node autosupport`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

"ONTAPコマンド リファレンス"

ONTAP AutoSupportマニフェストに含まれる情報の詳細

AutoSupport マニフェストでは、各 AutoSupport メッセージについて収集されるファイルの詳細が表示されます。AutoSupport マニフェストには、 AutoSupport が必要なファイルを収集できない場合の収集エラーに関する情報も含まれています。

AutoSupport マニフェストには次の情報が含まれています。

- AutoSupport メッセージのシーケンス番号
- AutoSupport メッセージに含まれている AutoSupport ファイル
- 各ファイルのサイズ（バイト単位）
- AutoSupport マニフェストによる収集のステータス
- 概要が 1 つ以上のファイルの収集に失敗した場合は、エラー AutoSupport

AutoSupportマニフェストを表示するには、コマンドを使用し `system node autosupport manifest show`ます。

AutoSupportマニフェストは、すべてのAutoSupportメッセージに含まれており、XML形式で表示されます。つまり、一般的なXMLビューアを使用して読むことも、デジタルアドバイザポータルを使用して表示することもできます。

計画

ONTAP AutoSupportを使用する準備

AutoSupportメッセージをNetAppに配信するようにONTAPクラスタを設定できます。その一環として、ローカルの（通常は組織内の）Eメール アドレスにメッセージのコピーを送信することもできます。使用可能なオプションを確認して、AutoSupportを設定する準備をしておく必要があります。

NetAppへのAutoSupportメッセージの配信

AutoSupportメッセージは、HTTPSまたはSMTPプロトコルを使用してNetAppに配信できます。ONTAP 9.15.1以降では、SMTPでTLSを使用することもできます。

> AutoSupport OnDemandとの通信および大容量ファイルのアップロードには、可能な限りHTTPSを使用してください。

次の点にも注意してください。

- AutoSupportメッセージに対して設定できる、NetAppへの配信チャネルは1つだけです。2つのプロトコルを使用してAutoSupportメッセージをNetAppに配信することはできません。

- AutoSupportでは、プロトコルごとに最大ファイル サイズが制限されます。AutoSupportメッセージのサイズが設定した制限を超えると、できる限り多くのメッセージが配信されますが、切り捨てが発生します。
- 必要に応じて、最大ファイル サイズを変更できます。の詳細については `system node autosupport modify`、を"ONTAPコマンド リファレンス"参照してください。
- どちらのプロトコルも、名前が解決されるアドレスファミリーに基づいて、IPv4またはIPv6経由で転送できます。
- AutoSupportメッセージを送信するためにONTAPによって確立されたTCP接続は、一時的で短命です。

HTTPS

これは最も堅牢な機能を提供します。次の点に注意してください。

- AutoSupport OnDemandと大容量ファイルの転送はサポートされません。
- 最初にHTTPS PUT要求が試行されます。要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。
- サーバがPUTをサポートしていない場合は、代わりにHTTPS POSTメソッドが使用されます。
- HTTPS転送のデフォルトの制限は50MBです。
- HTTPSプロトコルはポート443を使用します。

SMTP

原則として、SMTPを使用するのは、HTTPSが許可されていないかサポートされていない場合のみにしてください。次の点に注意してください。

- AutoSupport OnDemandと大容量ファイルの転送はサポートされません。
- SMTPサインイン クレデンシャルが設定されている場合は、暗号化されずにクリア テキストで送信されます。
- デフォルトの転送制限は5MBです。
- セキュアでないSMTPプロトコルはポート25を使用します。

TLSによるSMTPセキュリティの向上

SMTPを使用する場合、すべてのトラフィックは暗号化されず、簡単に傍受して読み取ることができます。ONTAP 9.15.1以降では、SMTP（SMTPS）でTLSを使用することもできます。この場合、TCP接続の確立後にセキュアチャネルをアクティブにする_explicit tls_が使用されます。

通常、SMTPSには次のポートが使用されます。ポート587

設定に関するその他の考慮事項

AutoSupportを設定する際は、さらにいくつかの考慮事項があります。

これらの考慮事項に関連するコマンドの詳細については、を参照してください"AutoSupportのセットアップ"。

電子メールを使用してローカルコピーを送信する

NetAppへのAutoSupportメッセージの配信に使用されるプロトコルに関係なく、各メッセージのコピーを1つ以上のローカルEメール アドレスに送信することもできます。たとえば、社内のサポート部門やパートナー組織にメッセージを送信できます。

SMTP（またはSMTPS）を使用してNetAppにメッセージを配信し、それらのメッセージのローカルEメール コピーも送信する場合は、同じEメール サーバ設定を使用します。

HTTPプロキシ

ネットワークの設定によっては、HTTPSプロトコルでプロキシURLの追加の設定が必要になる場合があります。テクニカルサポートへのAutoSupportメッセージの送信にHTTPSを使用していて、プロキシを使用している場合は、プロキシのURLを指定する必要があります。プロキシがデフォルト以外のポート（ポート3128）を使用する場合は、そのプロキシのポートを指定できます。必要に応じて、プロキシ認証のユーザ名とパスワードを指定することもできます。

サーバ証明書のインストール

TLS（HTTPSまたはSMTPS）では、サーバからダウンロードした証明書がルートCA証明書に基づいてONTAPによって検証されます。HTTPSまたはSMTPSを使用する前に、ルート証明書がONTAPにインストールされていること、およびONTAPがサーバ証明書を検証できることを確認する必要があります。この検証は、サーバ証明書に署名したCAに基づいて実行されます。

ONTAPには、豊富なルートCA証明書が事前にインストールされています。多くの場合、サーバの証明書は追加の設定なしでONTAPによってすぐに認識されます。サーバ証明書の署名方法によっては、ルートCA証明書と中間証明書のインストールが必要になる場合があります。

必要に応じて、次の手順に従って証明書をインストールします。必要な証明書はすべてクラスタレベルでインストールする必要があります。

例 **37.** 手順

System Manager

1. System Managerで、**[**クラスタ**]>***[設定]*を選択します。
2. [セキュリティ]*セクションまで下にスクロールします。
3. [証明書]*の横にあるを選択します → 。
4. タブで[追加]*をクリックします。
5. [インポート]*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて設定パラメータを設定します。
7. [追加]*をクリックします。

CLI

1. インストールを開始します。

```
security certificate install -type server-ca
```

の詳細については `security certificate install`、を"ONTAPコマンド リファレンス"参照してください。

2. 次のコンソール メッセージを探します。

```
Please enter Certificate: Press <Enter> when done
```

3. テキスト エディタで証明書ファイルを開きます。
4. 次の行を含めて、証明書全体をコピーします。

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. コマンド プロンプトの末尾に証明書を貼り付けます。
6. Enter*キーを押してインストールを完了します。
7. 次のいずれかのコマンドを実行して、証明書がインストールされていることを確認します。

```
security certificate show-user-installed
```

```
security certificate show
```

の詳細については `security certificate show`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "AutoSupportのセットアップ"
- "ONTAPコマンド リファレンス"

ONTAP AutoSupportのセットアップ

AutoSupportメッセージをNetAppテクニカルサポートに配信し、社内のサポート部門にEメールコピーを送信するようにONTAPクラスタを設定できます。その一環として、本番環境で使用する前に構成をテストすることもできます。

タスクの内容

ONTAP 9 .5以降では、クラスタのすべてのノードに対して同時にAutoSupportを有効にして設定できます。新しいノードがクラスタに追加されると、同じAutoSupport設定が自動的に継承されます。これをサポートするために、CLIコマンドの範囲は `system node autosupport modify`クラスタレベルです。 `-node`コマンドオプションは下位互換性のために保持されていますが、無視されます。

ONTAP 9 .4以前のリリースでは、コマンドは `system node autosupport modify`各ノードに固有です。クラスタでONTAP 9 .4以前を実行している場合は、クラスタ内の各ノードでAutoSupportを有効にして設定する必要があります。

開始する前に

AutoSupportメッセージをNetAppに配信するための推奨される転送設定はHTTPS（TLSを使用したHTTP）です。このオプションは、最も堅牢な機能と最高のセキュリティを提供します。

ONTAPクラスタを設定する前に、で詳細を確認してください"AutoSupportを使用する準備"。

手順

1. AutoSupportが有効になっていることを確認します。

```
system node autosupport modify -state enable
```

2. NetAppテクニカルサポートにAutoSupportメッセージを送信するには、次のコマンドを使用します。

```
system node autosupport modify -support enable
```

AutoSupportでAutoSupport OnDemandを使用できるようにする場合や、大容量ファイル（コアダンプファイルやパフォーマンスアーカイブファイルなど）をテクニカルサポートまたは指定のURLにアップロードする場合は、このオプションを有効にする必要があります。

AutoSupport OnDemandはデフォルトで有効になり、HTTPS転送プロトコルを使用してテクニカルサポートにメッセージを送信するように設定すると機能します。

3. NetAppテクニカルサポートによるAutoSupportメッセージの受信を有効にした場合は、メッセージに使用する転送プロトコルを指定します。

   次のオプションから選択できます。

状況	コマンドで設定するパラメータ `system node autosupport modify`
デフォルトのHTTPSプロトコルを使用する	a. をに `https`設定し `-transport`ます。 b. プロキシを使用する場合は、プロキシのURLをに設定し `-proxy-url`ます。この構成では、AutoSupport OnDemandとの通信および大容量ファイルのアップロードがサポートされます。
SMTPを使用	をに `smtp`設定し `-transport`ます。 この構成では、AutoSupport OnDemandや大容量ファイルのアップロードはサポートされません。

4. 社内のサポート部門やサポートパートナーにAutoSupportメッセージを送信するには、次の操作を実行します。

   a. 組織内の受信者を特定するには、コマンドの次のパラメータを設定し `system node autosupport modify`ます。

設定するパラメータ	パラメータの値
`-to`	重要なAutoSupportメッセージを受け取る社内サポート部門の、カンマで区切った5つまでの個別Eメールアドレスまたは配信リスト
`-noteto`	携帯電話やその他のモバイルデバイス用に設計された主要なAutoSupportメッセージの短縮版を受け取る社内サポート部門の、カンマで区切った5つまでの個別Eメールアドレスまたは配信リスト
`-partner-address`	すべてのAutoSupportメッセージを受信するサポートパートナー組織の、カンマで区切った5つまでの個別Eメールアドレスまたは配信リスト

   b. アドレスが正しく設定されていることを確認するには、コマンドを使用し `system node autosupport destinations show`ます。

5. 前の手順で社内のサポート部門の受信者アドレスを設定した場合、またはテクニカルサポートへのメッセージにSMTP転送を選択した場合は、コマンドの次のパラメータを設定してSMTPを設定し `system node autosupport modify`ます。

   ◦ 1つ以上のメールホストをカンマで区切って設定します。 `-mail-hosts`

     最大5つまで設定できます。

メールホスト名のあとにコロンとポート番号を指定することで、各メールホストのポート値を設定できます。たとえば、 `mymailhost.example.com:5678`5678はメールホストのポートです。

- を、AutoSupportメッセージを送信するEメールアドレスに設定します `-from`。

6. DNSを設定します。
7. 特定の設定を変更する場合は、必要に応じてコマンドオプションを追加します。

実行する処理	コマンドで設定するパラメータ `system node autosupport modify`
メッセージ内の機密データを削除、マスキング、またはエンコードしてプライベートデータを非表示にする	をに `true`設定し `-remove-private-data`ます。からに `true`変更する `false`と、すべてのAutoSupport履歴と関連ファイルが削除されます。
定期的なAutoSupportメッセージでのパフォーマンスデータの送信を停止する	をに `false`設定し `-perf`ます。

8. SMTPを使用してAutoSupportメッセージをNetAppに配信する場合は、オプションでTLSを有効にしてセキュリティを強化できます。
   a. 新しいパラメータに使用可能な値を表示します。

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

   b. SMTPメッセージ配信のTLSを有効にします。

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

   c. 現在の設定を表示します。

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. コマンドでパラメータを指定して `-node`、設定全体を確認します `system node autosupport show`。
10. コマンドを使用して、AutoSupportの処理を確認します `system node autosupport check show`。

    問題が報告された場合は、コマンドを使用し `system node autosupport check show-details`て詳細を確認します。

11. AutoSupportメッセージが送受信されていることをテストします。
    a. パラメータをに設定 `test`してコマンドを `-type`実行し `system node autosupport invoke`ます。

```
cluster1::> system node autosupport invoke -type test -node node1
```

b. NetAppがAutoSupportメッセージを受信していることを確認します。

```
system node autosupport history show -node local
```

適切なすべてのプロトコル宛先で、最新の発信AutoSupportメッセージのステータスがにに変わります `sent-successful`。

c. 必要に応じて、コマンドの、 `-noteto`または `-partner-address`パラメータ `system node autosupport modify`で設定したEメールアドレスを確認して、AutoSupportメッセージが社内のサポート部門またはサポートパートナーに送信されていることを確認します。 `-to`

関連情報

- "AutoSupportを使用する準備"
- "ONTAPコマンド リファレンス"

設定

ONTAP AutoSupport設定を管理します。

System Managerを使用して、AutoSupportアカウントの設定を管理できます。

System Managerで使用できない設定など、AutoSupportの設定オプションの詳細については、『』の "ONTAPコマンド リファレンス"を参照してください `system-node-autosupport-modify`。

AutoSupport設定の表示

System Managerを使用して、AutoSupportアカウントの設定を表示できます。

手順

1. System Manager で、 * Cluster > Settings * の順にクリックします。

「 * AutoSupport * 」セクションには、次の情報が表示されます。

- ステータス
- 転送プロトコル
- プロキシサーバ
- 送信元Eメールアドレス

2. セクションでを選択し、[その他のオプション（More Options）]*を選択します。

AutoSupport接続とEメール設定に関する追加情報が表示されます。また、メッセージの転送履歴も表示されます。

AutoSupportデータを生成して送信

System Managerでは、AutoSupportメッセージの生成を開始して、データを収集するクラスタノードを選択できます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. AutoSupport セクションでを選択し ⋮、 Generate and Send *を選択します。
3. 件名を入力します。
4. [データの収集元]*のチェックボックスをオンにして、データの収集元のノードを指定します。

AutoSupportへの接続をテストします。

System Managerからテストメッセージを送信して、AutoSupportへの接続を確認できます。

手順

1. System Manager で、 * Cluster > Settings * の順にクリックします。
2. AutoSupport セクションでを選択し ⋮、 Test Connectivity *を選択します。
3. メッセージの件名を入力します。

