



clustered Data ONTAP® 8.3

# ファイル アクセス管理ガイド (CIFS)

2015年6月 | 215-10729\_B0  
ng-gpso-jp-documents@netapp.com  
8.3.1用に更新



# 目次

|                                                                        |           |
|------------------------------------------------------------------------|-----------|
| <b>Data ONTAPにおけるSMBファイル アクセスの理解 .....</b>                             | <b>15</b> |
| FlexVolを備えたSVMでネームスペースとボリューム ジャンクションがSMBア<br>クセスに与える影響 .....           | 15        |
| FlexVolを備えたSVMのネームスペースとは .....                                         | 15        |
| ボリューム ジャンクションの使用に関するルール .....                                          | 15        |
| SMBおよびNFSネームスペースでのボリューム ジャンクションの使用<br>方法 .....                         | 16        |
| 一般的なNASネームスペース アーキテクチャとは .....                                         | 16        |
| ファイル アクセス管理のためのLIF設定要件 .....                                           | 19        |
| セキュリティ形式がデータ アクセスに与える影響 .....                                          | 20        |
| セキュリティ形式とその影響とは .....                                                  | 20        |
| セキュリティ形式を設定する場所とタイミング .....                                            | 21        |
| FlexVolを備えたSVMで使用するセキュリティ形式を決定する方法 .....                               | 21        |
| セキュリティ形式の継承の仕組み .....                                                  | 21        |
| 認証によってSMBアクセス セキュリティを確保する仕組み .....                                     | 22        |
| Kerberos認証 .....                                                       | 22        |
| NTLM認証 .....                                                           | 23        |
| FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセス<br>の保護方法 .....              | 23        |
| ネーム マッピングの仕組み .....                                                    | 23        |
| Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み .....                          | 24        |
| SMBアクセスでのエクスポート ポリシーの役割 .....                                          | 25        |
| CIFSの設定を大幅に変更すると、完了までにしばらく時間がかかることがあ<br>ります .....                      | 25        |
| <b>SVM(CIFSライセンスなし)用のActive Directoryコンピュータ アカウ<br/>ントの設定と管理 .....</b> | <b>26</b> |
| CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを<br>選択する方法 .....        | 26        |
| Active Directoryコンピュータ アカウントの管理 .....                                  | 27        |
| SVMのActive Directoryコンピュータ アカウントの作成 .....                              | 27        |
| SVMコンピュータ アカウントが関連付けられているActive Directoryド<br>メインの変更 .....             | 28        |
| SVMのActive Directoryコンピュータ アカウントに関する情報の表示 .....                        | 30        |
| SVMのActive Directoryコンピュータ アカウントの削除 .....                              | 30        |
| SVMのActive Directoryコンピュータ アカウント パスワードの変更また<br>はリセット .....             | 31        |
| Active Directoryコンピュータ アカウントのドメイン コントローラ接続の管理 .....                    | 32        |
| SVMで検出されたActive Directoryサーバに関する情報の表示 .....                            | 32        |
| Active Directoryサーバのリセットと再検出 .....                                     | 33        |
| 優先ドメイン コントローラの追加または削除 .....                                            | 34        |
| 優先ドメイン コントローラに関する情報の表示 .....                                           | 35        |

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>CIFSサーバのセットアップ .....</b>                                       | <b>36</b> |
| CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを<br>選択する方法 .....   | 36        |
| サポート対象のSMBクライアントおよびドメイン コントローラ .....                              | 37        |
| サポートされないWindowsの機能 .....                                          | 37        |
| CIFSサーバのセットアップの前提条件 .....                                         | 37        |
| CIFSサーバの設定の計画 .....                                               | 38        |
| タイム サービスを設定する前に収集する情報 .....                                       | 38        |
| IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収<br>集する情報 .....               | 39        |
| SVMを設定する前に収集する情報 .....                                            | 42        |
| SVM上でデータLIFを作成する前に収集する情報 .....                                    | 44        |
| ネーム サービスを設定する前に収集する情報 .....                                       | 46        |
| CIFSサーバを作成する前に収集する情報 .....                                        | 49        |
| CIFSサーバのセットアップ .....                                              | 50        |
| タイム サービスの設定(クラスタ管理者のみ) .....                                      | 52        |
| SVMのIPspaceの作成(クラスタ管理者のみ) .....                                   | 52        |
| 新しいブロードキャストドメインに使用できるポートの確認(クラスタ管<br>理者のみ) .....                  | 53        |
| 新しいブロードキャストドメインに追加するポートの既存のブロードキ<br>ャストドメインからの削除(クラスタ管理者のみ) ..... | 55        |
| IPspaceのブロードキャストドメインの作成(クラスタ管理者のみ) .....                          | 56        |
| IPspaceのサブネットの作成(クラスタ管理者のみ) .....                                 | 58        |
| CIFSサーバ用のFlexVolを備えたSVMの作成(クラスタ管理者のみ) .....                       | 59        |
| SVMでのLIFの作成(クラスタ管理者のみ) .....                                      | 61        |
| SVM用のDNSサービスの設定 .....                                             | 63        |
| SVMでの動的DNSの設定 .....                                               | 65        |
| CIFSサーバの作成 .....                                                  | 65        |
| SVM上のNISまたはLDAPネーム サービスの設定 .....                                  | 68        |
| Infinite VolumeのSMBサポートに関する情報の参照先 .....                           | 70        |
| <b>CIFSサーバの管理 .....</b>                                           | <b>71</b> |
| オプションを使用したCIFSサーバのカスタマイズ .....                                    | 71        |
| 使用できるCIFSサーバ オプション .....                                          | 71        |
| CIFSサーバ オプションの設定 .....                                            | 75        |
| 匿名ユーザに対するアクセス制限の設定 .....                                          | 76        |
| UNIXセキュリティ形式のデータに対するファイル セキュリティのSMB<br>クライアントへの提供方法の管理 .....      | 77        |
| CIFSサーバ オプションを使用してclustered Data ONTAPでDFSの自動<br>通知を制御する方法 .....  | 79        |
| CIFSサーバによるDFS対応の自動通知の管理 .....                                     | 80        |
| CIFSサーバのセキュリティ設定の管理 .....                                         | 81        |
| SVMディザスタリカバリ構成でのCIFSサーバ セキュリティ設定に関す<br>る重要な考慮事項 .....             | 81        |
| CIFSサーバのセキュリティ設定に関する情報の表示 .....                                   | 81        |

|                                                   |     |
|---------------------------------------------------|-----|
| ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化 .....          | 82  |
| CIFSサーバのKerberosセキュリティ設定の変更 .....                 | 83  |
| CIFSサーバの最低限の認証セキュリティレベルの設定 .....                  | 84  |
| AES暗号化によるKerberosベースの通信の強固なセキュリティ設定 .....         | 85  |
| SMB署名を使用したネットワークセキュリティの強化 .....                   | 87  |
| CIFSサーバのSMBを介したデータ転送に必要となるSMB暗号化の設定 .....         | 94  |
| SSL/TLS経由のLDAPを使用した通信の保護 .....                    | 97  |
| CIFSサーバでのデフォルトWindowsユーザからUNIXユーザへのマッピングの設定 ..... | 100 |
| デフォルトのUNIXユーザの設定 .....                            | 101 |
| ゲストUNIXユーザの設定 .....                               | 102 |
| ルートへのAdministratorsグループのマッピング .....               | 103 |
| SMBセッションを介して接続しているユーザのタイプに関する情報の表示 .....          | 104 |
| CIFSサーバでのSMBの設定 .....                             | 105 |
| サポートされるSMBのバージョン .....                            | 105 |
| SMB 2.xの有効化と無効化 .....                             | 108 |
| SMB 3.0の有効化と無効化 .....                             | 109 |
| 従来のoplockおよびoplockリリースでのクライアント パフォーマンスの向上 .....   | 110 |
| oplockを使用するときの書き込みキャッシュ データ消失に関する考慮事項 .....       | 110 |
| SMB共有の作成時におけるoplockの有効化と無効化 .....                 | 110 |
| 既存のSMB共有でのoplockの有効化と無効化 .....                    | 111 |
| ボリュームおよびqtreeでoplockを有効または無効にするコマンド .....         | 112 |
| oplockステータスの監視 .....                              | 113 |
| CIFSサーバへのグループ ポリシー オブジェクトの適用 .....                | 115 |
| サポートされるGPO .....                                  | 116 |
| CIFSサーバでGPOを使用するための要件 .....                       | 120 |
| CIFSサーバ上でのGPOサポートの有効化と無効化 .....                   | 120 |
| CIFSサーバでのGPOの更新方法 .....                           | 121 |
| CIFSサーバでのGPO設定の手動更新 .....                         | 122 |
| GPO設定に関する情報の表示 .....                              | 122 |
| 制限されたグループのGPOに関する詳細情報の表示 .....                    | 125 |
| 集約型アクセス ポリシーに関する情報の表示 .....                       | 127 |
| 集約型アクセス ポリシー ルールに関する情報の表示 .....                   | 128 |
| CIFSサーバのコンピュータ アカウント パスワードの変更 .....               | 130 |
| ドメイン アカウント パスワードの変更またはリセット .....                  | 130 |
| コンピュータ アカウント パスワードの自動変更のためのCIFSサーバの設定 .....       | 130 |
| CIFSサーバでのコンピュータ アカウント パスワードの自動変更の有効化 .....        | 131 |
| ドメイン コントローラ接続の管理 .....                            | 132 |
| 検出されたサーバに関する情報の表示 .....                           | 132 |
| サーバのリセットおよび再検出 .....                              | 132 |