AutoSupportの有効化または無効化

AutoSupportは、可能性のある構成上の問題をプロアクティブに特定し、サポートケースを迅速に解決するなど、NetAppのお客様に実証済みのビジネスメリットを提供します。新しいシステムでは、AutoSupportはデフォルトで有効になっています。必要に応じて、System Managerを使用して、ストレージシステムのヘルスを監視して通知メッセージを送信するAutoSupportの機能を無効にすることができます。AutoSupportを無効にしたあとで、再度有効にすることができます。

タスクの内容

AutoSupportを無効にする前に、NetAppコールホームシステムをオフにすると、次の利点が失われることに注意してください。

- ヘルスモニタリング：AutoSupportはストレージシステムのヘルスを監視し、テクニカルサポートおよび社内のサポート部門に通知を送信します。
- 自動化：AutoSupportはサポートケースのレポートを自動化します。ほとんどのサポートケースは、お客様が問題に気付く前に自動的にオープンされます。
- 迅速な解決: AutoSupportデータを送信するシステムでは、AutoSupportデータを送信しないシステムと比較して、サポートケースが半分の時間で解決されます。
- アップグレードの高速化：AutoSupportは、System Managerのバージョンアップグレード、アドオン、更新、ファームウェア更新の自動化など、お客様のセルフサービスワークフローを強化します。
- その他の機能: NetAppコンソールの一部のワークフローなど、他のツールの特定の機能は、 AutoSupport が有効になっている場合にのみ動作します。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. AutoSupport セクションでを選択し ⋮、 Disable *を選択します。
3. AutoSupportを再度有効にする場合は、* AutoSupport セクションでを選択し ⋮、 Enable *を選択します。

サポートケースの生成を抑制

ONTAP 9 .10.1以降では、System Managerを使用してAutoSupportに要求を送信し、サポートケースが生成されないようにすることができます。

タスクの内容

サポートケースが生成されないようにするには、抑制を実行するノードと時間数を指定します。

システムのメンテナンス作業中にAutoSupportで自動ケースが作成されないようにするには、サポートケースを抑制すると特に便利です。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. セクションでを選択し、[サポートケース生成の抑制（Suppress Support Case Generation）]*を選択します。
3. 抑制を実行する時間数を入力します。
4. 抑制を実行するノードを選択します。

サポートケースの生成を再開する

ONTAP 9 .10.1以降では、System Managerを使用してAutoSupportからサポートケースの生成を再開できます（抑制されていた場合）。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [サポートケース生成（AutoSupport）]セクションでを選択し、*[サポートケース生成の再開（Resume Support Case Generation）]*を選択します。
3. 生成を再開するノードを選択します。

AutoSupport設定の編集

System Managerを使用して、AutoSupportアカウントの接続やEメールの設定を変更できます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. セクションでを選択し、[その他のオプション（More Options）]*を選択します。
3. [接続]セクションまたは[電子メール]セクションで、を選択し Edit ていずれかのセクションの設定を変更します。

関連情報

- "AutoSupportを使用する準備"
- "AutoSupportのセットアップ"

スケジュールされたメンテナンス時間中に**ONTAP AutoSupport**ケースが作成されないようにする

AutoSupportケース抑制を使用すると、スケジュールされたメンテナンス時間中にトリガーされるAutoSupportメッセージによって不要なケースが作成されないようにすることが

できます。

手順

1. テキスト文字列（はメンテナンス時間の長さ（時間））を使用して、AutoSupportメッセージを手動で呼び出します `MAINT=xh x` 。<node>を、AutoSupportメッセージの送信元ノードの名前に置き換えます。

```
system node autosupport invoke -node <node> -message MAINT=xh
```

関連情報

- "ONTAPコマンド リファレンス"
- "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"

AutoSupportを使用したファイルのアップロード

ONTAP AutoSupportコアダンプファイルのアップロード

コアダンプファイルが保存されると、イベントメッセージが生成されます。AutoSupportサービスが有効になっており、NetAppサポートにメッセージを送信するように設定されている場合は、AutoSupportメッセージが送信され、自動Eメール確認応答が送信されます。

開始する前に

- 次の設定でAutoSupportをセットアップしておきます。
  - ノードでAutoSupportが有効になっている。
  - AutoSupportは、テクニカルサポートにメッセージを送信するように設定されています。
  - HTTPS転送プロトコルを使用するようにAutoSupportが設定されている。

    大容量ファイル（コアダンプファイルなど）を含むメッセージを送信する場合、SMTP転送プロトコルはサポートされません。

タスクの内容

NetAppサポートから要求された場合は、コマンドを使用して、HTTPS経由のAutoSupportサービスを通じてコアダンプファイルをアップロードすることもできます `system node autosupport invoke-core-upload`。

"分析用にONTAP 9コアファイルをアップロードする方法"

手順

1. コマンドを使用して、ノードのコアダンプファイルを表示します `system node coredump show`。

   次の例では、ローカルノードのコアダンプファイルが表示されます。

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
--------- ------------------------------------------- -----
-----------------
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. コマンドを使用して、AutoSupportメッセージを生成し、コアダンプファイルをアップロードし `system node autosupport invoke-core-upload`ます。

   次の例では、 AutoSupport メッセージが生成されてデフォルトの場所（テクニカルサポート）に送信されます。コアダンプファイルは、NetApp Support Siteであるデフォルトの場所にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

   次の例では、 AutoSupport メッセージが生成され、 URI に指定した場所に送信されます。コアダンプファイルはその URI にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

ONTAP AutoSupportパフォーマンスアーカイブファイルのアップロード

パフォーマンスアーカイブを含むAutoSupportメッセージを生成して送信できます。デフォルトでは、NetAppテクニカルサポートにAutoSupportメッセージが送信され、パフォーマンスアーカイブがNetAppサポートサイトにアップロードされます。メッセージの送信先とアップロード先には別の場所を指定できます。

開始する前に

- 次の設定を使用してAutoSupportをセットアップしておく必要があります。
  - ノードでAutoSupportが有効になっている。
  - AutoSupportは、テクニカルサポートにメッセージを送信するように設定されています。
  - HTTPS転送プロトコルを使用するようにAutoSupportが設定されている。

    大容量ファイル（パフォーマンスアーカイブファイルなど）を含むメッセージを送信する場合、SMTP転送プロトコルはサポートされません。

タスクの内容

アップロードするパフォーマンスアーカイブデータの開始日を指定する必要があります。ほとんどのストレージシステムでは、パフォーマンスアーカイブが2週間保持されるため、2週間前までの開始日を指定できま

す。たとえば、今日が1月15日の場合は、1月2日の開始日を指定できます。

ステップ

1. コマンドを使用して、AutoSupportメッセージを生成し、パフォーマンスアーカイブファイルをアップロードし `system node autosupport invoke-performance-archive`ます。

   次の例では、2015年1月12日から4時間分のパフォーマンスアーカイブファイルがAutoSupportメッセージに追加され、デフォルトの場所（NetAppサポートサイト）にアップロードされます。

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   次の例では、2015年1月12日から4時間分のパフォーマンスアーカイブファイルがAutoSupportメッセージに追加され、URIで指定した場所にアップロードされます。

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

トラブルシューティング

メッセージが受信されない場合の**ONTAP AutoSupport**のトラブルシューティング

システムがAutoSupportメッセージを送信しない場合は、AutoSupportがメッセージを生成できないことが原因か、メッセージを配信できないことが原因かを判断できます。

手順

1. コマンドを使用して、メッセージの配信ステータスを確認します `system node autosupport history show`。
2. ステータスを確認します。

このステータスです	意味
初期化中	収集プロセスが開始しています。この状態が一時的なものであれば問題はありません。ただし、この状態が続く場合は問題があります。
収集-失敗	AutoSupportはスプールディレクトリにAutoSupportコンテンツを作成できません。AutoSupportが収集しようとしているものを表示するには、コマンドを入力し `system node autosupport history show -detail`ます。
収集を実行中	AutoSupportはAutoSupportのコンテンツを収集しています。AutoSupportが収集している情報を表示するには、コマンドを入力し `system node autosupport manifest show`ます。

このステータスです	意味
キューに登録済み	AutoSupportメッセージは配信のためにキューに登録されますが、まだ配信されていません。
送信中	AutoSupportは現在メッセージを配信しています。
送信済み-成功	AutoSupportはメッセージを正常に配信しました。AutoSupportがメッセージを配信した場所を確認するには、コマンドを入力し `system node autosupport history show -delivery`ます。
無視	AutoSupportにはメッセージの送信先がありません。配信の詳細を表示するには、コマンドを入力し `system node autosupport history show -delivery`ます。
再キュー	AutoSupportはメッセージの配信を試みましたが、失敗しました。その結果、AutoSupportは別の試行のためにメッセージを配信キューに戻しました。エラーを表示するには、コマンドを入力し `system node autosupport history show`ます。
トランスミッション-失敗	AutoSupportは、指定された回数のメッセージ配信に失敗し、メッセージ配信の試行を停止しました。エラーを表示するには、コマンドを入力し `system node autosupport history show`ます。
OnDemand -無視	AutoSupportメッセージは正常に処理されましたが、AutoSupport OnDemandサービスによって無視されました。

3. 次のいずれかを実行します。

をクリックします	手順
initializingまたはcollection-failed	AutoSupportでメッセージを生成できないため、NetAppサポートにお問い合わせください。次のナレッジベースの記事に言及します。 "AutoSupport の配信に失敗しました：ステータスが「初期化中にエラーが発生しました"
ignore、re-queued、またはtransmission failed	AutoSupportでメッセージを配信できないため、SMTP、HTTP、またはHTTPSのデスティネーションが正しく設定されていることを確認します。

HTTPS経由の**ONTAP AutoSupport**メッセージ配信のトラブルシューティング

予期したAutoSupportメッセージが送信されず、HTTPSを使用している場合、または自動更新機能が動作していない場合は、いくつかの設定を確認して問題を解決できます。

開始する前に

基本的なネットワーク接続とDNSルックアップを確認しておく必要があります。

- ノード管理LIFの動作ステータスと管理ステータスがupになっている必要があります。
- 同じサブネット上の機能しているホストに、（ノードのLIFではなく）クラスタ管理LIFからpingを実行できる必要があります。
- サブネットの外部の機能しているホストに、クラスタ管理LIFからpingを実行できる必要があります。
- サブネットの外部の機能しているホストに、（IPアドレスではなく）ホストの名前を使用してクラスタ管理LIFからpingを実行できる必要があります。

タスクの内容

以下の手順は、 AutoSupport でメッセージを生成できているが、 HTTPS 経由でメッセージを配信できていないと判断した場合に実行します。

この手順でエラーが発生した場合、または1つの手順を完了できない場合は、問題を特定して対処してから次の手順に進みます。

手順

1. AutoSupportサブシステムの詳細なステータスを表示します。

   ```
   system node autosupport check show-details
   ```

   これには、テストメッセージを送信してAutoSupportの送信先への接続を確認し、AutoSupport構成設定で発生する可能性のあるエラーのリストを提供することが含まれます。

2. ノード管理LIFのステータスを確認します。

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   `status-oper`フィールドと `status-admin`フィールドがに戻ります `up`。の詳細については `up`、をlink:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAPコマンド リファレンス"^]参照してください。

3. あとで使用できるように、SVM名、LIF名、およびLIFのIPアドレスをメモしておきます。
4. DNSが有効で正しく設定されていることを確認します。

   ```
   vserver services name-service dns show
   ```

5. AutoSupportメッセージから返されたエラーに対処します。

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

返されたエラーのトラブルシューティングについては、を参照してください"ONTAP AutoSupport（Transport HTTPSおよびHTTP）解決ガイド"。

6. クラスタが必要なサーバとインターネットの両方に正常にアクセスできることを確認します。

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > アドレス `support.netapp.com`自体はping / tracerouteに応答しませんが、ホップ単位の情報は重要です。

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   いずれかのルートが機能していない場合は、ほとんどのサードパーティ製ネットワーククライアントでまたは `tracert`ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください `traceroute`。その後、ネットワーク構成とクラスタ構成のどちらに問題があるかを確認できます。の詳細については `network traceroute`、を"ONTAPコマンド リファレンス"参照してください。

7. AutoSupport転送プロトコルにHTTPSを使用している場合は、HTTPSトラフィックがネットワークから出ることができることを確認します。

   a. クラスタ管理LIFと同じサブネットにWebクライアントを設定します。

      プロキシサーバ、ユーザ名、パスワード、ポートを含め、すべての設定パラメータの値がAutoSupport設定と同じであることを確認します。

   b. Webクライアントを使用してにアクセスし `https://support.netapp.com`ます。

      アクセスは成功するはずです。成功しない場合は、HTTPSトラフィックとDNSトラフィックを許可するようにすべてのファイアウォールが設定されていること、およびプロキシ サーバが正しく設定されていることを確認します。support.netapp.comの静的名前解決の設定の詳細については、"NetAppナレッジベース: support.netapp.com のONTAPに HOST エントリを追加するにはどうすればよいでしょうか?"