|                                                   |            |
|---------------------------------------------------|------------|
| 優先ドメイン コントローラの追加 .....                            | 133        |
| 優先されるドメイン コントローラの管理用コマンド .....                    | 134        |
| CIFSサーバ用のNetBIOSエイリアスの管理 .....                    | 134        |
| CIFSサーバへのNetBIOSエイリアスのリストの追加 .....                | 134        |
| NetBIOSエイリアス リストからのNetBIOSエイリアスの削除 .....          | 135        |
| CIFSサーバのNetBIOSエイリアスのリストの表示 .....                 | 136        |
| SMBクライアントがNetBIOSエイリアスを使用して接続しているかどうかの確認 .....    | 137        |
| CIFSサーバに関するその他のタスクの管理 .....                       | 137        |
| SVMのプロトコルの変更 .....                                | 138        |
| CIFSサーバの停止と起動 .....                               | 139        |
| 別のOUへのCIFSサーバの移動 .....                            | 140        |
| CIFSサーバ移動前のSVM上の動的DNSドメインの変更 .....                | 140        |
| SVMのActive Directoryドメインへの参加 .....                | 141        |
| NetBIOS over TCP接続に関する情報の表示 .....                 | 142        |
| CIFSサーバの管理用コマンド .....                             | 142        |
| SMBアクセスとCIFSサービスでのIPv6の使用 .....                   | 143        |
| IPv6を使用するための要件 .....                              | 143        |
| SMBアクセスとCIFSサービスでのIPv6のサポート .....                 | 144        |
| IPv6を使用したCIFSサーバから外部サーバへの接続 .....                 | 145        |
| SMBでのIPv6の有効化(クラスタ管理者のみ) .....                    | 146        |
| SMBでのIPv6の無効化方法 .....                             | 146        |
| IPv6 SMBセッション情報の監視および表示 .....                     | 146        |
| <b>SMBを使用したファイル アクセスの設定 .....</b>                 | <b>147</b> |
| マルチプロトコル環境でのファイルとディレクトリの命名規則 .....                | 147        |
| ファイル名またはディレクトリ名に使用できる文字 .....                     | 147        |
| clustered Data ONTAPでファイル名とディレクトリ名が作成される仕組み ..... | 147        |
| マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別 .....        | 147        |
| セキュリティ形式の設定 .....                                 | 148        |
| SVMルート ボリュームでのセキュリティ形式の設定 .....                   | 149        |
| FlexVolでのセキュリティ形式の設定 .....                        | 149        |
| qtreeでのセキュリティ形式の設定 .....                          | 149        |
| NASネームスペースでのデータ ボリュームの作成と管理 .....                 | 150        |
| ジャンクション ポイントを指定したボリュームの作成 .....                   | 150        |
| ジャンクション ポイントが指定されていないデータ ボリュームの作成 .....           | 151        |
| NASネームスペースでの既存のボリュームのマウントまたはアンマウント .....          | 152        |
| ボリューム マウント ポイントとジャンクション ポイントに関する情報の表示 .....       | 153        |
| ストレージレベルのアクセス保護を使用したファイル アクセスの保護 .....            | 154        |
| ストレージレベルのアクセス保護の使用のユースケース .....                   | 156        |
| ストレージレベルのアクセス保護の設定ワークフロー .....                    | 156        |
| ストレージレベルのアクセス保護の設定 .....                          | 157        |

|                                                          |     |
|----------------------------------------------------------|-----|
| ストレージレベルのアクセス保護に関する情報の表示 .....                           | 162 |
| ストレージレベルのアクセス保護の削除 .....                                 | 163 |
| FlexVolでのSMBファイル名の変換のための文字マッピングの設定 .....                 | 164 |
| SMBファイル名の変換のための文字マッピングの管理コマンド .....                      | 166 |
| ネーム マッピングの作成 .....                                       | 167 |
| ネーム マッピングの変換ルール .....                                    | 167 |
| ネーム マッピングの作成 .....                                       | 168 |
| ネーム マッピングの管理用コマンド .....                                  | 169 |
| マルチドメイン ネーム マッピング検索の設定 .....                             | 170 |
| UNIXユーザからWindowsユーザへのネーム マッピングのためのマ<br>ルチドメイン検索 .....    | 170 |
| マルチドメイン ネーム マッピングの検索の有効化と無効化 .....                       | 172 |
| 信頼できるドメインのリセットおよび再検出 .....                               | 173 |
| 検出された信頼できるドメインに関する情報の表示 .....                            | 173 |
| 信頼できるドメインのリスト内の信頼できるドメインの追加、削除、また<br>は置換 .....           | 174 |
| 信頼できるドメインの優先リストに関する情報の表示 .....                           | 175 |
| SMB共有の作成と設定 .....                                        | 175 |
| デフォルトの管理共有とは .....                                       | 176 |
| 共有の命名に関する考慮事項 .....                                      | 177 |
| 非Unicodeクライアントはサポートされない .....                            | 178 |
| マルチプロトコル環境で共有を作成する際のディレクトリの大文字と小<br>文字の区別についての考慮事項 ..... | 178 |
| 共有パスの実行権限に関する要件の廃止 .....                                 | 178 |
| SMB共有の作成時に必要な情報 .....                                    | 179 |
| CIFSサーバでのSMB共有の作成 .....                                  | 180 |
| 既存のSMB共有に対する共有プロパティの追加または削除 .....                        | 187 |
| MMCを使用したSVM共有情報の表示 .....                                 | 189 |
| SMB共有の管理用コマンド .....                                      | 190 |
| SMB共有のACLを使用したファイル アクセスの保護 .....                         | 190 |
| SMB共有レベルACLの管理 .....                                     | 191 |
| Data ONTAPでの共有レベルのACLの使用方法 .....                         | 191 |
| SMB共有のACLの作成 .....                                       | 191 |
| SMB共有アクセス制御リストの管理用コマンド .....                             | 193 |
| ファイル権限を使用したファイル アクセスの保護 .....                            | 193 |
| Windowsの[セキュリティ]タブを使用した標準のNTFSファイル権限の<br>設定 .....        | 194 |
| Windowsの[セキュリティ]タブを使用した詳細なNTFSファイル権限の<br>設定 .....        | 196 |
| Data ONTAP CLIを使用したNTFSファイル権限の設定方法 .....                 | 199 |
| SMB経由でファイルにアクセスする際のUNIXファイル権限によるアク<br>セス制御方法 .....       | 199 |
| DAC(ダイナミック アクセス制御)を使用したファイル アクセスの保護 .....                | 200 |
| サポートされるダイナミック アクセス制御機能 .....                             | 201 |

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| CIFSサーバでダイナミック アクセス制御と集約型アクセス ポリシーを<br>使用する際の考慮事項 .....             | 202        |
| ダイナミック アクセス制御の有効化と無効化 .....                                         | 203        |
| CIFSサーバ上のデータを保護する集約型アクセス ポリシーの設定 .....                              | 204        |
| ダイナミック アクセス制御セキュリティに関する情報の表示 .....                                  | 206        |
| ダイナミック アクセス制御のリバートに関する考慮事項 .....                                    | 207        |
| ダイナミック アクセス制御と集約型アクセス ポリシーの設定方法およ<br>び使用方法の参照先 .....                | 208        |
| エクスポート ポリシーを使用したSMBアクセスの保護 .....                                    | 208        |
| SMBアクセスでのエクスポート ポリシーの使用方法 .....                                     | 209        |
| アップグレード時に既存のSMBエクスポート ポリシーが受ける影響 .....                              | 210        |
| SMBアクセスに関するエクスポート ポリシーの有効化と無効化 .....                                | 210        |
| エクスポート ルールの仕組み .....                                                | 212        |
| SMB経由のアクセスを制限または許可するエクスポート ポリシー ル<br>ールの例 .....                     | 213        |
| SMBのエクスポート ポリシーをリバートする際の考慮事項 .....                                  | 215        |
| <b>SMBを使用したファイル アクセスの管理 .....</b>                                   | <b>216</b> |
| ローカル ユーザおよびローカル グループを使用した認証と許可 .....                                | 216        |
| Data ONTAPでのローカル ユーザとローカル グループの使用方法 .....                           | 216        |
| ローカル権限とは .....                                                      | 220        |
| 要件および考慮事項 .....                                                     | 221        |
| 事前定義のBUILTINグループとそのデフォルトの権限 .....                                   | 222        |
| ローカル ユーザとローカル グループ機能の有効化と無効化 .....                                  | 224        |
| ローカル ユーザ アカウントの管理 .....                                             | 226        |
| ローカル グループの管理 .....                                                  | 232        |
| ローカル権限の管理 .....                                                     | 239        |
| トラバース チェックのバイパスの設定 .....                                            | 242        |
| ユーザまたはグループに対するディレクトリのトラバース チェックのバ<br>イパスの許可 .....                   | 244        |
| ユーザまたはグループに対するディレクトリのトラバース チェックのバ<br>イパスの禁止 .....                   | 245        |
| ファイル セキュリティと監査ポリシーに関する情報の表示 .....                                   | 246        |
| NTFSセキュリティ形式のボリュームのファイル セキュリティに関する<br>情報の表示 .....                   | 247        |
| mixedセキュリティ形式のボリュームのファイル セキュリティに関する<br>情報の表示 .....                  | 250        |
| UNIXセキュリティ形式のボリュームのファイル セキュリティに関する<br>情報の表示 .....                   | 252        |
| CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示 .....                           | 253        |
| CLIを使用したFlexVolのNFSv4監査ポリシーに関する情報の表示 .....                          | 255        |
| CLIを使用したSVMのNTFSファイル セキュリティ、NTFS監査ポリシー、ストレ<br>ージレベルのアクセス保護の管理 ..... | 257        |
| CLIを使用してファイルおよびフォルダのセキュリティを設定するユー<br>ースケース .....                    | 258        |