8. ONTAP 9.10.1以降で自動更新を有効にする場合は、次の追加URLへのHTTPS接続が確立されていることを確認してください。

   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

SMTP経由の**ONTAP AutoSupport**メッセージ配信のトラブルシューティング

システムが SMTP 経由で AutoSupport メッセージを配信できない場合は、いくつかの設定を確認することで問題を解決できます。

開始する前に

基本的なネットワーク接続とDNSルックアップを確認しておく必要があります。

- ノード管理LIFの動作ステータスと管理ステータスがupになっている必要があります。

- 同じサブネット上の機能しているホストに、（ノードのLIFではなく）クラスタ管理LIFからpingを実行できる必要があります。
- サブネットの外部の機能しているホストに、クラスタ管理LIFからpingを実行できる必要があります。
- サブネットの外部の機能しているホストに、（IPアドレスではなく）ホストの名前を使用してクラスタ管理LIFからpingを実行できる必要があります。

タスクの内容

以下の手順は、 AutoSupport でメッセージを生成できているが、 SMTP 経由でメッセージを配信できていないと判断した場合に実行します。

この手順でエラーが発生した場合、または1つの手順を完了できない場合は、問題を特定して対処してから次の手順に進みます。

特に指定がないかぎり、すべてのコマンドを ONTAP の CLI に入力します。

手順

1. ノード管理LIFのステータスを確認します。

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   `status-oper`フィールドと `status-admin`フィールドがに戻ります `up`。の詳細については `up`、をlink:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAPコマンド リファレンス"^]参照してください。

2. あとで使用できるように、SVM名、LIF名、およびLIFのIPアドレスをメモしておきます。
3. DNSが有効で正しく設定されていることを確認します。

   vserver services name-service dns show

4. AutoSupportで使用するように設定されているすべてのサーバを表示します。

   system node autosupport show -fields mail-hosts

   表示されたすべてのサーバ名を記録します。

5. 前の手順で表示された各サーバについて、および `support.netapp.com`ノードからサーバまたはURLにアクセスできることを確認します。

   network traceroute -node local -destination *server_name*

   これらのルートのいずれかが機能していない場合は、ほとんどのサードパーティ製ネットワーククライアントで検出された「 traceroute 」または「 tracert 」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これにより、ネットワーク構成とクラスタ構成のどちらに問題があるかを判断できます。

6. メールホストとして指定したホストにログインし、このホストが SMTP 要求を処理できることを確認します。

netstat -aAn|grep 25

`25`は、リスナーのSMTPポート番号です。

次のようなメッセージが表示されます。

```
ff64878c tcp        0      0  *.25    *.*    LISTEN.
```

7. 他のホストで、メールホストのSMTPポートを使用したTelnetセッションを開きます。

   telnet *mailhost* 25

   次のようなメッセージが表示されます。

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. Telnetのプロンプトで、メールホストからメッセージをリレーできることを確認します。

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name`は、ネットワークのドメイン名です。

   リレーが拒否されたことを示すエラーが返された場合は、メールホストでリレーが有効になっていません。システム管理者に問い合わせてください。

9. Telnetのプロンプトで、テストメッセージを送信します。

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   行の最後のピリオド（ . ）を単独で入力してください。このピリオドは、メッセージが完了したことをメールホストに示します。

   エラーが返された場合は、メールホストが正しく設定されていません。システム管理者に問い合わせてください。

10. ONTAPコマンドラインインターフェイスから、アクセス可能な信頼できる電子メールアドレスにAutoSupportテストメッセージを送信します。

    system node autosupport invoke -node local -type test

11. 試行のシーケンス番号を確認します。

    system node autosupport history show -node local -destination smtp

    タイムスタンプに基づいて、シーケンス番号を探します。これはおそらく最新の試みです。

12. テストメッセージのエラーを表示します。

    system node autosupport history show -node local -seq-num seq_num -fields error

    というエラーが表示された場合は `Login denied`、SMTPサーバがクラスタ管理LIFからの送信要求を受け入れていません。転送プロトコルとしてHTTPSを使用するように変更しない場合は、サイトのネットワーク管理者に連絡して、この問題に対処するためのSMTPゲートウェイの設定を依頼してください。

    このテストが成功しても mailto ： autosupport@netapp.com に同じメッセージが送信されない場合は、すべての SMTP メールホストで SMTP リレーが有効になっていることを確認するか、転送プロトコルとして HTTPS を使用してください。

    ローカルで管理されている E メールアカウントへのメッセージの送信も失敗する場合は、次の両方の条件に該当する添付ファイルを転送するように SMTP サーバが設定されていることを確認してください。

    - サフィックスが「 7z
    - MIME タイプが「 application/x-7x-compressed 」。

ONTAP AutoSupportサブシステムのトラブルシューティング

`system node check show`コマンドを使用すると、`AutoSupport`の設定と配信に関連する問題の検証とトラブルシューティングを行うことができます。

ステップ

1. 次のコマンドを使用して、 AutoSupport サブシステムのステータスを表示します。

使用するコマンド	作業
`system node autosupport check show`	AutoSupport HTTPSデスティネーション、AutoSupport SMTPデスティネーション、AutoSupport OnDemandサーバ、AutoSupport設定のステータスなど、AutoSupportサブシステムの全体的なステータスを表示する
`system node autosupport check show-details`	エラーの詳細な説明や対処方法など、 AutoSupport サブシステムの詳細なステータスを表示する

健全性の監視

ONTAPシステムの健常性監視の詳細

ヘルスモニタは、クラスタ内の特定の重大な状態をプロアクティブに監視し、障害やリスクを検出した場合にアラートを生成します。アクティブなアラートがある場合は、クラスタのヘルスステータスがデグレードと報告されます。アラートには、デグレード状態のシステムヘルスへの対応に必要な情報が含まれています。

ステータスがデグレードの場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を確認できます。問題を解決すると、システムのヘルスステータスは自動的にOKに戻ります。

システムのヘルスステータスには、複数のヘルスモニタが反映されます。個 々 のヘルスモニタのステータスがデグレードになると、システムヘルス全体のステータスがデグレードになります。

クラスタ内のシステムヘルスの監視におけるクラスタスイッチのサポート状況 ONTAP については、Hardware Universe を参照してください。

"Hardware Universe でサポートされるスイッチ"

クラスタスイッチヘルスモニタ（CSHM）AutoSupportメッセージの原因とアラートの解決に必要な対処方法の詳細については、技術情報アーティクルを参照してください。

"AutoSupport メッセージ：ヘルスモニタプロセス CSHM"

ONTAPの健全性監視コンポーネントの詳細

個々のヘルスモニタには、特定の条件に該当する場合にアラートをトリガーする一連のポリシーがあります。ヘルスモニタの仕組みを理解しておくと、問題に対応し、将来のアラートを制御するのに役立ちます。

ヘルスモニタは、次のコンポーネントで構成されています。

- 特定のサブシステムの個 々 のヘルスモニタ（各ヘルスモニタに独自のヘルスステータスがある）

  たとえば、ストレージサブシステムにはノード接続ヘルスモニタがあります。

- 個々のヘルスモニタのヘルスステータスを統合したシステム全体のヘルスモニタ

  1 つのサブシステムのステータスがデグレードになると、システム全体のステータスがデグレードになります。サブシステムにアラートがない場合、システム全体のステータスは OK です。

各ヘルスモニタは、次の主要な要素で構成されています。

- ヘルスモニタが発生させる可能性があるアラート

  各アラートには、アラートの重大度や原因の可能性などの詳細が定義されています。

- 各アラートをいつトリガーするかを特定するヘルスポリシー

各ヘルスポリシーには、アラートをトリガーする正確な条件または変更であるルール式があります。

ヘルスモニタは、サブシステム内のリソースの条件または状態の変化を継続的に監視し、検証します。条件または状態の変化がヘルスポリシーのルール式に一致すると、ヘルスモニタはアラートを生成します。アラートにより、サブシステムのヘルスステータスおよびシステム全体のヘルスステータスがデグレードします。

ONTAPのシステムヘルスアラートの対応について

システムヘルスアラートが発生したら、承認し、その詳細を確認し、原因となっている状況を修復して、再発しないようにすることができます。

ヘルスモニタからアラートが発せられた場合、次のいずれかの方法で対応できます。

- 影響を受けるリソース、アラートの重大度、考えられる原因、考えられる影響、対処方法など、アラートに関する情報を取得します。
- アラートが発生した時刻、他のユーザがすでにアラートを承認しているかどうかなど、アラートに関する詳細情報を取得します。
- 特定のシェルフやディスクなど、影響を受けるリソースまたはサブシステムの状態に関するヘルス関連の情報を取得します。
- アラートを承認して、問題に対応中のユーザがいることを示し、自分自身を「承認者」と指定します。
- ケーブル接続を修正して接続の問題を解決するなど、アラートに記載されている対処方法を実行して問題を解決します。
- アラートが自動的にクリアされなかった場合は削除します。
- サブシステムのヘルスステータスに影響しないように、アラートを抑制します。

  問題を把握した場合は、抑制が役に立ちます。アラートを抑制すると、そのアラートは引き続き発生する可能性がありますが、抑制されたアラートが発生すると、サブシステムのヘルスは「 ok-with-suppressed 」と表示されます。

ONTAPシステムヘルスアラートのカスタマイズの詳細

ヘルスモニタが生成するアラートを制御するには、アラートをいつトリガーするかを定義するシステムヘルスポリシーを有効または無効にします。これにより、特定の環境に合わせてヘルス監視システムをカスタマイズできます。

ポリシーの名前は、生成されたアラートの詳細情報を表示するか、特定のヘルスモニタ、ノード、またはアラートIDのポリシー定義を表示して確認できます。

ヘルスポリシーの無効化は、アラートの抑制とは異なります。アラートを抑制してもサブシステムのヘルスステータスには影響しませんが、アラートは引き続き発生する可能性があります。

ポリシーを無効にすると、ポリシールール式で定義されている条件または状態でアラートがトリガーされなくなります。

無効にするアラートの例

たとえば、役に立たないアラートが発生したとします。アラートのポリシーIDを取得するには、コマンドを使用し `system health alert show –instance`ます。ポリシーに関する情報を表示するには、コマンドでポリシ

ーIDを使用し `system health policy definition show`ます。ルール式やポリシーに関するその他の情報を確認したあと、ポリシーを無効にすることにしました。ポリシーを無効にするには、コマンドを使用し `system health policy definition modify`ます。

関連情報

- "system health alert show"

ONTAP AutoSupport健全性アラートのトリガーについて

システムヘルスアラートは、AutoSupportメッセージおよびイベント管理システム（EMS）内のイベントをトリガーします。これにより、ヘルスモニタシステムを直接使用するだけでなく、AutoSupportメッセージおよびEMSを使用してシステムの健全性を監視できます。

アラートから5分以内にAutoSupportメッセージが送信されます。AutoSupportメッセージには、前のAutoSupportメッセージ以降に生成されたすべてのアラートが含まれます。ただし、同じリソースおよび考えられる原因について前の週にアラートが重複するアラートは除きます。

一部のアラートでは、AutoSupportメッセージがトリガーされません。ヘルスポリシーでAutoSupportメッセージの送信が無効になっている場合、アラートはAutoSupportメッセージをトリガーしません。たとえば、問題の発生時にAutoSupportですでにメッセージが生成されているため、ヘルスポリシーによってAutoSupportメッセージがデフォルトで無効になる場合があります。コマンドを使用すると、AutoSupportメッセージをトリガーしないようにポリシーを設定でき `system health policy definition modify`ます。

コマンドを使用すると、前の週に送信されたアラートトリガー型AutoSupportメッセージのすべてのリストを表示できます `system health autosupport trigger history show`。

また、アラートによってEMSに対するイベントの生成もトリガーされます。イベントは、アラートが作成されるたび、およびアラートがクリアされるたびに生成されます。

使用可能なONTAPクラスタヘルスモニタの詳細

ヘルスモニタは複数あり、それぞれがクラスタの異なる部分を監視します。ヘルスモニタは、イベント検出、アラート送信、およびクリアされたイベントの削除を行い、ONTAP システム内で発生したエラーからのリカバリに役立ちます。

ヘルスモニタ名（識別子）	サブシステム名（識別子）	目的
イーサネット スイッチ	スイッチ（Switch-Health）	ONTAPイーサネットスイッチヘルスモニタ（CSHM）は、分析用のログを収集しながら、クラスタとストレージネットワークスイッチのステータスを監視します。デフォルトでは、CSHMは5分ごとにSNMPv2c経由で各スイッチをポーリングし、サポート性、監視ステータス、温度センサー、CPU利用率、インターフェイスの設定と接続、クラスタスイッチの冗長性、ファンと電源の動作に関する情報を含むリソーステーブルを更新します。また、設定されている場合、CSHMは1時間ごとにSSH/SCP経由でログを収集し、さらに分析するためにAutoSupport経由で送信します。要求に応じて、CSHMはSSH/SCPを使用して、より詳細なテクニカルサポートログ収集を実行することもできます。 詳細については、を参照してください "スイッチヘルスの監視" 。
MetroClusterファブリック	スイッチ	MetroCluster 構成のバックエンドファブリックトポロジを監視して、間違ったケーブル接続およびゾーニングなどの設定ミスや、 ISL の障害を検出します。
MetroClusterの健常性	インターコネクト、 RAID 、ストレージ	FC-VI アダプタ、 FC イニシエータアダプタ、取り残されたアグリゲートやディスク、およびクラスタ間ポートを監視します
ノード接続（node-connect）	CIFS のノンストップオペレーション（ CIFS-NDO ）	SMB 接続を監視して、 Hyper-V アプリケーションへのノンストップオペレーションを実現します。
ストレージ（SAS-connect）	ノードレベルでシェルフ、ディスク、およびアダプタを監視して、適切なパスと接続を維持します。	システム
該当なし	他のヘルスモニタからの情報を集約します。	システム接続（system-connect）

ONTAPシステムヘルスアラートの自動受信

コマンドを使用すると、システムヘルスアラートを手動で表示できます `system health alert show`。ただし、ヘルスモニタがアラートを生成したときに通知を自動的に受信するには、特定のEvent Management System（EMS；イベント管理システム）メッセージに登録する必要があります。

タスクの内容

次の手順では、すべてのhm.alert.raisedメッセージおよびすべてのhm.alert.clearedメッセージの通知を設定する方法を示します。

すべての hm.alert.raised メッセージとすべての hm.alert.cleared メッセージには SNMP トラップが含まれます。SNMPトラップの名前はと `HealthMonitorAlertCleared`です `HealthMonitorAlertRaised`。

の詳細については `system health alert show`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. コマンドを使用して `event destination create`、EMSメッセージの送信先を定義します。

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

   の詳細については `event destination create`、を"ONTAPコマンド リファレンス"参照してください。

2. コマンドを使用し `event route add-destinations`て、メッセージと `hm.alert.cleared`メッセージを送信先にルーティングし `hm.alert.raised`ます。

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

   の詳細については `event route add-destinations`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "System Managerを使用したONTAPネットワークの可視化"
- "DATA ONTAPでSNMP監視を設定する方法"

デグレードしたONTAPシステムヘルスへの対応

システムのヘルスステータスがデグレードした場合は、アラートを表示して考えられる原因および対処方法について一読し、デグレードしたサブシステムに関する情報を表示して、問題を解決できます。抑制されたアラートも表示されるため、変更して確認済みかどうかを確認できます。

タスクの内容

AutoSupportメッセージやEMSイベントを表示するか、コマンドを使用すると、アラートが生成されたことを確認できます `system health`。

手順

1. コマンドを使用し `system health alert show`て、システムヘルスを侵害しているアラートを表示します。
2. アラートに示された原因の考えられる影響、考えられる影響、および対処方法を一読し、問題を解決できるか、または詳細情報が必要かを判断します。
3. 詳細情報が必要な場合は、コマンドを使用し `system health alert show -instance`て、アラートで利用可能なその他の情報を確認します。
4. 特定のアラートについて作業中であることを示すには、パラメータを指定してコマンドを `-acknowledge` 実行し `system health alert modify`ます。
5. アラートのフィールドに記載されている対処方法を実行して、問題を解決し `Corrective Actions`ます。

   対処方法には、システムのリブートなどがあります。

   問題が解決すると、アラートは自動的にクリアされます。サブシステムに他のアラートがない場合は、サブシステムのヘルスがに変わります `OK`。すべてのサブシステムのヘルスがOKの場合は、システム全体のヘルスステータスがに変わります `OK`。

6. コマンドを使用し `system health status show`て、システムのヘルスステータスがになっていることを確認し `OK`ます。

   システムヘルスステータスがになっていない場合は `OK`、この手順を繰り返します。

関連情報

- "system health alert modify"