|                                                                                      |            |
|--------------------------------------------------------------------------------------|------------|
| CLIを使用してファイルおよびフォルダのセキュリティを設定する場合<br>の制限事項 .....                                     | 258        |
| セキュリティ記述子を使用したファイルおよびフォルダのセキュリティ<br>の適用方法 .....                                      | 259        |
| SVMディザスタリカバリ デスティネーションでローカル ユーザまたは<br>グループを使用するファイルとディレクトリのポリシーを適用する際<br>の考慮事項 ..... | 260        |
| CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリ<br>ティの設定および適用 .....                             | 261        |
| CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの<br>設定および適用 .....                                  | 275        |
| セキュリティ ポリシー ジョブの管理の考慮事項 .....                                                        | 287        |
| NTFSセキュリティ記述子の管理用コマンド .....                                                          | 288        |
| NTFS DACLアクセス制御エントリの管理用コマンド .....                                                    | 288        |
| NTFS SACLアクセス制御エントリの管理用コマンド .....                                                    | 288        |
| セキュリティ ポリシーの管理用コマンド .....                                                            | 289        |
| セキュリティ ポリシー タスクの管理用コマンド .....                                                        | 289        |
| セキュリティ ポリシー ジョブの管理用コマンド .....                                                        | 290        |
| セキュリティトレースを使用したファイルおよびディレクトリへのアクセスの検<br>証およびトラブルシューティング .....                        | 290        |
| セキュリティトレースの仕組み .....                                                                 | 290        |
| アクセスのタイプによるセキュリティトレース モニタのチェック .....                                                 | 291        |
| セキュリティトレースを作成する際の考慮事項 .....                                                          | 291        |
| セキュリティトレースの実行 .....                                                                  | 292        |
| セキュリティトレースの結果の解釈方法 .....                                                             | 299        |
| SMB共有のメタデータ キャッシュの設定 .....                                                           | 300        |
| SMBメタデータのキャッシングの仕組み .....                                                            | 300        |
| SMBメタデータのキャッシングの有効化 .....                                                            | 301        |
| SMBメタデータ キャッシュ エントリの有効期間の設定 .....                                                    | 301        |
| ファイル ロックの管理 .....                                                                    | 302        |
| プロトコル間のファイル ロックについて .....                                                            | 302        |
| Data ONTAPによる読み取り専用ビットの処理方法 .....                                                    | 302        |
| 共有パス コンポーネントのロックの処理に関するData ONTAPと<br>Windowsの違い .....                               | 303        |
| ロックに関する情報の表示 .....                                                                   | 303        |
| ロックの解除 .....                                                                         | 305        |
| SMBアクティビティの監視 .....                                                                  | 305        |
| SMBセッション情報の表示 .....                                                                  | 306        |
| 開いているSMBファイルに関する情報の表示 .....                                                          | 308        |
| 使用可能な統計オブジェクトと統計カウンタの確認 .....                                                        | 311        |
| 統計情報の表示 .....                                                                        | 313        |
| <b>CIFSクライアントベースのサービスの導入 .....</b>                                                   | <b>315</b> |
| オフライン ファイルを使用したオフラインで使用するファイルのキャッシング .....                                           | 315        |
| オフライン ファイルを使用するための要件 .....                                                           | 316        |
| オフライン ファイルを導入する際の考慮事項 .....                                                          | 316        |

|                                                                 |            |
|-----------------------------------------------------------------|------------|
| CLIを使用したSMB共有でのオフライン ファイル サポートの設定 .....                         | 317        |
| コンピュータの管理MMCを使用したSMB共有でのオフライン ファイル<br>サポートの設定 .....             | 318        |
| 移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザ<br>プロファイルの一元的な格納 .....     | 319        |
| 移動プロファイルを使用するための要件 .....                                        | 320        |
| 移動プロファイルの設定 .....                                               | 320        |
| フォルダ リダイレクトを使用したCIFSサーバへのデータの格納 .....                           | 320        |
| フォルダ リダイレクトを使用するための要件 .....                                     | 321        |
| フォルダ リダイレクトの設定 .....                                            | 321        |
| SMB 2.xを使用するWindowsクライアントからの~snapshotディレクトリへのアク<br>セス方法 .....   | 322        |
| 以前のバージョン機能を使用したファイルとフォルダのリカバリ .....                             | 323        |
| Microsoftの以前のバージョン機能を使用するための要件 .....                            | 323        |
| [以前のバージョン]タブを使用したSnapshotコピー データの表示およ<br>び管理 .....              | 324        |
| Snapshotコピーが以前のバージョン機能で使えるかどうかの確認 ..                            | 325        |
| 以前のバージョン機能のアクセスを有効にするSnapshot設定の作成 ....                         | 326        |
| ジャンクションを含むディレクトリをリストアする場合の考慮事項 .....                            | 326        |
| <b>CIFSサーバベースのサービスの導入 .....</b>                                 | <b>327</b> |
| ホーム ディレクトリの管理 .....                                             | 327        |
| clustered Data ONTAPにおける動的ホーム ディレクトリの仕組み .....                  | 327        |
| ホーム ディレクトリ共有の追加 .....                                           | 328        |
| ホーム ディレクトリ検索パスの追加 .....                                         | 330        |
| %w変数と%d変数を使用したホーム ディレクトリ設定の作成 .....                             | 331        |
| %u変数を使用したホーム ディレクトリ の設定 .....                                   | 333        |
| 追加のホーム ディレクトリ の設定 .....                                         | 336        |
| 検索パスの管理用コマンド .....                                              | 336        |
| SMBユーザのホーム ディレクトリ パスに関する情報の表示 .....                             | 337        |
| ユーザのホーム ディレクトリへのアクセスの管理 .....                                   | 337        |
| UNIXシンボリック リンクへのSMBクライアント アクセスの設定 .....                         | 338        |
| Data ONTAPを使用してUNIXシンボリック リンクへのSMBクライアント<br>アクセスを提供する方法 .....   | 339        |
| SMBアクセス用にUNIXシンボリック リンクを設定する場合の制限 .....                         | 340        |
| CIFSサーバオプションを使用してclustered Data ONTAPでDFSの自動<br>通知を制御する方法 ..... | 340        |
| CIFSサーバによるDFS対応の自動通知の管理 .....                                   | 341        |
| SMB共有でのUNIXシンボリック リンク サポートの設定 .....                             | 342        |
| SMB共有のシンボリック リンク マッピングの作成 .....                                 | 343        |
| シンボリック リンクのマッピングの管理用コマンド .....                                  | 344        |
| BranchCacheを使用したブランチ オフィスでのSMB共有のコンテンツのキャッ<br>シュ .....          | 344        |
| 要件、考慮事項、および推奨事項 .....                                           | 345        |
| BranchCacheの設定 .....                                            | 348        |
| BranchCache対応のSMB共有の設定 .....                                    | 352        |

|                                                                                 |            |
|---------------------------------------------------------------------------------|------------|
| BranchCacheの設定の管理および監視 .....                                                    | 355        |
| SMB共有でのBranchCacheの無効化 .....                                                    | 363        |
| SVMでのBranchCacheの無効化と有効化 .....                                                  | 365        |
| SVMのBranchCache設定の削除 .....                                                      | 367        |
| リバートした場合のBranchCacheの動作 .....                                                   | 368        |
| Microsoftリモートコピーのパフォーマンスの向上 .....                                               | 368        |
| ODXの仕組み .....                                                                   | 369        |
| ODXの使用要件 .....                                                                  | 370        |
| ODXを使用する場合の考慮事項 .....                                                           | 371        |
| ODXのユースケース .....                                                                | 372        |
| ODXの有効化と無効化 .....                                                               | 373        |
| Auto LocationでSMB自動ノード リファールを提供することでクライアントの<br>応答時間を改善 .....                    | 373        |
| 自動ノード リファールを使用する際の要件と考慮事項 .....                                                 | 374        |
| 自動ノード リファールのサポート .....                                                          | 376        |
| SMB自動ノード リファールの有効化と無効化 .....                                                    | 377        |
| 統計を使用した自動ノード リファール アクティビティの監視 .....                                             | 377        |
| Windowsクライアントを使用してクライアント側のSMB自動ノード リファ<br>ール情報を監視する方法 .....                     | 379        |
| アクセススペースの列挙を使用した共有のフォルダのセキュリティ確保 .....                                          | 379        |
| SMB共有でのアクセススペースの列挙の有効化と無効化 .....                                                | 380        |
| Windowsクライアントからのアクセススペースの列挙の有効化と無効化 ...                                         | 381        |
| <b>Microsoft Hyper-VおよびSQL Server over SMBソリューション用の<br/>Data ONTAPの設定 .....</b> | <b>382</b> |
| Hyper-VおよびSQL Server over SMBのノンストップ オペレーションとは .....                            | 382        |
| SMB経由のノンストップ オペレーションを実現するプロトコル .....                                            | 383        |
| Hyper-VおよびSQL Server over SMBでのノンストップ オペレーション<br>の主要な概念 .....                   | 383        |
| SMB 3.0の機能がSMB共有を介したノンストップ オペレーションをサ<br>ポートする仕組み .....                          | 385        |
| 透過的なフェイルオーバーを強化するための監視プロトコルの機能 .....                                            | 385        |
| リモートVSSによる共有ベースのバックアップ .....                                                    | 387        |
| リモートVSSの概念 .....                                                                | 387        |
| リモートVSSで使用されるディレクトリ構造の例 .....                                                   | 388        |
| SnapManager for Hyper-VによるHyper-V over SMBのリモートVSSベ<br>ースのバックアップの管理方法 .....     | 389        |
| Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピー オフロ<br>ードの使用方法 .....           | 390        |
| 設定要件と考慮事項 .....                                                                 | 392        |
| Data ONTAPとライセンスの要件 .....                                                       | 392        |
| ネットワークとデータLIFの要件 .....                                                          | 393        |
| Hyper-V over SMB用のCIFSサーバとボリュームの要件 .....                                        | 393        |
| SQL Server over SMB用のCIFSサーバとボリュームの要件 .....                                     | 394        |
| Hyper-V over SMBでの継続的可用性を備えた共有の要件と考慮事<br>項 .....                                | 395        |

|                                                                                 |            |
|---------------------------------------------------------------------------------|------------|
| SQL Server over SMBでの継続的可用性を備えた共有の要件と考慮事項 .....                                 | 397        |
| Hyper-V over SMB構成用のリモートVSSの考慮事項 .....                                          | 398        |
| SQL ServerおよびHyper-V over SMB用のODXコピー オフロード要件 ..                                | 399        |
| SQL ServerおよびHyper-V over SMB構成に関する推奨事項 .....                                   | 399        |
| Hyper-VまたはSQL Server over SMB構成の計画 .....                                        | 400        |
| ボリューム設定ワークシートの完了 .....                                                          | 400        |
| SMB共有設定ワークシートの完了 .....                                                          | 401        |
| Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成 ..... | 403        |
| Kerberos認証およびNTLMv2認証の許可の確認 (Hyper-V over SMB共有) .....                          | 404        |
| ドメイン アカウントがデフォルトのUNIXユーザにマッピングされていることの確認 .....                                  | 405        |
| SVMルート ボリュームのセキュリティ形式がNTFSに設定されていることの確認 .....                                   | 407        |
| 必要なCIFSサーバ オプションの設定の確認 .....                                                    | 408        |
| 自動ノード リファラルの無効化の確認 .....                                                        | 409        |
| NTFSデータ ボリュームの作成 .....                                                          | 410        |
| 継続的可用性を備えたSMB共有の作成 .....                                                        | 411        |
| ユーザ アカウント(SMB共有のSQL Server用)へのSeSecurityPrivilege 権限の追加 .....                   | 412        |
| VSSシャドウ コピーのディレクトリ階層の設定 (Hyper-V over SMB要求用) .....                             | 413        |
| Hyper-VおよびSQL Server over SMB構成の管理 .....                                        | 413        |
| 継続的な可用性を確保するための既存の共有の設定 .....                                                   | 414        |
| Hyper-V over SMBバックアップでのVSSシャドウ コピーの有効化と無効化 .....                               | 416        |
| Hyper-V over SMB構成をリバートする際の考慮事項 .....                                           | 417        |
| SQL Server over SMB構成をリバートする際の考慮事項 .....                                        | 417        |
| 統計を使用したHyper-VおよびSQL Server over SMBアクティビティの監視 .....                            | 418        |
| 使用可能な統計オブジェクトと統計カウンタの確認 .....                                                   | 418        |
| SMB統計の表示 .....                                                                  | 420        |
| 非破壊的な操作が可能であることの確認 .....                                                        | 420        |
| ヘルス監視を使用してノンストップ オペレーションのステータスが正常かどうかを確認する方法 .....                              | 420        |
| システム ヘルスの監視を使用したノンストップ オペレーションのステータスの表示 .....                                   | 421        |
| SMB共有の継続的な可用性の設定の確認 .....                                                       | 422        |
| LIFステータスの確認 .....                                                               | 424        |
| SMBセッションの継続的可用性の確認 .....                                                        | 425        |
| <b>FlexVolを備えたSVMでのNASイベントの監査 .....</b>                                         | <b>432</b> |
| 監査の仕組み .....                                                                    | 432        |
| 監査の基本概念 .....                                                                   | 432        |
| Data ONTAP監査プロセスの仕組み .....                                                      | 433        |

|                                                            |            |
|------------------------------------------------------------|------------|
| 監査を有効にする際のアグリゲート スペースに関する考慮事項 .....                        | 435        |
| 監査の要件と考慮事項 .....                                           | 435        |
| サポートされる監査イベント ログの形式 .....                                  | 436        |
| 監査イベント ログの表示 .....                                         | 436        |
| イベントビューアを使用したアクティブな監査ログの表示方法 .....                         | 437        |
| 監査できるSMBイベント .....                                         | 438        |
| 監査対象オブジェクトへの完全パスの決定 .....                                  | 440        |
| シンボリックリンクおよびハード リンクを監査する際の考慮事項 .....                       | 440        |
| NTFS代替データ ストリームを監査する際の考慮事項 .....                           | 441        |
| 監査できるNFSファイルおよびディレクトリのアクセス イベント .....                      | 442        |
| 監査設定の計画 .....                                              | 443        |
| SVMでのファイルとディレクトリの監査設定の作成 .....                             | 448        |
| 監査設定の作成 .....                                              | 448        |
| SVMでの監査の有効化 .....                                          | 450        |
| 監査設定の確認 .....                                              | 450        |
| ファイルおよびフォルダの監査ポリシーの設定 .....                                | 450        |
| NTFSセキュリティ形式のファイルおよびディレクトリの監査ポリシーの<br>設定 .....             | 451        |
| UNIXセキュリティ形式のファイルおよびディレクトリの監査設定 .....                      | 455        |
| ファイルおよびディレクトリに適用されている監査ポリシーに関する情報の表<br>示 .....             | 455        |
| Windowsの[セキュリティ]タブを使用した監査ポリシーに関する情報の<br>表示 .....           | 455        |
| CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示 .....                  | 457        |
| 監査設定の管理 .....                                              | 459        |
| 監査イベント ログの手動ローテーション .....                                  | 459        |
| SVMでの監査の有効化と無効化 .....                                      | 459        |
| 監査設定に関する情報の表示 .....                                        | 461        |
| 監査設定を変更するコマンド .....                                        | 462        |
| 監査設定の削除 .....                                              | 462        |
| リバート時のプロセス .....                                           | 463        |
| 監査およびステージング用のボリュームのスペースに関する問題のトラブル<br>シューティング .....        | 463        |
| イベント ログ ボリュームに関するスペースの問題のトラブルシューティ<br>ング方法 .....           | 463        |
| ステージング ボリュームに関するスペースの問題のトラブルシューテ<br>イング方法(クラスタ管理者のみ) ..... | 464        |
| <b>FlexVolを備えたSVMでのFPolicyによるファイルの監視と管理 .....</b>          | <b>465</b> |
| FPolicyの仕組み .....                                          | 465        |
| FPolicyソリューションの2つの要素とは .....                               | 465        |
| 同期通知および非同期通知とは .....                                       | 465        |
| FPolicyの実装でクラスタ コンポーネントが果たす役割 .....                        | 466        |
| FPolicyと外部FPolicyサーバとの連携 .....                             | 467        |
| ノードと外部FPolicyサーバの間の通信プロセス .....                            | 468        |
| SVMネームスペースにおけるFPolicyサービスの仕組み .....                        | 470        |