デグレードした**ONTAP**システムヘルスへの対応について

ノードへの 2 つのパスが不足しているシェルフが原因でデグレードしたシステムヘルスの特定の例を使用して、アラートに対応するときに CLI に表示される内容を確認します。

ONTAP を起動したあと、システムヘルスを確認すると、ステータスがデグレードしていることがわかります。

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

アラートを表示して、問題箇所を見つけ、シェルフ 2 にノード 1 へのパスが 2 つないことを確認します。

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

アラートの詳細を表示して、アラート ID などの詳細情報を取得します。

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

アラートを確認して対応中であることを示します。

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

シェルフ 2 とノード 1 との間のケーブルを修正してから、システムをリブートします。次に、システムヘルスを再度確認し、ステータスがになっていることを確認し `OK`ます。

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

関連情報

- "system health alert modify"

ONTAPシステムのヘルスの監視用コマンド

コマンドを使用すると、システムリソースの健全性に関する情報の表示、アラートへの対応、以降のアラートの設定を行うことができます `system health`。CLIコマンドを使用すると、ヘルスモニタの設定に関する詳細情報を表示できます。の詳細については `system health`、を"ONTAPコマンド リファレンス"参照してください。

システムヘルスのステータスを表示する

状況	使用するコマンド
個 々 のヘルスモニタの全体的なステータスを反映した、システムのヘルスステータスを表示する	`system health status show`
ヘルスモニタを使用できるサブシステムのヘルスステータスを表示する	`system health subsystem show`

ノード接続のステータスを表示します。

状況	使用するコマンド
ノードからストレージシェルフへの接続に関する詳細（ポート情報、HBAポート速度、I/Oスループット、1秒あたりのI/O処理率など）を表示する	`storage shelf show -connectivity` 各シェルフに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。
ドライブとアレイLUNに関する情報（使用可能なスペース、シェルフとベイの番号、所有ノード名など）を表示する	`storage disk show` パラメータを使用し `-instance`て、各ドライブに関する詳細な情報を表示します。
ストレージシェルフポートに関する詳細情報（ポートタイプ、速度、ステータスなど）を表示する	`storage port show` 各アダプタに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

クラスタとストレージネットワークスイッチの監視

状況	使用するコマンド（**ONTAP 9.8**以降）	使用するコマンド（**ONTAP 9.7**以前）
クラスタが監視するスイッチを表示する	`system switch ethernet show`	`system cluster-switch show`
削除したスイッチ（コマンド出力のReason列に表示）を含む、クラスタが現在監視しているスイッチを表示する このコマンドはadvanced権限レベルで使用できます。	`system switch ethernet show-all`	`system cluster-switch show-all`
検出されていないスイッチの監視の設定	`system switch ethernet create`	`system cluster-switch create`
クラスタが監視するスイッチに関する情報（デバイス名、IPアドレス、SNMPバージョン、コミュニティストリングなど）を変更する	`system switch ethernet modify`	`system cluster-switch modify`
スイッチの監視を無効にする	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
監視対象からスイッチを削除します。	`system switch ethernet delete`	`system cluster-switch delete`
データベースに格納されているスイッチ設定情報を完全に削除する（これにより、スイッチの自動検出が再度有効になる）	`system switch ethernet delete -force`	`system cluster-switch delete -force`
スイッチを使用したログ収集の実行	`system switch ethernet log`	`system cluster-switch log`

詳細については、および"ログ収集の設定"を参照してください"スイッチヘルスの監視"。

生成されたアラートへの対応

状況	使用するコマンド
アラートがトリガーされたリソースやノード、アラートの重大度や考えられる原因など、生成されたアラートに関する情報を表示する	`system health alert show`

状況	使用するコマンド
生成された各アラートの情報を表示する	`system health alert show -instance`
誰かがアラートに対して作業していることを示します。	`system health alert modify`
アラートを承認する	`system health alert modify -acknowledge`
サブシステムのヘルスステータスに影響しないように後続のアラートを抑制する	`system health alert modify -suppress`
自動的にクリアされなかったアラートを削除する	`system health alert delete`
あるアラートでAutoSupportメッセージがトリガーされたかどうかを確認するためなど、過去1週間にアラートによってトリガーされたAutoSupportメッセージに関する情報を表示する	`system health autosupport trigger history show`

以降のアラートの設定

状況	使用するコマンド
特定のリソースの状態で特定のアラートを発行するかどうかを制御するポリシーを有効または無効にする	`system health policy definition modify`

健全性監視の設定に関する情報を表示する

状況	使用するコマンド
ヘルスモニタに関する情報（ノード、名前、サブシステム、ステータスなど）を表示する	`system health config show` パラメータを使用し `-instance`て、各ヘルスモニタの詳細情報を表示します。
ヘルスモニタで生成される可能性があるアラートに関する情報を表示する	`system health alert definition show` 各アラート定義に関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

状況	使用するコマンド
アラートが発行されるタイミングを決定するヘルスモニタのポリシーに関する情報を表示する	`system health policy definition show` パラメータを使用し `-instance`て、各ポリシーの詳細な情報を表示します。ポリシーのステータス（有効または無効）、ヘルスモニタ、アラートなどによってアラートのリストをフィルタリングするには、その他のパラメータを使用します。

関連情報

- "storage port show"
- "収納棚ショー"
- "system health alert delete"

ONTAP環境情報の表示

センサーを使用して、システムの環境コンポーネントを監視できます。環境センサーについて表示できる情報には、タイプ、名前、状態、値、およびしきい値の警告などがあります。

ステップ

1. 環境センサーに関する情報を表示するには、コマンドを使用し `system node environment sensors show`ます。

ファイルシステム分析

ONTAPファイルシステム分析の詳細

ファイルシステム分析（FSA）はONTAP 9.8で初めて導入され、ONTAP FlexGroupまたはFlexVolボリューム内のファイルの使用状況やストレージ容量の傾向をリアルタイムで可視化します。この標準搭載された機能により、外部ツールは不要になり、ストレージの使用状況や、ビジネスニーズに合わせてストレージを最適化する機会があるかどうかに関する重要な分析情報が得られます。

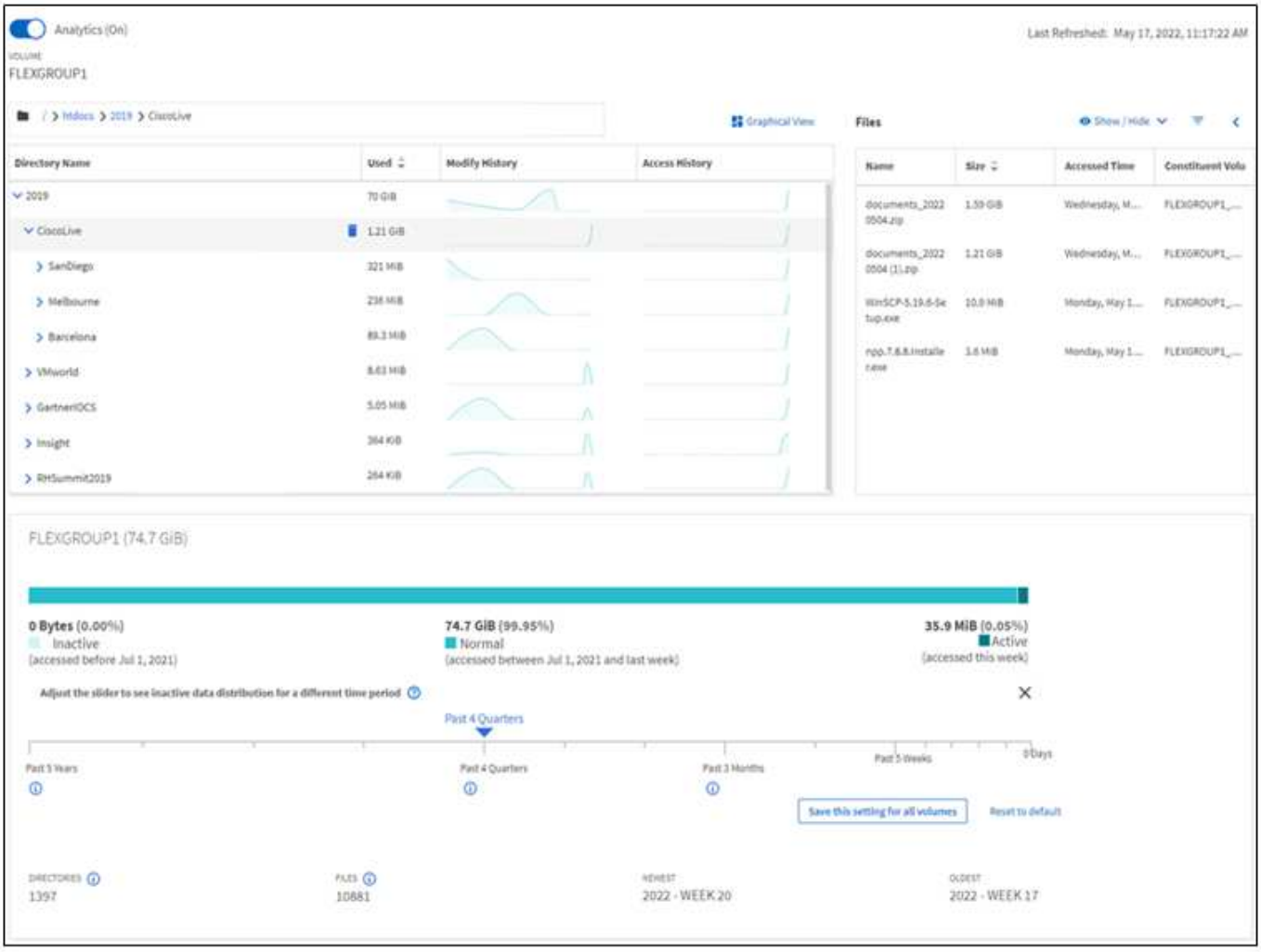
FSAを使用すると、NAS内のボリュームのファイルシステム階層のすべてのレベルが可視化されます。たとえば、Storage VM（SVM）、ボリューム、ディレクトリ、ファイルの各レベルで使用率と容量の分析情報を取得できます。FSAを使用すると、次のような質問に答えることができます。

- ストレージがいっぱいになっているのは何ですか？また、別のストレージに移動できる大きなファイルはありますか？
- 最もアクティブなボリューム、ディレクトリ、ファイルはどれですか？ストレージパフォーマンスはユーザのニーズに合わせて最適化されていますか？

- 先月に追加されたデータの量
- 最もアクティブなストレージユーザと最もアクティブでないストレージユーザを教えてください。
- プライマリストレージにあるアクセス頻度の低いデータや休止状態のデータの量そのデータを低コストのコールド階層に移動できますか。
- 予定していたサービス品質（QoS）の変更は、頻繁にアクセスされる重要なファイルへのアクセスに悪影響を及ぼしますか？

ファイルシステム分析は、ONTAPシステムマネージャに統合されています。System Managerのビューには次の機能があります。

- リアルタイムの可視化で、効果的なデータ管理と運用を実現
- リアルタイムのデータ収集と集約
- サブディレクトリ、ファイルのサイズと数、および関連付けられたパフォーマンスプロファイル
- 変更履歴とアクセス履歴のファイル経過時間ヒストグラム



サポートされるボリュームタイプ

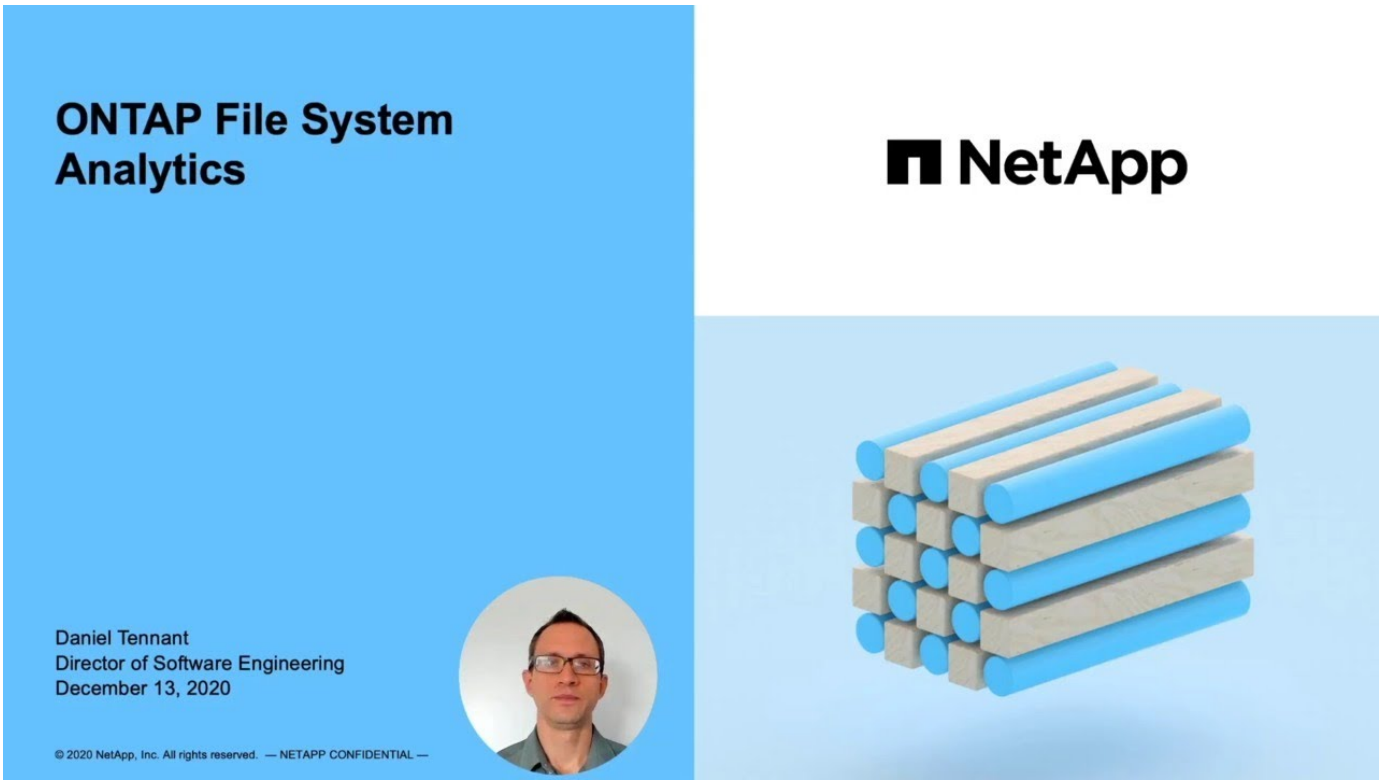
ファイルシステム分析は、FlexCacheキャッシュとSnapMirrorデスティネーションボリュームを除き、アクティブなNASデータがあるボリュームを可視化するように設計されています。