|                                                |            |
|------------------------------------------------|------------|
| FPolicyの設定タイプ .....                            | 470        |
| ネイティブFPolicyの設定を作成する場合 .....                   | 471        |
| 外部FPolicyサーバを使用する設定を作成する状況 .....               | 471        |
| FPolicyのパススルー リードによる階層型ストレージ管理のユーザビリティ向上 ..... | 472        |
| FPolicyパススルー リードが有効になっている場合の読み取り要求の処理方法 .....  | 473        |
| FPolicyを設定するための要件、考慮事項、およびベストプラクティス .....      | 473        |
| FPolicyの設定方法 .....                             | 473        |
| FPolicyを設定するための要件 .....                        | 473        |
| FPolicyを設定する際のベストプラクティスと推奨事項 .....             | 474        |
| パススルー リードのアップグレードおよびリバートに関する考慮事項 ....          | 474        |
| FPolicyの設定手順とは .....                           | 475        |
| FPolicy構成の計画 .....                             | 476        |
| FPolicy外部エンジンの設定の計画 .....                      | 476        |
| FPolicyイベントの設定の計画 .....                        | 483        |
| FPolicyポリシーの設定の計画 .....                        | 488        |
| FPolicyスコープの設定の計画 .....                        | 493        |
| FPolicyの設定の作成 .....                            | 496        |
| FPolicy外部エンジンの作成 .....                         | 497        |
| FPolicyポリシー イベントの作成 .....                      | 498        |
| FPolicyポリシーの作成 .....                           | 499        |
| FPolicyスコープの作成 .....                           | 500        |
| FPolicyポリシーの有効化 .....                          | 501        |
| FPolicyの設定の変更 .....                            | 501        |
| FPolicy設定の変更改用コマンド .....                       | 502        |
| FPolicyポリシーの有効化と無効化 .....                      | 502        |
| FPolicyの設定に関する情報の表示 .....                      | 503        |
| showコマンドの仕組み .....                             | 503        |
| FPolicyの設定に関する情報を表示するコマンド .....                | 503        |
| FPolicyポリシーのステータスに関する情報の表示 .....               | 504        |
| 有効なFPolicyポリシーに関する情報の表示 .....                  | 505        |
| FPolicyサーバの接続の管理 .....                         | 505        |
| 外部FPolicyサーバへの接続 .....                         | 506        |
| 外部FPolicyサーバからの切断 .....                        | 506        |
| 外部FPolicyサーバへの接続に関する情報の表示 .....                | 506        |
| FPolicyパススルー リード接続のステータスに関する情報の表示 .....        | 508        |
| <b>著作権に関する情報 .....</b>                         | <b>510</b> |
| <b>商標に関する情報 .....</b>                          | <b>511</b> |
| <b>マニュアルの更新について .....</b>                      | <b>512</b> |
| <b>索引 .....</b>                                | <b>513</b> |

## Data ONTAPにおけるSMBファイル アクセスの理解

CIFSサーバを設定し、SMBクライアントがクラスタのファイルにアクセスできるようにSMB共有を設定する前に、SMBファイル アクセスの概念について確認しておく必要があります。

### FlexVolを備えたSVMでネームスペースとボリューム ジャンクションがSMBアクセスに与える影響

ネームスペースおよびボリューム ジャンクションとは何かを理解し、ストレージ環境のStorage Virtual Machine (SVM) 上のSMBアクセスを正しく設定するためのそれらの使用方法を把握しておく必要があります。

#### 関連コンセプト

[NASネームスペースでのデータ ボリュームの作成と管理](#)(150ページ)

#### 関連タスク

[FlexVolでのSMBファイル名の変換のための文字マッピングの設定](#)(164ページ)

### FlexVolを備えたSVMのネームスペースとは

ネームスペースとは、複数のボリュームをジャンクション ポイントで論理的にグループ化して、Storage Virtual Machine (SVM) のルート ボリュームから派生する1つの論理的なファイルシステムにまとめたものです。SVMごとにネームスペースが1つあります。

データSVMのCIFSサーバおよびNFSサーバは、ネームスペース内にデータを格納し、ネームスペース内のデータにアクセスできます。各クライアントは、ネームスペースの最上位にエクスポートをマウントするか最上位にある単一のSMB共有にアクセスすることで、ネームスペース全体にアクセスすることができます。

SVM管理者が各ボリューム ジャンクションにエクスポートを作成することもできます。この場合、クライアントはネームスペース内の中間的地点にマウントポイントを作成したり、ネームスペース内の任意のディレクトリ パスをポイントするCIFS共有を作成することができます。

ボリュームは、ネームスペース内の任意の場所にマウントすることでいつでも追加できます。新たに追加されたボリュームのジャンクションよりも上位のネームスペース内の場所にアクセスしているクライアントは、十分な権限があれば、新しいボリュームにすぐにアクセスすることができます。

### ボリューム ジャンクションの使用に関するルール

ボリューム ジャンクションは、複数のボリュームを1つの論理ネームスペースにまとめて、NASクライアントにデータ アクセスを提供する方法です。ボリューム ジャンクションがどのように構成されるかを理解しておけば、そのルールを理解して使用することができます。

NASクライアントからジャンクション経由でデータにアクセスする際、ジャンクションは通常のディレクトリと同じように表示されます。ジャンクションは、ルートより下のマウントポイントにボリュームをマウントすると形成され、それを使用してファイルシステム ツリーが作成されます。ファイルシステム ツリーの最上位は常にルート ボリュームであり、スラッシュ(/)で表されます。ジャンクションは、あるボリュームのディレクトリから別のボリュームのルート ディレクトリへの接合点になります。

- ジャンクション ポイントを指定せずにボリュームを作成することもできますが、ネームスペース内のジャンクション ポイントにボリュームをマウントするまでは、ボリューム内のデータをエクスポートしたり(NFS)、共有を作成したり(CIFS)することはできません。
- ボリュームを作成時にマウントしなかった場合は、作成後にマウントできます。

- ボリュームをジャンクション ポイントにマウントすることで、ネームスペースにいつでも新しいボリュームを追加できます。
- マウント済みのボリュームをアンマウントできます。ただし、ボリュームのアンマウント中は、ボリュームのすべてのデータに対するNASクライアントからのアクセスが中断され、アンマウントするボリュームの下にある子ジャンクション ポイントにマウントされているボリュームにもアクセスできなくなります。
- ジャンクション ポイントは、親ボリューム ジャンクションのすぐ下に作成することも、ボリューム内のディレクトリに作成することもできます。  
たとえば、「vol3」というボリュームのジャンクションのパスは、/vol1/vol2/vol3や/vol1/dir2/vol3でも、/dir1/dir2/vol3でもかまいません。

## SMBおよびNFSネームスペースでのボリューム ジャンクションの使用方法

ネームスペース内のいずれかのジャンクション ポイントにボリュームをマウントすると、単一の論理ネームスペースが作成されます。ボリュームの作成時にジャンクション ポイントを指定した場合、そのボリュームは作成された時点で自動的にマウントされ、NASアクセスに使用できるようになります。マウントしたボリュームにはSMB共有およびNFSエクスポートを作成できます。

ジャンクション ポイントを指定しない場合、ボリュームはオンラインになりますが、NASのファイルアクセス用にマウントされません。NASのファイル アクセス用にボリュームを使用できるようにするには、ボリュームをジャンクション ポイントにマウントする必要があります。

## 一般的なNASネームスペース アーキテクチャとは

すべてのStorage Virtual Machine (SVM) ネームスペースはルート ボリュームから派生しますが、SVMネームスペースを作成するときに使用できる一般的なNASネームスペース アーキテクチャがいくつかあります。ビジネス要件やワークフロー要件に合わせて、ネームスペース アーキテクチャを選択できます。

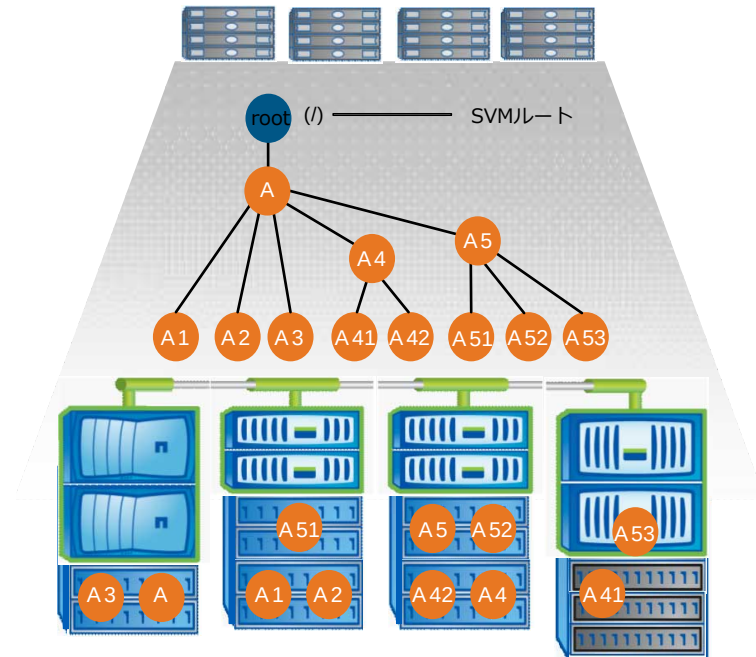
ネームスペース階層の最上位は常にルートボリュームであり、スラッシュ(/)で表します。ルートの下位のネームスペース アーキテクチャは以下の3つの基本カテゴリに分類されます。