ファイルシステム分析機能の可用性

ONTAPの各リリースでは、ファイルシステム分析の範囲が拡張されます。

	ONTAP 9.14.1以降	ONTAP 9.13.1	ONTAP 9 12.1	ONTAP 9.11.1	ONTAP 9 10.1	ONTAP 9.9.1	ONTAP 9.8
System Managerでの視覚化	○	○	○	○	○	○	○
容量分析	○	○	○	○	○	○	○
アクセス頻度の低いデータの情報	○	○	○	○	○	○	○
Data ONTAP 7-Modeから移行したボリュームのサポート	○	○	○	○	○	○	いいえ
System Managerで非アクティブ期間をカスタマイズする機能	○	○	○	○	○	○	いいえ
ボリュームレベルでのアクティビティの追跡	○	○	○	○	○	いいえ	いいえ
アクティビティ追跡データをCSVにダウンロード	○	○	○	○	○	いいえ	いいえ
SVMレベルのアクティビティ追跡	○	○	○	○	いいえ	いいえ	いいえ
タイムライン	○	○	○	○	いいえ	いいえ	いいえ
使用状況分析	○	○	○	いいえ	いいえ	いいえ	いいえ
ファイルシステム分析をデフォルトで有効にするオプション	○	○	いいえ	いいえ	いいえ	いいえ	いいえ
初期化スキャン進行状況モニタ	○	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

ファイルシステム分析の詳細



関連情報

- "TR-4687 ：『 Best Practices guidelines for ONTAP File System Analytics 』"
- "ナレッジベース：NetApp ONTAP ファイルシステム分析をオンにしたあとにレイテンシが大きく変動する、または変動する"

ONTAPファイルシステム分析を有効にする

容量分析などの使用状況データを収集して表示するには、ボリュームでファイルシステム分析を有効にする必要があります。

ONTAP 9.17.1以降、NASプロトコル用に割り当てられたONTAPクラスタ上の新規SVMで作成されたボリュームでは、ファイルシステム分析（FSA）がデフォルトで有効になります。FSAはボリュームの作成と同時に自動的に有効化され、追加の設定なしですぐに分析機能を利用できます。新規ボリュームでファイルシステム分析を有効にしない場合は、 "新しいボリュームでFSAを無効にする" SVM から。

タスクの内容

- ONTAP 9.8以降では、新規または既存のボリュームでファイルシステム分析を有効にできます。システムをONTAP 9.8以降にアップグレードした場合、すべてのアップグレード プロセスが完了したことを確認してからファイルシステム分析を有効にしてください。
- 分析を有効にするのにかかる時間は、ボリュームのサイズと内容によって異なります。System Managerでは進捗状況が表示され、完了すると分析データが表示されます。初期化スキャンの進捗状況に関する詳細情報が必要な場合は、ONTAP CLIコマンドを使用し `volume analytics show`ます。
    - ONTAP 9 .15.1以降では、1つのノードで同時に実行できる初期化スキャンは4つだけです。新しいスキャンを開始する前に、スキャンが完了するまで待つ必要があります。ONTAPでは、ボリュームに十分な利用可能スペースがあることも強制され、十分でない場合はエラーメッセージが表示されます。ボリュームの使用可能なスペースの少なくとも5~8%に空きがあることを確認します。ボリュームでオ

ートサイズが有効になっている場合は、自動拡張時の最大サイズに基づいて利用可能なサイズを計算します。

- ONTAP 9 14.1以降、ONTAPでは、スキャンの進行状況に影響するスロットルイベントに関する通知に加えて、初期化スキャンの進行状況を追跡できます。
- 初期化スキャンに関するその他の考慮事項については、を参照してくださいスキャンに関する考慮事項。
- の詳細については `volume analytics show`、を"ONTAPコマンド リファレンス"参照してください。

既存のボリュームでファイルシステム分析を有効にする

ファイルシステム分析は、ONTAPシステムマネージャまたはCLIを使用して有効にできます。

例 **38.** ステップ

System Manager

ONTAP 9.10.1以降	**ONTAP 9.9.1** および**ONTAP 9.8**
1. Storage > Volumes （ストレージ）を選択します。 2. 目的のボリュームを選択します。個別のボリューム・メニューから、 * ファイル・システム > エクスプローラ * を選択します。 3. [Enable Analytics]*または[Disable Analytics]*を選択します。	1. Storage > Volumes （ストレージ）を選択します。 2. 目的のボリュームを選択し、* Explorer *を選択します。 3. [Enable Analytics]*または[Disable Analytics]*を選択します。

CLI

CLIを使用したファイルシステム分析の有効化

1. 次のコマンドを実行します。

```
volume analytics on -vserver <svm_name> -volume <volume_name> [-
foreground {true|false}]
```

デフォルトではこのコマンドはフォアグラウンドで実行されます。進捗状況が表示され、完了すると分析データが表示されます。より正確な情報が必要な場合は、 `-foreground false`オプションを選択し、 `volume analytics show` CLI で初期化の進行状況を表示するコマンド。

2. ファイルシステム分析を有効にしたら、System ManagerまたはONTAP REST APIを使用して分析データを表示します。

の詳細については `volume analytics on`、を"ONTAPコマンド リファレンス"参照してください。

ファイルシステム分析のデフォルト設定を変更

ONTAP 9.13.1以降では、SVMまたはクラスタの設定を変更して、新しいボリュームに対してデフォルトでファイルシステム分析を有効にすることができます。

例 **39.** 手順

System Manager

System Managerを使用している場合は、Storage VMまたはクラスタの設定を変更して、ボリューム作成時に容量分析とアクティビティ追跡をデフォルトで有効にすることができます。デフォルトの有効化は設定の変更後に作成されたボリュームにのみ適用され、既存のボリュームには適用されません。

クラスタのファイルシステム分析設定を変更します。

1. システム マネージャーで、クラスター設定 に移動します。
2. *クラスタ設定*で、ファイルシステム設定タブを確認します。設定を変更するには、 アイコン。
3. アクティビティ トラッキング フィールドに、アクティビティ トラッキングをデフォルトで有効にする SVM の名前を入力します。このフィールドを空白のままにすると、すべてのSVMでアクティビティ追跡が無効なままになります。

   新しいストレージ VM でアクティビティ トラッキングをデフォルトで無効にするには、[新しいストレージ VM で有効にする] ボックスのチェックを外します。

4. 分析 フィールドに、容量分析をデフォルトで有効にするストレージ VM の名前を入力します。このフィールドを空白のままにすると、すべてのSVMで容量分析が無効なままになります。

   新しいストレージ VM で容量分析をデフォルトで無効にするには、[新しいストレージ **VM** で有効にする] ボックスのチェックを外します。

5. [保存（ Save ）] を選択します。

SVMのファイルシステム分析設定を変更します。

1. 変更する SVM を選択し、*ストレージ VM 設定*を選択します。
2. ファイル システム分析 カードで、トグルを使用して、ストレージ VM 上のすべての新しいボリュームのアクティビティ追跡と容量分析を有効または無効にします。

CLI

ONTAP CLIを使用して、新しいボリュームでファイルシステム分析をデフォルトで有効にするようにStorage VMを設定できます。

SVMでファイルシステム分析をデフォルトで有効にする

1. SVMを編集し、新しく作成されたすべてのボリュームに対して容量分析とアクティビティ追跡をデフォルトで有効にします。

   ```
   vserver modify -vserver <svm_name> -auto-enable-activity-tracking
   true -auto-enable-analytics true
   ```

   の詳細については `vserver modify`、を"ONTAPコマンド リファレンス"参照してください。

関連情報

- "ONTAPコマンド リファレンス"

FSA を使用して ONTAP ファイルシステムのアクティビティを表示する

ファイルシステム分析（FSA）を有効にすると、選択したボリュームのルートディレクトリの内容を各サブツリーで使用されているスペースでソートして表示できます。

任意のファイルシステムオブジェクトを選択して、ファイルシステムを参照し、ディレクトリ内の各オブジェクトに関する詳細情報を表示します。ディレクトリの情報をグラフィカルに表示することもできます。時間の経過とともに、各サブツリーの履歴データが表示されます。3000を超えるディレクトリがある場合、使用スペースはソートされません。

エクスプローラ

File System Analytics * Explorer * 画面は、次の 3 つの領域で構成されています。

- ディレクトリとサブディレクトリのツリービュー。名前、サイズ、変更履歴、およびアクセス履歴を表示する展開可能なリスト。
- ファイル。ディレクトリリストで選択したオブジェクトの名前、サイズ、およびアクセス時間が表示されます。
- ディレクトリリストで選択されているオブジェクトのアクティブデータと非アクティブデータの比較。

  ONTAP 9 .9.1以降では、レポート対象の範囲をカスタマイズできます。デフォルト値は1年です。これらのカスタマイズに基づいて、ボリュームの移動や階層化ポリシーの変更などの対処策を実行できます。

デフォルトではアクセス時間が表示されます。ただし、CLIから（コマンドで `volume modify`オプションを `false`に設定して）ボリュームのデフォルトを変更した場合は `-atime-update`、最終変更時刻のみが表示されます。例：

- ツリービューには、 * アクセス履歴 * は表示されません。
- ファイルビューが変更されます。
- [アクティブ/非アクティブデータ]ビューは変更後の時間に基づいて表示され(`mtime`ます）。

これらの表示を使用して、次の項目を確認できます。

- スペースを最も消費するファイルシステムの場所
- ディレクトリおよびサブディレクトリ内のファイルおよびサブディレクトリ数を含む、ディレクトリツリーに関する詳細情報
- 古いデータを含むファイルシステムの場所（スクラッチツリー、一時ツリー、ログツリーなど）

FSAの出力を解釈する際は、次の点に注意してください。

- FSAは、処理されるデータ量ではなく、データがいつどこで使用されているかを示します。たとえば、最近アクセスまたは変更されたファイルが大量のスペースを消費しても、必ずしもシステム処理の負荷が高いことを示しているとは限りません。
- [ボリュームエクスプローラ *] タブで FSA のスペース消費を計算する方法は、他のツールとは異なる場合があります。特に、ボリュームで Storage Efficiency 機能が有効になっている場合、ボリューム概要 * で報告される消費量と大きく異なる可能性があります。これは、 * ボリュームエクスプローラ * タブには効率化による削減効果がないためです。
- ディレクトリ表示のスペースに制限があるため、 *List View* で 8 レベルを超えるディレクトリ階層を表示

することはできません。8 レベルを超えるディレクトリを詳細に表示するには、 *Graphical View* に切り替え、目的のディレクトリを見つけて、 *List View* に切り替える必要があります。これにより、ディスプレイに追加の画面スペースが使用できるようになります。

手順

1. 選択したボリュームのルートディレクトリの内容を表示します。

ONTAP 9.10.1以降	**ONTAP 9.9.1**および**9.8**
[* Storage] > [Volumes] を選択し、目的のボリュームを選択します。個別のボリューム・メニューから、 * ファイル・システム > エクスプローラ * を選択します。	[* ストレージ] 、 [ボリューム] の順にクリックし、目的のボリュームを選択して、 [* エクスプローラ *] をクリックします。

関連情報

- "ボリュームの変更"

FSA による ONTAP アクティビティ追跡の有効化

ONTAP 9.10.1以降のファイルシステム分析にはアクティビティ追跡機能が含まれています。この機能を使用すると、ホットオブジェクトを特定してデータをCSVファイルとしてダウンロードできます。ONTAP 9.11.1以降では、アクティビティ追跡がSVM範囲に拡張されました。また、ONTAP 9.11.1以降では、アクティビティ追跡のタイムラインが設定されており、アクティビティ追跡データを最大5分まで確認できます。

アクティビティトラッキングでは、次の4つのカテゴリでモニタリングを実行できます。

- ディレクトリ
- ファイル
- クライアント
- ユーザ

アクティビティトラッキングには、監視対象のカテゴリごとに、読み取りIOPS、書き込みIOPS、読み取りスループット、書き込みスループットが表示されます。アクティビティトラッキングに関するクエリは、過去5秒間の間にシステムで検出されたホットスポットに関連して、10～15秒ごとに更新されます。

アクティビティ追跡情報はおおよそのものであり、データの正確さは受信I/Oトラフィックの分布によって異なります。

System Managerの[Activity Tracking]をボリュームレベルで表示すると、展開したボリュームのメニューのみがアクティブに更新されます。いずれかのボリュームのビューが折りたたまれている場合は、ボリュームの表示が展開されるまで更新されません。更新を停止するには、 * 更新を一時停止 * ボタンを使用します。アクティビティデータはCSV形式でダウンロードでき、選択したボリュームについてキャプチャされたすべてのポイントインタイムデータが表示されます。

ONTAP 9.11.1以降では、タイムライン機能を使用して、ボリュームまたはSVM上のホットスポットのアクティビティを記録し、約5秒ごとに継続的に更新して過去5分間のデータを保持することができます。タイムラインデータは、ページの表示領域にあるフィールドに対してのみ保持されます。追跡カテゴリを折りたたんだり、タイムラインが表示されないようにスクロールしたりすると、タイムラインはデータの収集を停止しま

す。デフォルトでは、タイムラインは無効になっており、[アクティビティ]タブから移動すると自動的に無効になります。

単一のボリュームのアクティビティ追跡を有効にする

アクティビティ追跡は、ONTAP System ManagerまたはCLIを使用して有効にできます。

タスクの内容

ONTAP REST APIまたはSystem ManagerでRBACを使用する場合は、アクティビティ追跡へのアクセスを管理するためのカスタムロールを作成する必要があります。このプロセスについては、を参照してくださいロールベースアクセス制御。

System Manager

手順

1. Storage > Volumes （ストレージ）を選択します。目的のボリュームを選択します。個 々 のボリュームメニューから[File System]を選択し、[Activity]タブを選択します。
2. 上位のディレクトリ、ファイル、クライアント、およびユーザに関する個々のレポートを表示するには、 * Activity Tracking * をオンにします。
3. 更新を行わずにデータをより詳細に分析するには、 * 更新を一時停止 * を選択します。データをダウンロードして、レポートのCSVレコードを作成することもできます。

CLI

手順

1. アクティビティトラッキングを有効にする：

```
volume activity-tracking on -vserver svm_name -volume volume_name
```

2. 次のコマンドを使用して、ボリュームのアクティビティ追跡の状態がオンまたはオフになっているかどうかを確認します。

```
volume activity-tracking show -vserver svm_name -volume volume_name -state
```