- ネームスペースのルートへのジャンクション ポイントが1つだけの単一のブランチ ツリー
- ネームスペースのルートへのジャンクション ポイントが複数ある複数のブランチ ツリー
- ボリュームごとにネームスペースのルートへの個別のジャンクション ポイントがある複数のスタンドアロン ボリューム

### 単一のブランチ ツリーのネームスペース

単一のブランチ ツリーのアーキテクチャでは、SVMネームスペースのルートへの挿入ポイントが1つあります。この挿入ポイントは、ルートの下位のジャンクションされたボリュームまたはディレクトリのどちらかです。それ以外のすべてのボリュームは、この挿入ポイントの下位のジャンクション ポイント(ボリュームまたはディレクトリ)でマウントされます。



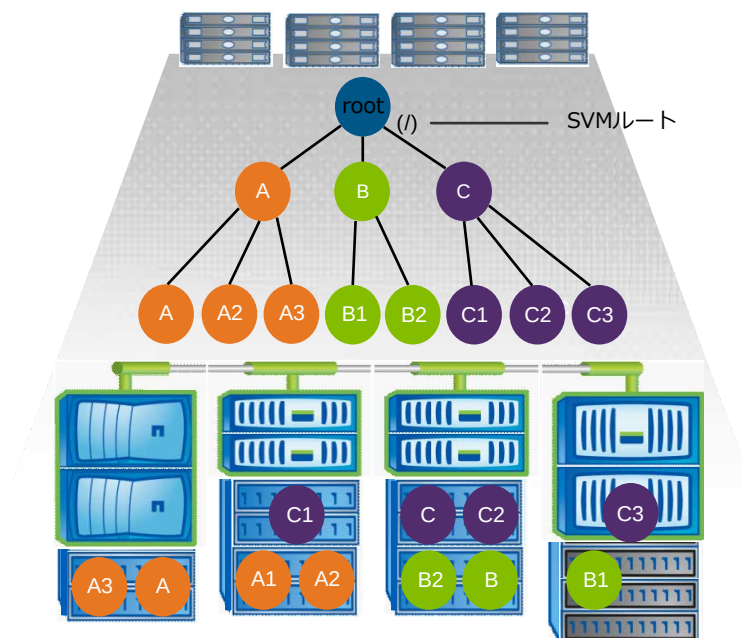


たとえば、上記のネームスペース アーキテクチャを使用する一般的なボリューム ジャンクション構成は、すべてのボリュームが単一の挿入ポイント(「data」という名前のディレクトリ)の下にジャンクションされる次のような構成になります。

| Vserver | Volume   | Junction Active | Junction Path     | Junction Path Source |
|---------|----------|-----------------|-------------------|----------------------|
| vs1     | corp1    | true            | /data/dir1/corp1  | RW_volume            |
| vs1     | corp2    | true            | /data/dir1/corp2  | RW_volume            |
| vs1     | data1    | true            | /data/data1       | RW_volume            |
| vs1     | eng1     | true            | /data/data1/eng1  | RW_volume            |
| vs1     | eng2     | true            | /data/data1/eng2  | RW_volume            |
| vs1     | sales    | true            | /data/data1/sales | RW_volume            |
| vs1     | vol1     | true            | /data/vol1        | RW_volume            |
| vs1     | vol2     | true            | /data/vol2        | RW_volume            |
| vs1     | vol3     | true            | /data/vol3        | RW_volume            |
| vs1     | vs1_root | -               | /                 | -                    |

### 複数のブランチ ツリーのネームスペース

複数のブランチ ツリーのネームスペースには、SVMネームスペースのルートへの挿入ポイントが複数あります。挿入ポイントは、ルートの下で結合(ジャンクション)されたボリュームまたはディレクトリのどちらかです。それ以外のすべてのボリュームは、これらの挿入ポイントの下のジャンクション ポイント(ボリュームまたはディレクトリ)でマウントされます。

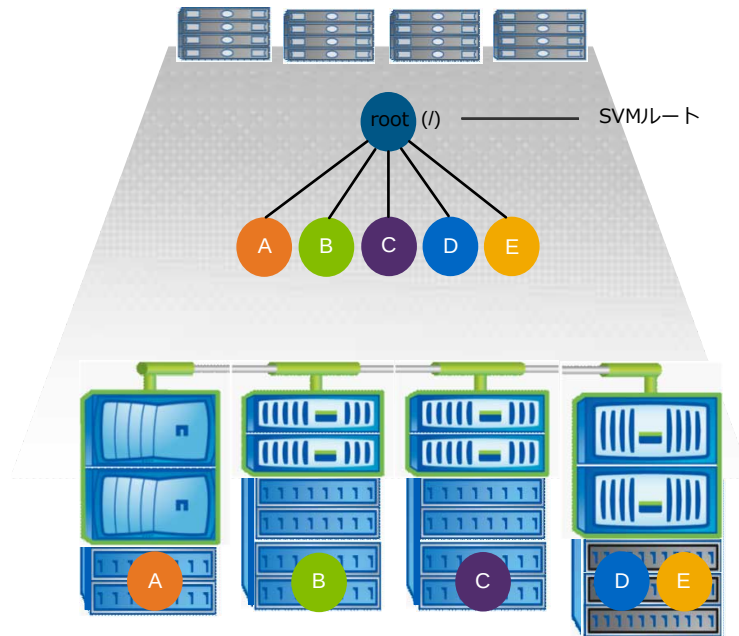


たとえば、上記のネームスペース アーキテクチャを使用する標準的なボリューム ジャンクション構成は、SVMのルートボリュームへの3つの挿入ポイントがある以下のような構成になります。挿入ポイントのうち2つは、それぞれ「data」、「projects」という名前のディレクトリです。もう1つの挿入ポイントは、「audit」という名前のジャンクション ボリュームです。

| Vserver | Volume      | Junction Active | Junction Path      | Junction Path Source |
|---------|-------------|-----------------|--------------------|----------------------|
| vs1     | audit       | true            | /audit             | RW_volume            |
| vs1     | audit_logs1 | true            | /audit/logs1       | RW_volume            |
| vs1     | audit_logs2 | true            | /audit/logs2       | RW_volume            |
| vs1     | audit_logs3 | true            | /audit/logs3       | RW_volume            |
| vs1     | eng         | true            | /data/eng          | RW_volume            |
| vs1     | mktg1       | true            | /data/mktg1        | RW_volume            |
| vs1     | mktg2       | true            | /data/mktg2        | RW_volume            |
| vs1     | project1    | true            | /projects/project1 | RW_volume            |
| vs1     | project2    | true            | /projects/project2 | RW_volume            |
| vs1     | vs1_root    | -               | /                  | -                    |

### 複数のスタンドアロン ボリュームのネームスペース

スタンドアロン ボリュームのアーキテクチャでは、すべてのボリュームにSVMネームスペースのルートへの挿入ポイントがありますが、ボリュームは別のボリュームの下でジャンクションされていません。各ボリュームは一意のパスを持ち、ルート直下でジャンクションされているか、ルートの下のディレクトリでジャンクションされています。



たとえば、上記のネームスペース アーキテクチャを使用する標準的なボリューム ジャンクション構成は、SVMのルート ボリュームへの5つの挿入ポイントがあり、それぞれが1つのボリュームへのパスを表す以下のような構成になります。

| Vserver | Volume   | Junction Active | Junction Path | Junction Path Source |
|---------|----------|-----------------|---------------|----------------------|
| vs1     | eng      | true            | /eng          | RW_volume            |
| vs1     | mktg     | true            | /vol/mktg     | RW_volume            |
| vs1     | project1 | true            | /project1     | RW_volume            |
| vs1     | project2 | true            | /project2     | RW_volume            |
| vs1     | sales    | true            | /sales        | RW_volume            |
| vs1     | vs1_root | -               | /             | -                    |

## ファイル アクセス管理のためのLIF設定要件

ファイル アクセス制御を適切に管理するため、Data ONTAPは、NIS、LDAP、およびActive Directoryサーバなどの外部サービスと通信します。Storage Virtual Machine (SVM) のLIFは、これらの通信を許可するように正しく設定されている必要があります。

外部サービスとの通信は、SVMのデータLIFを介して行われます。したがって、各ノードでSVMのデータLIFがすべての必要な外部サービスに到達できるように正しく設定されていることを確認してください。

### 関連コンセプト

[CIFSサーバのセットアップ](#) (50ページ)

### 関連情報

[clustered Data ONTAP 8.3 ネットワーク管理ガイド](#)

## セキュリティ形式がデータ アクセスに与える影響

ストレージ システムの各ボリュームおよびqtrelには、セキュリティ形式が設定されています。セキュリティ形式は、ユーザを許可する際に使用されるボリュームのデータに対するアクセス権のタイプを決定します。どのようなセキュリティ形式があるかを把握し、その設定のタイミングと場所、アクセス権への影響、ボリューム タイプによる違いなどについて理解しておく必要があります。

### 関連コンセプト

[UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法の管理](#)(77ページ)

### 関連タスク

[SVMルート ボリュームでのセキュリティ形式の設定](#) (149ページ)

[FlexVolでのセキュリティ形式の設定](#)(149ページ)

[qtrelでのセキュリティ形式の設定](#)(149ページ)

## セキュリティ形式とその影響とは

セキュリティ形式には、UNIX、NTFS、mixed、およびunifiedの4種類があり、セキュリティ形式ごとにデータに対する権限の扱いが異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データ アクセスの制御にData ONTAPで使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、あるボリュームでUNIXセキュリティ形式を使用している場合でも、Data ONTAPはマルチプロトコルに対応しているため、SMBクライアントは引き続きデータにアクセスできます (適切に認証および許可されている場合)。ただしData ONTAPが使用するのはUNIX権限で、これはUNIXクライアントのみが標準ツールを使用して変更できます。

| セキュリティ形式                       | 権限を変更できるクライアント | クライアントが使用できる権限 | 有効になるセキュリティ形式 | ファイルにアクセスできるクライアント |
|--------------------------------|----------------|----------------|---------------|--------------------|
| UNIX                           | NFS            | NFSv3モード ビット   | UNIX          | NFSとSMB            |
|                                |                | NFSv4.x ACL    | UNIX          |                    |
| NTFS                           | SMB            | NTFS ACL       | NTFS          |                    |
| mixed                          | NFSまたはSMB      | NFSv3モード ビット   | UNIX          |                    |
|                                |                | NFSv4.x ACL    | UNIX          |                    |
|                                |                | NTFS ACL       | NTFS          |                    |
| unified<br>(Infinite Volumeのみ) | NFSまたはSMB      | NFSv3モード ビット   | UNIX          |                    |
|                                |                | NFSv4.1 ACL    | UNIX          |                    |
|                                |                | NTFS ACL       | NTFS          |                    |

セキュリティ形式がmixedまたはunifiedの場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。権限を最後に変更したクライアントがNFSv3クライアントの場合、権限はUNIX NFSv3モード ビットになります。最後のクライアントがNFSv4クライアントの場合、権限はNFSv4 ACLになります。最後のクライアントがSMBクライアントの場合、権限はWindows NTFS ACLになります。

**注:** Data ONTAPは最初にデフォルトのファイル権限をいくつか設定します。デフォルトでは、UNIX、mixed、およびunifiedのセキュリティ形式のボリュームにあるデータについては、セキュリティ形式はUNIX、権限の種類はUNIXモードビット（特に指定しないかぎり0755）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントが設定するまで変わりません。同様に、NTFSセキュリティ形式のボリュームにあるデータについては、デフォルトでNTFSセキュリティ形式が有効になり、すべてのユーザにフル コントロール権限を許可するACLが割り当てられます。

#### 関連情報

[Clustered Data ONTAP 8.3 Infinite Volumes Management Guide](#)

## セキュリティ形式を設定する場所とタイミング

セキュリティ形式は、FlexVol（ルートボリュームとデータボリュームのどちらでも可）およびqtree上に設定できます。セキュリティ形式は、作成時に手作業で設定したり、自動的に継承したり、後から変更したりすることができます。

**注:** Infinite Volumeは、常にunifiedセキュリティ形式を使用します。Infinite Volumeのセキュリティ形式は設定も変更もできません。

## FlexVolを備えたSVMで使用するセキュリティ形式を決定する方法

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります。第1の要素は、ファイルシステムの管理者のタイプで、第2の要素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定する際には、環境のニーズを考慮して最適なセキュリティ形式を選択し、アクセス権の管理に関する問題を回避する必要があります。以下は決定時に考慮すべき項目です。

| セキュリティ形式 | 以下の場合に選択                                                                                                                                                                    |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNIX     | <ul style="list-style-type: none"> <li>ファイルシステムがUNIX管理者によって管理されている。</li> <li>ユーザの大半がNFSクライアントである。</li> <li>データにアクセスするアプリケーションで、サービス アカウントとしてUNIXユーザが使用される。</li> </ul>       |
| NTFS     | <ul style="list-style-type: none"> <li>ファイルシステムがWindows管理者によって管理されている。</li> <li>ユーザの大半がSMBクライアントである。</li> <li>データにアクセスするアプリケーションで、サービス アカウントとしてWindowsユーザが使用される。</li> </ul> |
| mixed    | ファイルシステムがUNIX管理者とWindows管理者の両方によって管理され、ユーザがNFSクライアントとSMBクライアントの両方で構成される。                                                                                                    |

## セキュリティ形式の継承の仕組み

新しいFlexVolまたはqtreeの作成時にセキュリティ形式を指定しない場合、セキュリティ形式は継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVolは、そのFlexVolを含むStorage Virtual Machine (SVM) のルート ボリュームのセキュリティ形式を継承します。

- qtreeは、そのqtreeを含むFlexVolのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含むFlexVolまたはqtreeのセキュリティ形式を継承します。

Infinite Volumeはセキュリティ形式を継承できません。Infinite Volumeのファイルおよびディレクトリは、常にunifiedセキュリティ形式を使用します。Infinite Volumeとそれに含まれるファイルおよびディレクトリのセキュリティ形式は、変更できません。

## 認証によってSMBアクセス セキュリティを確保する仕組み

認証とは、エンティティのIDを検証するプロセスです。SMB接続を確立してStorage Virtual Machine (SVM)に格納されているデータにアクセスする前に、ユーザはCIFSサーバが属しているドメインで認証される必要があります。

CIFSサーバでは、KerberosとNTLM (NTLMv1またはNTLMv2)の2つの認証方法がサポートされます。ドメイン ユーザの認証に使用されるデフォルトの方法はKerberosです。

### 関連コンセプト

[FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法](#) (23ページ)

[Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み](#) (24ページ)

[ローカル ユーザおよびローカル グループを使用した認証と許可](#) (216ページ)

### 関連タスク

[CIFSサーバの最低限の認証セキュリティレベルの設定](#) (84ページ)

[CIFSサーバのKerberosセキュリティ設定の変更](#) (83ページ)

[Kerberosベースの通信用のAES暗号化の有効化と無効化](#) (86ページ)

[ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化](#) (82ページ)

## Kerberos認証

Data ONTAPは、許可されたSMBセッションの作成時にKerberos認証をサポートします。

Kerberosは、クライアント / サーバ環境内で強力な認証を提供するプロトコルです。プロトコルの基本原理は、秘密鍵を共有化する暗号化方式です。これにより、ネットワーク環境にセキュアな認証を提供します。

KerberosはActive Directoryのプライマリ認証サービスです。KerberosサーバのKerberos Key Distribution Center (KDC; キー配布センター) サービスは、Active Directoryに対してセキュリティ プリンシパルに関する情報の格納や取得を行います。NTLMモデルと異なる点は、Active Directory クライアントがCIFSサーバなどの別のコンピュータとのセッションの確立を求める場合、直接KDC にアクセスしてそのセッションのクレデンシャルを取得するところです。

### KDCリソースのSID圧縮機能

Active DirectoryサーバがWindows Server 2012上にホストされている場合、Key Distribution Center (KDC) でリソースSID圧縮機能を使用できます。

Microsoftでは、Windows Server 2012向けのKerberos実装の強化機能として、リソースドメイン内のグループのセキュリティ識別子 (SID) をKDCで自動的に圧縮するKDCリソースSID圧縮と呼ばれる機能を導入しています。この圧縮により、サービス チケットのサイズが小さくなり、チケットのサイズが大きいために発生するアプリケーション認証エラーを減らすことができます。KDCでは、リソースSIDを圧縮するためにターゲット リソースが属するリソースドメインのSIDを格納し、各リソースのSIDのRIDの部分だけを認証データのResourceGroupIdの部分に挿入します。



## NTLM認証

NTLMクライアント認証は、パスワードに基づくユーザ固有の秘密の共有知識に基づいて、チャレンジ-応答プロトコルを使用して行われます。

ユーザがローカルのWindowsユーザ アカウントを使用してSMB接続を行った場合、認証は、NTLMv2を使用するCIFSサーバによってローカルで行われます。

## FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法

WindowsユーザとUNIXユーザ間のユーザ マッピングは、マルチプロトコル アクセスの基本となる要素です。SMB経由のマルチプロトコル アクセスでは、ユーザのWindows IDおよびUNIX ID間のユーザ マッピングに基づいて、ボリュームおよびqtree内でファイルおよびフォルダ操作を実行するユーザ権限が評価されます。

Data ONTAPでは常に、認証プロセス時にユーザのWindows IDがユーザのUNIX IDにマッピングされます。マッピングされたUNIXユーザとUNIXユーザのグループに関する情報は、Windowsユーザのクレデンシャルを使用して保存されます。したがって、ユーザ クレデンシャルには、マッピングされたUNIXクレデンシャルも含まれます。

Data ONTAPではユーザ名がマッピングされます。グループはマッピングされません。ただし、ファイル アクセスを決定する際にはグループ メンバーシップが非常に重要になるため、マッピング プロセスの一環として、マッピングされたUNIXユーザのグループ メンバーシップがユーザ マッピング情報と一緒に取得され、キャッシュされます。