3. 有効にしたら、ONTAP System ManagerまたはONTAP REST APIを使用してアクティビティ追跡データを表示します。

複数ボリュームのアクティビティ追跡を有効にする

System ManagerまたはCLIを使用して、複数のボリュームのアクティビティ追跡を有効にすることができます。

タスクの内容

ONTAP REST APIまたはSystem ManagerでRBACを使用する場合は、アクティビティ追跡へのアクセスを管理するためのカスタムロールを作成する必要があります。このプロセスについては、を参照してくださいロールベースアクセス制御。

System Manager

特定のボリュームに対して有効化

1. Storage > Volumes （ストレージ）を選択します。目的のボリュームを選択します。個 々 のボリュームメニューから[File System]を選択し、[Activity]タブを選択します。
2. アクティビティ追跡を有効にするボリュームを選択します。ボリュームリストの上部で、その他のオプション*ボタンを選択します。［*アクティビティトラッキングを有効にする］を選択します。
3. SVMレベルでアクティビティの追跡を表示するには、表示するSVMを* Storage > Volumes *から選択します。[File System]タブ、[Activity]の順に選択すると、アクティビティ追跡が有効になっているボリュームのデータが表示されます。

すべてのボリュームに対して有効にする

1. Storage > Volumes （ストレージ）を選択します。メニューからSVMを選択します。
2. 「* File System 」タブに移動し、「 More *」タブを選択して、SVM内のすべてのボリュームでアクティビティの追跡を有効にします。

CLI

ONTAP 9.13.1以降では、ONTAP CLIを使用して複数のボリュームのアクティビティ追跡を有効にすることができます。

手順

1. アクティビティトラッキングを有効にする：

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   `*`指定したStorage VM上のすべてのボリュームに対してアクティビティ追跡を有効にします。

   ボリューム名のあとに続けてを使用し !、指定したボリュームを除くSVM上のすべてのボリュームに対してアクティビティ追跡を有効にします。

2. 処理が成功したことを確認します。

   ```
   volume show -fields activity-tracking-state
   ```

3. 有効にしたら、ONTAP System ManagerまたはONTAP REST APIを使用してアクティビティ追跡データを表示します。

FSA による ONTAP 使用状況分析の有効化

ONTAP 9.12.1以降では、使用状況分析を有効にして、ボリューム内のどのディレクトリが最もスペースを使用しているかを確認できます。ボリューム内のディレクトリの総数、またはボリューム内のファイルの総数を表示できます。Reportingは、最もスペースを使用する25個のディレクトリに制限されます。

大規模ディレクトリの分析は15分ごとに更新されます。ページ上部の[Last refreshed]のタイムスタンプを確認

すると、最新の更新を監視できます。[ダウンロード]ボタンをクリックして、Excelブックにデータをダウンロードすることもできます。ダウンロード処理はバックグラウンドで実行され、選択したボリュームについて最新の情報が表示されます。結果が表示されずにスキャンが再開された場合は、ボリュームがオンラインであることを確認してください。SnapRestoreなどのイベントが発生すると、ファイルシステム分析で大容量ディレクトリのリストが再構築されます。

手順

1. Storage > Volumes （ストレージ）を選択します。目的のボリュームを選択します。
2. 個別のボリューム・メニューから、ファイル・システム*を選択します。次に、 Usage *タブを選択します。
3. 使用状況の分析を有効にするには、* Analytics *スイッチを切り替えます。
4. System Managerには、最大サイズのディレクトリを降順で示す棒グラフが表示されます。

> ONTAPでは、上位ディレクトリのリストの収集中に、データの一部が表示される場合や、データがまったく表示されない場合があります。スキャンの進行状況は、スキャン中に表示される[**Usage**]タブで確認できます。

特定のディレクトリに関する詳細な情報を得るには、次のONTAP ファイルシステムのアクティビティを表示する手順を実行します。

FSAのONTAP分析に基づいて是正措置を講じる

ONTAP 9 .9.1以降では、ファイルシステム分析画面から、現在のデータと必要な結果に基づいて直接対処できます。

ディレクトリとファイルの削除

エクスプローラ画面で、削除するディレクトリまたは個 々 のファイルを選択できます。ディレクトリは、低レイテンシの非同期ディレクトリ削除機能を使用して削除されます。（ONTAP 9.9.1以降では、分析が有効になっていない場合でも、ディレクトリの非同期削除を実行できます）。

ONTAP 9.10.1以降	ONTAP 9.9.1の場合
1. ストレージ > ボリューム を選択し、目的のボリューム名を選択します。 2. 個々のボリューム ページで、ファイル システム タブを選択し、エクスプローラー タブを選択します。 3. *エクスプローラー*ビューで、目的のディレクトリを選択します。 4. 削除するには、ファイルまたはフォルダの上にマウスを移動し、削除オプションが表示されます。 一度に削除できるオブジェクトは 1 つだけです。 ディレクトリとファイルを削除しても、新しいストレージ容量の値はすぐには表示されません。	1. Storage > Volumes （ストレージ）を選択します。 2. 目的のボリュームを選択し、* Explorer *を選択します。 3. *エクスプローラー*ビューで、目的のディレクトリを選択します。 4. 削除するには、ファイルまたはフォルダの上にマウスを移動し、削除オプションが表示されます。

ストレージ階層にメディアコストを割り当て、使用頻度の低いデータストレージのコストを比較

メディアコストは、ストレージコストの評価に基づいて割り当てる値で、GBあたりの通貨を選択します。設定すると、System Managerは割り当てられたメディアコストを使用して、ボリュームを移動する際の予想される削減量を予測します。

設定したメディアコストは永続的ではなく、1つのブラウザセッションに対してのみ設定できます。

手順

1. [* ストレージ > 階層 *] をクリックし、目的のローカル階層（アグリゲート）タイルの [* メディアコストの設定] をクリックします。

   比較を有効にするには、アクティブな階層と非アクティブな階層を選択してください。

2. 通貨タイプと金額を入力します。

   メディアコストを入力または変更すると、すべてのメディアタイプで変更が行われます。

ボリュームを移動してストレージコストを削減

分析画面やメディアコストの比較に基づいて、ローカル階層内の低コストのストレージにボリュームを移動できます。

比較および移動できるボリュームは一度に1つだけです。

手順

1. メディアコストの表示を有効にしたら、 [* ストレージ > 階層 *] をクリックし、 [* ボリューム *] をクリックします。
2. ボリュームのデスティネーションオプションを比較するには、ボリュームのをクリックし 、*[移動]*を

クリックします。

3. [Select Destination Local Tier] （宛先ローカル階層の選択）画面で、推定コスト差異を表示する宛先階層を選択します。
4. オプションを比較したら、目的の階層を選択し、 * 移動 * をクリックします。

ONTAPファイルシステム分析によるロールベースアクセス制御

ONTAP 9.12.1以降のONTAPには、という名前の事前定義されたRole-Based Access Control（RBAC；ロールベースアクセス制御）ロールが含まれてい `admin-no-fsa`ます。この `admin-no-fsa`ロールは管理者レベルの`Privileges`を付与しますが、ユーザは`ONTAP CLI`、`REST API`、および`System Manager`でエンドポイントに関連する処理（ファイルシステム分析）を実行できません `files`。

役割の詳細については `admin-no-fsa`、を参照してくださいクラスタ管理者の事前定義されたロール。

ONTAP 9 12.1より前にリリースされたバージョンのONTAPを使用している場合は、ファイルシステム分析へのアクセスを制御する専用のロールを作成する必要があります。12.1より前のバージョンのONTAPでは、ONTAP CLIまたはONTAP ONTAP 9を使用してRBACアクセス許可を設定する必要があります。

System Manager

ONTAP 9.12.1以降では、System Managerを使用してファイルシステム分析用のRBAC権限を設定できます。

手順

1. [* Cluster]>[Settings]（設定）を選択します。**[セキュリティ]***で、[ユーザとロール]*に移動し、を選択します →。
2. [ロール]*で、を選択します ＋ Add 。
3. ロールの名前を指定します。[Role Attributes]で、適切なを指定してユーザロールのアクセス権または制限を設定し"APIエンドポイント"ます。ファイルシステム分析のアクセスまたは制限を設定するには、プライマリパスとセカンダリパスについて次の表を参照してください。

制限	プライマリパス	セカンダリパス
ボリュームのアクティビティ追跡	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
SVMでのアクティビティ追跡	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
すべてのファイルシステム分析処理	`/api/storage/volumes`	`/:uuid/files`

UUIDの代わりにを使用して、エンドポイントですべてのボリュームまたはSVMにポリシーを設定できます `/*/`。

各エンドポイントのアクセスPrivilegesを選択します。

4. [保存（ Save ）] を選択します。
5. ユーザにロールを割り当てるには、を参照してください管理者アクセスの制御。

CLI

ONTAP 9 12.1より前にリリースされたONTAPのバージョンを使用している場合は、ONTAP CLIを使用

してカスタムロールを作成します。

手順

1. すべての機能にアクセスできるデフォルトロールを作成します。

   これは、制限ロールを作成する前に実行する必要があります。これは、アクティビティトラッキングでのみロールが制限されるようにするためです。

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. 制限ロールを作成します。

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. ロールにSVMのWebサービスへのアクセスを許可します。

   - `rest`RESTAPI呼び出し
   - `security`パスワード保護用
   - `sysmgr`System Managerへノアクセスヨウ

     ```
     vserver services web access create -vserver <svm-name> -name rest -role
     storageAdmin

     vserver services web access create -vserver <svm-name> -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver <svm-name> -name sysmgr -role
   storageAdmin
   ```

4. ユーザを作成します。

   ユーザに適用するアプリケーションごとに、個別のcreateコマンドを発行する必要があります。同じユーザに対してcreateを複数回呼び出すと、その1人のユーザにすべてのアプリケーションが適用され、毎回新しいユーザが作成されることはありません。アプリケーションタイプのパラメータは、`http`ONTAP REST APIおよびSystem Managerに適用されます。

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. 新しいユーザクレデンシャルを使用して、System Managerにログインするか、ONTAP REST APIを使用してファイルシステム分析データにアクセスできるようになりました。

詳細情報

- クラスタ管理者の事前定義されたロール
- System Managerで管理者アクセスを制御
- "RBACロールとONTAP REST APIの詳細については、こちらをご覧ください"

- "security login create"

ONTAPファイルシステム分析に関する考慮事項

ファイルシステム分析の実装に伴う使用制限とパフォーマンスへの潜在的な影響を理解しておく必要があります。

SVMの保護関係

ファイルシステム分析を有効にしたボリュームが格納されているSVMで保護関係が確立されている場合、デスティネーションSVMには分析データはレプリケートされません。リカバリ処理でソースSVMを再同期した場合は、リカバリ後に必要なボリュームについて分析を手動で再度有効にする必要があります。

パフォーマンスに関する考慮事項

ファイルシステム分析を有効にすると、メタデータの初回収集時のパフォーマンスが低下することがあります。多くの場合、この状況は利用率が最大になっているシステムで発生します。このようなシステムでは、代わりにONTAP System Managerのパフォーマンス監視ツールを使用できます。

遅延が著しく増加した場合は、"NetAppナレッジベース: NetApp ONTAPファイル システム分析をオンにした後のレイテンシが高くなったり変動したりする" 。

スキャンに関する考慮事項

容量分析を有効にすると、ONTAPは容量分析の初期化スキャンを実行します。スキャンは、容量分析が有効になっているボリューム内のすべてのファイルのメタデータにアクセスします。スキャン中にファイルデータは読み取られません。ONTAP 9.14.1以降では、REST API、System Managerの[*** Explorer**]タブ、またはCLIコマンドを使用して、スキャンの進行状況を追跡できます `volume analytics show`。スロットルイベントが発生した場合は、ONTAPから通知が送信されます。

ボリュームでファイルシステム分析を有効にする場合は、ボリュームの使用可能なスペースの少なくとも5~8%が空きスペースであることを確認してください。ボリュームでオートサイズが有効になっている場合は、自動拡張時の最大サイズに基づいて利用可能なサイズを計算します。ONTAP 9 .15.1以降では、ボリュームでファイルシステム分析を有効にすると、使用可能なスペースが不足していると、ONTAPにエラーメッセージが表示されます。

スキャンが完了すると、ファイルシステムの変更に応じてリアルタイムでファイルシステム分析が継続的に更新されます。

スキャンに必要な時間は、ボリューム上のディレクトリとファイルの数に比例します。スキャンではメタデータが収集されるため、ファイルサイズはスキャン時間に影響しません。

初期化スキャンの詳細については、を参照してください"TR-4867：『Best Practice Guidelines for File System Analytics』"。

ベストプラクティス

アグリゲートを共有しないボリュームでスキャンを開始する必要があります。現在どのアグリゲートがどのボリュームをホストしているかを確認するには、次のコマンドを使用します。

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

スキャン中もボリュームはクライアント トラフィックを処理します。クライアント トラフィックが少ない時間帯にスキャンを開始することを推奨します。

クライアント トラフィックが増加すると、システム リソースが消費され、スキャンにかかる時間が長くなります。

ONTAP 9.12.1以降では、System ManagerおよびONTAP CLIでデータ収集を一時停止できます。

- ONTAP CLIを使用する場合の処理：
  - 次のコマンドを使用してデータ収集を一時停止できます。 `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - クライアントトラフィックの速度が低下したら、次のコマンドを使用してデータ収集を再開できます。 `volume analytics initialization resume -vserver svm_name -volume volume_name`
- System Managerを使用している場合は、ボリュームメニューの*ビューで[データ収集の一時停止]および[データ収集の再開]*ボタンを使用してスキャンを管理します。

EMSノセツテイ

ONTAP EMS構成の詳細

重要なイベント管理システム（EMS）のイベント通知をEメールアドレス、syslogサーバ、簡易管理ネットワークプロトコル（SNMP）トラップホスト、またはWebhookアプリケーションに直接送信するようにONTAP 9を設定することで、早急な対応が必要なシステムの問題をすぐに通知することができます。

重要なイベント通知はデフォルトでは有効になっていないため、Eメールアドレス、syslogサーバ、SNMPトラップホスト、またはWebhookアプリケーションのいずれかに通知を送信するようにEMSを設定する必要があります。

のリリース固有のバージョンを確認します"ONTAP 9 EMSリファレンス"。

EMSイベントのマッピングで廃止されたONTAPコマンドセット（イベントの送信先、イベントルートなど）を使用している場合は、マッピングを更新することを推奨します。"廃止されたONTAP コマンドからEMSマッピングを更新する方法について説明します"です。

System Managerを使用したONTAP EMSイベント通知とフィルタの設定

System Managerを使用して、早急な対応を要するシステムの問題を通知するために、Event Management System（EMS；イベント管理システム）によるイベント通知の配信方法を設定できます。

ONTAPのバージョン	System Manager で実行できる作業
ONTAP 9.12.1以降	リモートsyslogサーバにイベントを送信するときに、Transport Layer Security（TLS）プロトコルを指定します。

ONTAP 9.10.1以降	SNMPトラップホストに加え、Eメールアドレス、syslogサーバ、Webフックアプリケーションを設定します。
ONTAP 9.10.0から9.7	SNMPトラップホストのみを設定します。他のEMSデスティネーションは、ONTAP CLIを使用して設定できます。を参照して "EMSの設定 - 概要"

EMSイベント通知の送信先を追加する

System Managerを使用して、EMSメッセージの送信先を指定できます。

ONTAP 9.12.1以降では、Transport Layer Security（TLS）プロトコルを使用して、リモートsyslogサーバの指定ポートにEMSイベントを送信できます。の詳細については `event notification destination create`、を"ONTAPコマンド リファレンス"参照してください。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [Notifications Management]セクションで、をクリックし、*[View Event Destinations]*をクリックします。
3. [* 通知管理] ページで、 [イベントの送信先 *] タブを選択します。
4. をクリックします。 + Add
5. 名前、EMSデスティネーションタイプ、およびフィルタを指定します。

   必要に応じて、新しいフィルタを追加できます。[新しいイベントフィルタの追加 *] をクリックします。

6. 選択したEMSデスティネーションタイプに応じて、次の項目を指定します。

構成する	指定または選択 …
SNMPトラップホスト	• トラップホスト名
Eメール （9.10.1以降）	• 送信先Eメールアドレス • メールサーバ • 送信元Eメールアドレス
syslogサアハ （9.10.1以降）	• サーバのホスト名またはIPアドレス • syslogポート（9.12.1以降） • syslog転送（9.12.1以降） TCP Encrypted を選択すると、**Transport Layer Security**（**TLS**）プロトコルが有効になります。**syslog**ポート*に値を入力しない場合は、「 Syslog transport *」の選択に基づいてデフォルトが使用されます。

ウェブフック （9.10.1以降）	• Webhook URL • クライアント認証（クライアント証明書を指定する場合は、このオプションを選択します）

新しい**EMS**イベント通知フィルタを作成する

ONTAP 9 .10.1以降では、System Managerを使用してカスタマイズした新しいフィルタを定義し、通知を処理するルールを指定できます。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [Notifications Management]セクションで、をクリックし、*[View Event Destinations]*をクリックします。
3. [* 通知管理 *] ページで、 [* イベント・フィルタ *] タブを選択します。
4. をクリックします。 + Add
5. 名前を指定し、既存のイベントフィルタからルールをコピーするか、新しいルールを追加するかを選択します。
6. 選択に応じて、次の手順を実行します。

選択した場合	次に、次の手順を実行します。
• 既存のイベントフィルタからルールをコピー *	1. 既存のイベントフィルタを選択します。 2. 既存のルールを変更します。 3. 必要に応じて、をクリックして他のルールを追加します + Add。
• 新しいルールを追加 *	新しいルールごとに、タイプ、名前パターン、重大度、および SNMP トラップのタイプを指定します。

EMSイベント通知の送信先を編集する

ONTAP 9 .10.1以降では、System Managerを使用してイベント通知の送信先情報を変更できます。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [Notifications Management]セクションで、をクリックし、*[View Event Destinations]*をクリックします。
3. [**Notifications Management**] ページで、 **[*Events Destinations**] タブを選択します。
4. イベントの送信先の名前の横にあるをクリックし、*[編集]*をクリックします。
5. イベントの送信先情報を変更し、 * 保存 * をクリックします。

EMSイベント通知フィルタを編集する

ONTAP 9 .10.1以降では、System Managerを使用してカスタマイズしたフィルタを変更し、イベント通知の処理方法を変更できます。

システム定義のフィルタは変更できません。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [Notifications Management]セクションで、をクリックし、*[View Event Destinations]*をクリックします。
3. [* 通知管理 *] ページで、 [* イベント・フィルタ *] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックし、*[編集]*をクリックします。
5. イベントフィルタの情報を変更し、 [保存（ Save ）] をクリックします。

EMSイベント通知の送信先を削除する

ONTAP 9 .10.1以降では、System Managerを使用してイベント通知の送信先を削除できます。

SNMPの送信先は削除できません。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [Notifications Management]セクションで、をクリックし、*[View Event Destinations]*をクリックします。
3. [* 通知管理] ページで、 [イベントの送信先 *] タブを選択します。
4. イベントの送信先の名前の横にあるをクリックし、*[削除]*をクリックします。

EMSイベント通知フィルタを削除する

ONTAP 9 .10.1以降では、System Managerを使用してカスタマイズしたフィルタを削除できます。

システム定義のフィルタは削除できません。

手順

1. [クラスタ]>[設定]*をクリックします。
2. [Notifications Management]セクションで、をクリックし、*[View Event Destinations]*をクリックします。
3. [* 通知管理 *] ページで、 [* イベント・フィルタ *] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックし、*[削除]*をクリックします。

関連情報

- "ONTAP EMSリファレンス"
- "CLIを使用したイベント通知を受信するSNMPトラップホストの設定"

CLIを使用したEMSイベント通知の設定

ONTAP EMSの設定ワークフロー

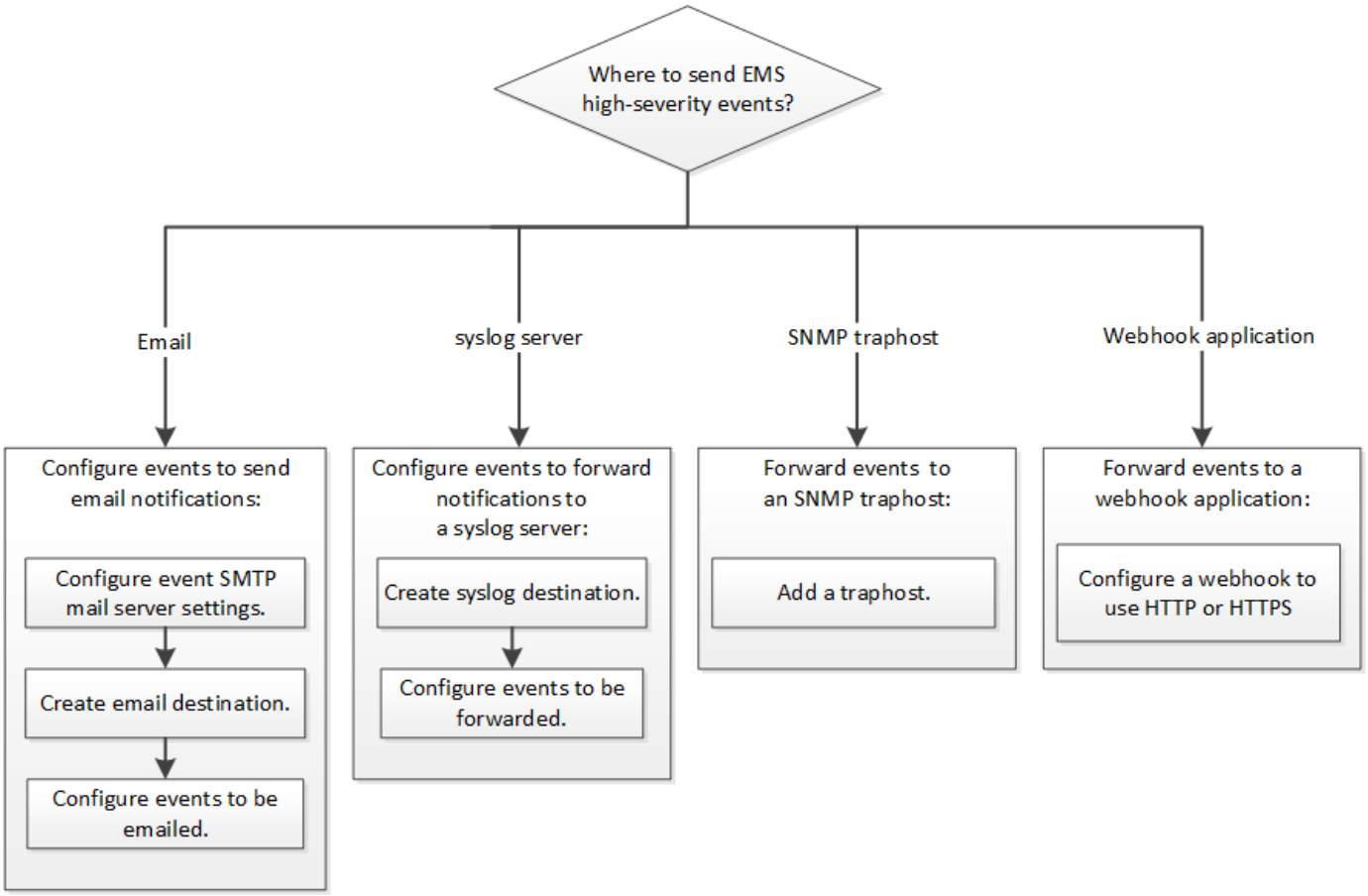
重要なEMSイベント通知がEメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebhookアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

タスクの内容

サーバやアプリケーションなど、他のシステムで記録されたイベントを集約するためにすでにsyslogサーバを使用している場合は、ストレージシステムからの重要なイベントの通知にもそのsyslogサーバを使用すると簡単です。

syslogサーバがまだない場合は、重要なイベントの通知にEメールを使用する方が簡単です。

イベント通知をすでにSNMPトラップホストに転送している場合は、そのトラップホストで重要なイベントが発生していないか監視できます。



選択肢

- イベント通知を送信するようにEMSを設定します。

状況	参照先

EMSの重要なイベント通知をEメールアドレスに送信する	重要なEMSイベントを設定してEメール通知を送信する
EMSの重要なイベント通知をsyslogサーバに転送する	重要なEMSイベントの通知をsyslogサーバに転送するように設定する
EMSのイベント通知をSNMPトラップホストに転送する場合	イベント通知を受信するためのSNMPトラップホストの設定
EMSのイベント通知をWebhookアプリケーションに転送する場合	重要なEMSイベントを設定して通知をWebhookアプリケーションに転送する

重要な**ONTAP EMS**イベントを設定して**E**メール通知を送信する

最も重要なイベントの通知をEメールで受信するには、重要なアクティビティを示すイベントについてEメールメッセージを送信するようにEMSを設定する必要があります。

開始する前に

クラスタでEメールアドレスを解決するようにDNSが設定されている必要があります。

タスクの内容

このタスクは、クラスタの実行中であれば、ONTAPコマンドラインでコマンドを入力していつでも実行できます。

手順

1. イベントSMTPメールサーバを設定します。

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

   の詳細については `event config modify`、を"ONTAPコマンド リファレンス"参照してください。

2. イベント通知用のEメール送信先を作成します。

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

   の詳細については `event notification destination create`、を"ONTAPコマンド リファレンス"参照してください。

3. Eメール通知を送信するための重要なイベントを設定します。

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

   の詳細については `event notification create`、を"ONTAPコマンド リファレンス"参照してください。

重要なONTAP EMSイベントの通知をsyslogサーバに転送するように設定する

重大度の高いイベントの通知をsyslogサーバに記録するには、重要なアクティビティを示すイベントの通知を転送するようにEMSを設定する必要があります。

開始する前に

クラスタでsyslogサーバ名を解決するようにDNSが設定されている必要があります。

タスクの内容

イベント通知用のsyslogサーバがまだない場合は、最初にsyslogサーバを作成する必要があります。他のシステムのイベントを記録するためにすでにsyslogサーバを使用している場合は、重要なイベントの通知にそのsyslogサーバを使用できます。

このタスクは、クラスタの実行中であれば、ONTAP CLIでコマンドを入力していつでも実行できます。

ONTAP 9 .12.1以降では、Transport Layer Security（TLS）プロトコルを使用して、リモートsyslogサーバ上の指定ポートにEMSイベントを送信できます。次の2つの新しいパラメータを使用できます。

`tcp-encrypted`

にを指定する `syslog-transport`と `tcp-encrypted`、ONTAPは証明書を検証してデスティネーションホストのIDを検証します。デフォルト値はです `udp-unencrypted`。

`syslog-port`

デフォルト値 `syslog-port`のパラメータは、パラメータの設定によって異なり `syslog-transport`ます。がに設定されて `tcp-encrypted`いる場合、 `syslog-transport`の `syslog-port`デフォルト値は6514です。

手順

1. 重要なイベントのsyslogサーバの送信先を作成します。

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   ONTAP 9 . 12.1以降では、に次の値を指定でき `syslog-transport`ます。

   - `udp-unencrypted`-セキュリティなしのUser Datagram Protocol（ユーザデータグラムプロトコル）
   - `tcp-unencrypted`-セキュリティなしの伝送制御プロトコル
   - `tcp-encrypted`- Transport Layer Security（TLS）を使用したTransmission Control Protocol（Transmission Control Protocol）

     デフォルトのプロトコルはです `udp-unencrypted`。

   の詳細については `event notification destination create`、を"ONTAPコマンド リファレンス"参照してください。

2. 重要なイベントについて、syslogサーバに通知を転送するように設定します。

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

の詳細については `event notification create`、を"ONTAPコマンド リファレンス"参照してください。

イベント通知を受信するための**ONTAP SNMP**トラップホストの設定

SNMPトラップホストでイベント通知を受信するには、トラップホストを設定する必要があります。

開始する前に

- クラスタでSNMPとSNMPトラップが有効になっている必要があります。

  SNMPおよびSNMPトラップはデフォルトで有効になっています。

- クラスタでトラップホスト名を解決するようにDNSが設定されている必要があります。

タスクの内容

イベント通知（SNMPトラップ）を受信するように設定したSNMPトラップホストがまだない場合は、SNMPトラップホストを追加する必要があります。

このタスクは、クラスタの実行中であれば、ONTAPコマンドラインでコマンドを入力していつでも実行できます。

ステップ

1. イベント通知を受信するように設定されたSNMPトラップホストがまだない場合は、SNMPトラップホストを追加します。

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   SNMPでデフォルトでサポートされるすべてのイベント通知がSNMPトラップホストに転送されます。

重要な**ONTAP EMS**イベントを設定して通知を**Webhook**アプリケーションに転送する

重要なイベント通知をWebhookアプリケーションに転送するようにONTAPを設定できます。必要な設定手順は、選択したセキュリティのレベルによって異なります。

EMSイベント転送を設定する準備

Webhookアプリケーションにイベント通知を転送するようにONTAPを設定する前に、いくつかの概念と要件を考慮する必要があります。

Webhookアプリケーション

ONTAPイベント通知を受信できるWebhookアプリケーションが必要です。Webhookはユーザ定義のコールバックルーチンで、実行されるリモートアプリケーションまたはサーバの機能を拡張します。Webhookは、宛先URLにHTTP要求を送信することにより、クライアント（この場合はONTAP）によって呼び出されるか、アクティブになります。具体的には、ONTAPは、Webhookアプリケーションをホストしているサーバーに、XML形式のイベント通知の詳細とともにHTTP POST要求を送信します。

セキュリティオプション

Transport Layer Security（TLS）プロトコルの使用方法に応じて、いくつかのセキュリティオプションを使用できます。選択するオプションによって、必要なONTAP設定が決まります。

TLSは、インターネットで広く使用されている暗号化プロトコルです。1つ以上の公開鍵証明書を使用して、プライバシー、データの整合性、および認証を提供します。証明書は、信頼された認証局によって発行されます。

HTTP

HTTPを使用してイベント通知を転送できます。この設定では、接続はセキュアではありません。ONTAPクライアントとWebhookアプリケーションのIDは検証されません。さらに、ネットワークトラフィックは暗号化または保護されません。設定の詳細については、を参照してください"Webフックの転送先でHTTPを使用するための設定"。

HTTPS

セキュリティを強化するために、webhookルーチンをホストするサーバーに証明書をインストールできます。HTTPSプロトコルは、ONTAPによってWebhookアプリケーションサーバのIDを検証するために使用されます。また、ネットワークトラフィックのプライバシーと整合性を確保するために、両方の当事者によって使用されます。設定の詳細については、を参照してください"HTTPSを使用するようにWebhookの宛先を設定する"。

相互認証を使用する**HTTPS**

Webブック要求を発行するONTAPシステムにクライアント証明書をインストールすることで、HTTPSセキュリティをさらに強化できます。Webhookアプリケーションサーバの**ID**を検証し、ネットワークトラフィックを保護するONTAPに加えて、WebhookアプリケーションはONTAPクライアントのIDを検証します。この双方向ピア認証は、_Mutual TLS_と呼ばれています。設定の詳細については、を参照してください"相互認証でHTTPSを使用するようにWebhookの宛先を設定する"。

関連情報

- "Transport Layer Security（TLS）プロトコルバージョン1.3"

Webフックの転送先で**HTTP**を使用するための設定

HTTPを使用してWebフック アプリケーションにイベント通知を転送するようにONTAPを設定できます。これはセキュリティが最も低いオプションですが、設定が最も簡単です。

手順

1. イベントを受信する新しい送信先を作成し `restapi-ems`ます。

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   上記のコマンドでは、デスティネーションに* HTTP *スキームを使用する必要があります。

   の詳細については `event notification destination create`、を"ONTAPコマンド リファレンス"参照してください。

2. フィルタと `restapi-ems`宛先をリンクする通知を作成し `important-events`ます。

   ```
   event notification create -filter-name important-events -destinations restapi-
   ```

`ems`

の詳細については `event notification create`、を"ONTAPコマンド リファレンス"参照してください。

HTTPSを使用するようにWebhookの宛先を設定する

HTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAP を設定できます。ONTAPはサーバ証明書を使用して、WebhookアプリケーションのIDを確認し、ネットワークトラフィックを保護します。

開始する前に

- Webhookアプリケーションサーバの秘密鍵と証明書を生成する
- ルート証明書をONTAPにインストールできるようにする

手順

1. Webhookアプリケーションをホストするサーバーに、適切なサーバー秘密鍵と証明書をインストールします。具体的な設定手順は、サーバによって異なります。
2. ONTAPにサーバルート証明書をインストールします。

   ```
   security certificate install -type server-ca
   ```

   コマンドは証明書を要求します。

3. イベントを受信する送信先を作成し `restapi-ems`ます。

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   上記のコマンドでは、デスティネーションに* HTTPS *スキームを使用する必要があります。

4. フィルタと新しい `restapi-ems`宛先をリンクする通知を作成し `important-events`ます。

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

相互認証でHTTPSを使用するようにWebhookの宛先を設定する

相互認証を使用してHTTPSを使用してWebhookアプリケーションにイベント通知を転送するようにONTAPを設定できます。この構成では、2つの証明書があります。ONTAPは、サーバ証明書を使用してWebhookアプリケーションのIDを確認し、ネットワークトラフィックを保護します。さらに、Webhookをホストするアプリケーションは、クライアント証明書を使用してONTAPクライアントのIDを確認します。

開始する前に

ONTAPを設定する前に、次の作業を行う必要があります。

- Webhookアプリケーションサーバの秘密鍵と証明書を生成する
- ルート証明書をONTAPにインストールできるようにする
- ONTAPクライアントの秘密鍵と証明書を生成する

手順

1. タスクの最初の2つの手順を実行し"HTTPSを使用するようにWebhookの宛先を設定する"てサーバ証明書をインストールし、ONTAPがサーバのIDを確認できるようにします。
2. Webhookアプリケーションに適切なルート証明書と中間証明書をインストールして、クライアント証明書を検証します。
3. ONTAPにクライアント証明書をインストールします。

   ```
   security certificate install -type client
   ```

   コマンドは秘密鍵と証明書を要求します。
4. イベントを受信する送信先を作成し `restapi-ems`ます。

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   上記のコマンドでは、デスティネーションに* HTTPS *スキームを使用する必要があります。
5. フィルタと新しい `restapi-ems`宛先をリンクする通知を作成し `important-events`ます。

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

関連情報

- "セキュリティ証明書のインストール"

廃止された**EMS**イベントマッピングを更新する

ONTAP EMSイベントマッピングモデルの詳細

ONTAP 9 .0より前のバージョンでは、EMSイベントをイベント名のパターンマッチングに基づいてイベントの送信先にマッピングする必要がありました。(`event destination` `event route`このモデルを使用するONTAPコマンドセット）は、最新バージョンのONTAPでも引き続き使用できますが、ONTAP 9 .0以降では廃止されています。

ONTAP 9 .0以降のONTAP EMSイベントのデスティネーションマッピングのベストプラクティスは、拡張性に優れたイベントフィルタモデルを使用することです。拡張性に優れたイベントフィルタモデルでは、、`event notification`の `event notification destination`各コマンドセットを使用して複数のフィールドに対してパターンマッチングが行われ `event filter`ます。

廃止されたコマンドを使用してEMSマッピングが設定されている場合は、の `event notification` `event notification destination`各コマンドセットを使用するようにマッピングを更新する必要があります `event filter`。の詳細については `event`、を"ONTAPコマンド リファレンス"参照してください。

イベントの送信先には次の2種類があります。

1. * システムで生成される送信先 * ：システムで生成される 5 つのイベントの送信先があります（デフォル

トで作成）。

- `allevents`
- `asup`
- `criticals`
- `pager`
- `traphost`

  システムによって生成される送信先の一部は、特別な目的に使用されます。たとえば、 ASUP デスティネーションは、 callhome.* イベントを ONTAP の AutoSupport モジュールにルーティングして AutoSupport メッセージを生成します。

2. ユーザが作成した送信先：コマンドを使用して手動で作成し `event destination create`ます。

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

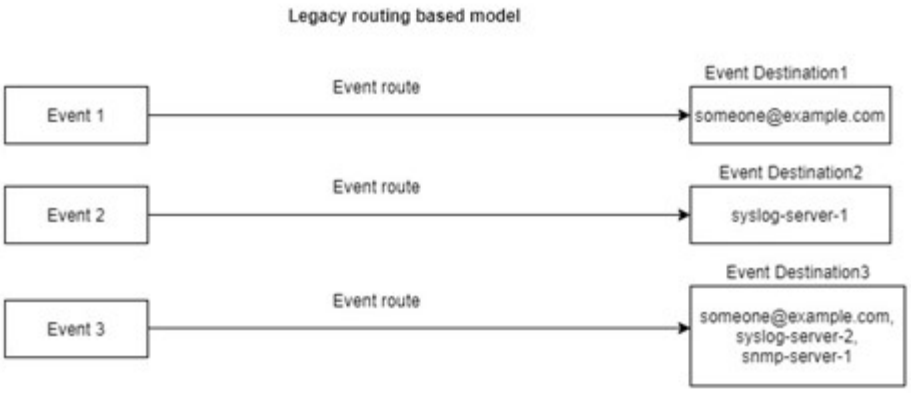
廃止されたモデルでは、コマンドを使用してEMSイベントがデスティネーションに個別にマッピングされ`event route add-destinations`ます。

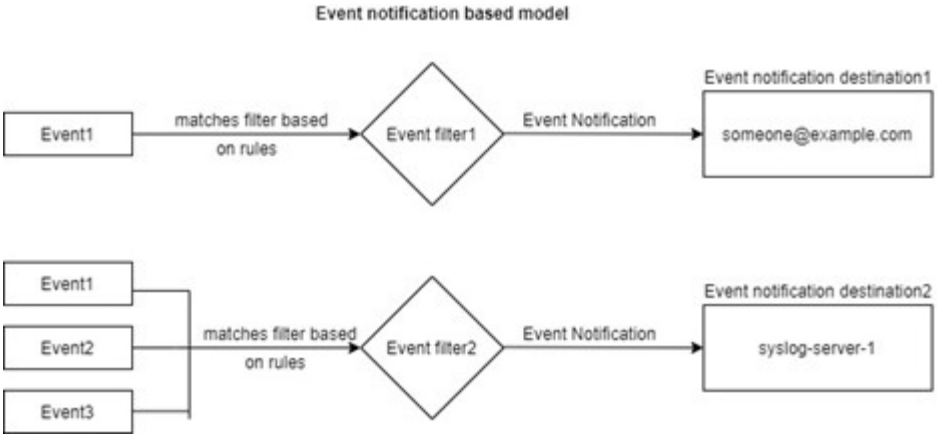
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

より拡張性に優れた新しいEMSイベント通知メカニズムは、イベントフィルタとイベント通知の送信先に基づいています。新しいイベント通知メカニズムの詳細については、次の技術情報アーティクルを参照してください。

- "ONTAP 9 のイベント管理システムの概要"





廃止されたコマンドから**ONTAP EMS**イベントマッピングを更新する

現在、廃止されたONTAPコマンドセットを使用してEMSイベントの(`event destination` `event route`マッピングが設定されている場合は、次の手順に従って、 `event notification`の各 `event notification destination`コマンドセットを使用するようにマッピングを更新する必要があります `event filter`。

手順

1. コマンドを使用して、システム内のすべてのイベントの送信先をリストします `event destination show`。

```
cluster-1::event*> destination show

Hide
Name              Mail Dest.         SNMP Dest.          Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                  -                  -
false
asup              -                  -                  -
false
criticals         -                  -                  -
false
pager             -                  -                  -
false
test              test@xyz.com       -                  -
false
traphost          -                  -                  -
false
6 entries were displayed.
```

2. 各送信先について、コマンドを使用してマッピングされているイベントを一覧表示します `event route show -destinations <destination name>`。

```
cluster-1::event*> route show -destinations test
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

3. これらすべてのイベントのサブセットを含む対応するを作成します `event filter`。たとえば、*イベントのみを含める `raid.aggr.`場合は、フィルタの作成時にパラメータにワイルドカードを使用し `message-name`ます。単一のイベントに対してフィルタを作成することもできます。

   の詳細については `event filter`、を"ONTAPコマンド リファレンス"参照してください。

   最大50個のイベントフィルタを作成できます。

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. 各エンドポイント（SMTP/SNMP/syslogなど）用に `event destination`を作成します。 `event notification destination`

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name             Type         Destination
--------------   ----------   --------------------
dest1            email        test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost    snmp         - (from "system snmp traphost")
2 entries were displayed.
```

および `event destination`の詳細については `event notification destination`、を"ONTAP コマンド リファレンス"参照してください。

5. イベントフィルタをイベント通知の送信先にマッピングして、イベント通知を作成します。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                      Destinations
---- -------------------------------  -----------------
1    default-trap-events              snmp-traphost
2    asup_events                      dest1
2 entries were displayed.
```

6. マッピングが設定されている `event route`ごとに、手順1～5を繰り返し `event destination`ます。

> SNMPの送信先にルーティングされたイベントは、イベント通知の送信先にマッピングする必要があります `snmp-traphost`。SNMPトラップホストの送信先は、システムで設定されたSNMPトラップホストを使用します。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

               Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

ONTAPコマンド リファレンス

ONTAPの各メジャーリリースでは、一般的に利用可能なCLIコマンド（ONTAPマニュアルページまたはマニュアルページ）が"ONTAP コマンドリファレンス" 。これらのコマンド リファレンスでは、各ONTAPリリースでのCLIコマンドの使い方が説明されています。

マニュアルページは、 ONTAPコマンドラインでも参照できます。 `man`指示。詳細はこちら `man`の中で"ONTAPコマンド リファレンス" 。

限定サポートバージョンのONTAPのコマンドリファレンス（PDFのみ）

- "ONTAP 9.4"

CLI比較ツール

NetAppサポートサイトのを使用して、ONTAPリリース間でのコマンドラインインターフェイス（CLI）コマンドの変更点を確認できます"CLI比較ツール"。

関連情報

- ONTAPコマンドラインインターフェイスの使用
- CLIコマンドディレクトリノイドウホウホウ
- "storage disk show"

法的通知

法的通知では、著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、およびNetAppの商標ページに記載されているマークは、NetApp、Inc.の商標です。その他の会社名および製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

ONTAP

"ONTAP 9.17.1 に関するお知らせ" "ONTAP 9.16.1に関する注意事項" "ONTAP 9.16.0に関する注意事項" "ONTAP 9.15.1に関する注意事項" "ONTAP 9.15.0に関する注意事項" "ONTAP 9.14.1に関する注意事項" "ONTAP 9.14.0に関する注意事項" "ONTAP 9.13.1に関する注意事項" "ONTAP 9.12.1に関する注意事項" "ONTAP 9.12.0に関する注意事項" "ONTAP 9.11.1に関する注意事項" "ONTAP 9.10.1に関する注意事項" "ONTAP 9.10.0に関する注意事項" "ONTAP 9.9.1に関する注意事項" "ONTAP 9.8に関する注意事項" "ONTAP 9.7に関する注意事項" "ONTAP 9.6に関する注意事項" "ONTAP 9.5に関する注意事項" "ONTAP 9.4に関する注意事項" "ONTAP 9.3に関する注意事項" "ONTAP 9.2に関する注意事項" "ONTAP 9.1に関する注意事項"

MetroCluster IP構成向けONTAPメディエーター

"9.9.1 ONTAP Mediator for MetroCluster IP構成に関する通知" "9.8 ONTAP Mediator for MetroCluster IP構成に関する通知" "9.7 ONTAP Mediator for MetroCluster IP構成に関する通知"

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。