### 関連コンセプト

[ネーム マッピングの仕組み](#) (23ページ)

[Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み](#) (24ページ)

[ネーム マッピングの作成](#) (167ページ)

[マルチドメイン ネーム マッピング検索の設定](#) (170ページ)

### 関連タスク

[デフォルトのUNIXユーザの設定](#) (101ページ)

## ネーム マッピングの仕組み

Data ONTAPは、ユーザ名をマッピングするときにいくつかの手順を実行します。具体的には、ローカルのネーム マッピング データベースおよびLDAPのチェック、ユーザ名の試行、(設定済みの場合は)デフォルト ユーザの使用です。

Data ONTAPがユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネーム マッピング データベースおよびLDAPサーバで既存のマッピングをチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、Storage Virtual Machine (SVM) のネーム サービスで決まります。

- WindowsからUNIXへのマッピングの場合  
マッピングが見つからなかった場合、小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。無効だった場合、デフォルトのUNIXユーザを使用します (設定済みの場合)。デフォルトのUNIXユーザが設定されておらず、この方法でもData ONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。
- UNIXからWindowsへのマッピングの場合  
マッピングが見つからなかった場合、CIFSドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合、デフォルトのCIFSユーザを使用します (設定済みの場合)。デフ

オルトのCIFSユーザが設定されておらず、この方法でもData ONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

## Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み

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

### セキュリティレイヤの種類

すべてのストレージ オブジェクトに、次のセキュリティレイヤを最大で3種類含めることができます。

- **エクスポート (NFS) および共有 (SMB) セキュリティ**  
エクスポートおよび共有セキュリティは、特定のNFSエクスポートまたはSMB共有へのクライアント アクセスに適用されます。管理者権限を持つユーザは、SMBクライアントとNFSクライアントからエクスポートおよび共有レベルのセキュリティを管理できます。
- **ストレージレベルのアクセス保護ファイルおよびディレクトリ セキュリティ**  
ストレージレベルのアクセス保護セキュリティは、SVMのボリュームに適用されます。ストレージレベルのアクセス保護は、すべてのNASプロトコルからストレージレベルのアクセス保護が適用されているストレージ オブジェクトへのすべてのアクセスに適用されます。  
NFSまたはSMBクライアントからファイルやディレクトリのセキュリティ設定を表示しても、ストレージレベルのアクセス保護セキュリティは表示されません。システム (WindowsまたはUNIX) 管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。
- **NTFS、UNIX、およびNFSv4のネイティブのファイルレベルのセキュリティ**  
ストレージ オブジェクトを表すファイルやディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスにSMBとNFSのどちらを使用するかに関係なく有効です。

### Data ONTAPでNFSアクセスにストレージレベルのアクセス保護が使用される仕組み

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

ストレージレベルのアクセス保護は、UNIX専用のSVMで、CIFSサーバを含まないSVMには適用されません。

### 関連コンセプト

[セキュリティ形式がデータ アクセスに与える影響](#) (20ページ)

[FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法](#) (23ページ)

[セキュリティ形式の設定](#) (148ページ)

[SMB共有の作成と設定](#) (175ページ)

[SMB共有のACLを使用したファイル アクセスの保護](#) (190ページ)

[ファイル権限を使用したファイル アクセスの保護](#) (193ページ)

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#) (154ページ)



## SMBアクセスでのエクスポート ポリシーの役割

Data ONTAP 8.2以降、SMBアクセスのエクスポート ポリシーは省略可能になり、デフォルトで無効になっています。ストレージレベルのアクセス制御と共有とファイルの権限に加えてSMBアクセス制御のレイヤを追加したい場合は、SMBのエクスポート ポリシーを有効にすることができます。

### 関連コンセプト

[エクスポート ポリシーを使用したSMBアクセスの保護](#)(208ページ)

## CIFSの設定を大幅に変更すると、完了までにしばらく時間がかかることがあります

ストレージ システムのCLIで入力したコマンドは、通常はすぐに 実行されます。ただし、CLIのコマンドでCIFSの設定が 大幅に変更される場合は、CLIのコマンドを入力して正常に実行されたことを示す確認のメッセージが表示されてから、設定の変更が完了するまでに 時間がかかることがあります。

変更内容が大きく、対象となるオブジェクトが多いほど、完了するまでの時間が長くなります。たとえば、数千の共有を新規に作成したり 数千の共有のACLを変更したりすると時間がかかります。完了までに時間がかかるのは、以下に関連するコマンドを実行する場合です。

- サーバ
- ホーム ディレクトリ
- 共有
- 共有ACL
- スーパーユーザ
- シンボリックリンク パス マッピング
- サーバのセキュリティ

このような設定を大幅に変更する場合は、変更が完了するまでの 時間を考慮するようにしてください。

## SVM(CIFSライセンスなし)用のActive Directoryコンピュータ アカウントの設定と管理

---

クラスタ ノードでCIFSライセンスが有効でなくても、Storage Virtual Machine(SVM、旧Vserver)用のActive Directory(AD)コンピュータ アカウントを作成および管理する必要があります。また、ADコンピュータ アカウント用の優先ドメイン コントローラも構成および管理できます。

### CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する方法

Active DirectoryドメインのメンバーであるCIFSサーバを使用してStorage Virtual Machine(SVM)を設定することも、CIFSのライセンスを取得していない場合は、Active DirectoryドメインにSVMのコンピュータ アカウントを作成することもできます。これらの設定の違いについて、またSVMでCIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する方法について理解する必要があります。

SVMごとに作成できるActive Directoryアカウントは1つだけです。そのため、CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する必要があります。

- 現在SVMにActive Directoryコンピュータ アカウントが設定されており、その後クラスタにCIFSのライセンスを設定してSVMにフル機能のCIFSサーバを作成する場合は、先にActive Directoryコンピュータ アカウントを削除する必要があります。
- 現在SVMにCIFSサーバがあるが今後はSVMでフル機能のCIFSサーバを使用する必要がなく、代わりにActive Directoryコンピュータ アカウントを設定したい場合は、先にCIFSサーバを削除する必要があります。

#### CIFSサーバ

次の状況が当てはまる場合は、CIFSサーバを作成することを選択してください。

- クラスタにCIFSのライセンスがある。  
CIFSのライセンスがあるのは1つのノードでも複数のノードでも構いません。
- ファイル サービスやCIFSのその他の付加価値機能、たとえばホーム ディレクトリ、シンボリック リンク アクセスなどの機能をSMBクライアントに提供したい。

#### Active Directoryコンピュータ アカウント

次の状況が当てはまる場合は、Active Directoryコンピュータ アカウントを作成することを選択してください。

- クラスタにCIFSのライセンスがない。
- SVMのActive Directoryコンピュータ アカウントを作成し、ファイル サービスやCIFSの付加価値機能以外の目的に使用したい。  
たとえば、iSCSIまたはFCプロトコル経由でデータにアクセスするアプリケーションのサービス アカウントとしてActive Directoryアカウントを使用する場合などです。

#### 関連コンセプト

[Active Directoryコンピュータ アカウントの管理](#)(27ページ)

[CIFSサーバのセットアップ](#)(50ページ)

## Active Directoryコンピュータ アカウントの管理

Active Directoryコンピュータ アカウントの管理では、コンピュータ アカウントの作成、情報の表示、削除、コンピュータ アカウントが属するドメインの変更、コンピュータ アカウントのパスワードの変更やリセットを行うことができます。

### 関連コンセプト

[CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する方法](#) (26 ページ)

[Active Directoryコンピュータ アカウントの管理](#) (27 ページ)

[CIFSサーバのセットアップ](#) (36 ページ)

## SVMのActive Directoryコンピュータ アカウントの作成

Storage Virtual Machine (SVM) にドメイン内のコンピュータ アカウントを割り当てたいが、CIFSのライセンスを設定したくない場合や、SMBファイル アクセスまたはCIFSの付加機能を設定する必要がない場合は、SVMのActive Directoryコンピュータ アカウントを作成できます。

### 開始する前に

- クラスタ時間を、SVMコンピュータ アカウントを関連付けるドメインのActive Directoryドメイン コントローラの時間と、5分以内の誤差で同期する必要があります。  
Active Directoryドメインと同じNTPサーバを時刻同期に使用するか、Active Directoryドメイン コントローラをクラスタ タイム サーバとして使用するよう、クラスタNTPサービスを設定することを推奨します。
- SVMコンピュータ アカウントを関連付けるドメイン内のOU (組織単位) にコンピュータ アカウントを追加するための十分な権限が必要です。
- DNSサーバやActive Directoryドメイン コントローラなど、必要なすべての外部サーバに到達できるようにSVMのデータLIFが正しく設定されている必要があります。
- SVMでDNSが設定されている必要があります。また、DNSサーバがコンピュータ アカウントを関連付けるドメインのActive Directory統合DNSに設定されているか、DNSサーバにドメイン LDAPおよびドメイン コントローラ サーバのサービス ロケーション レコード (SRV) が含まれている必要があります。
- DNSサーバでSVMコンピュータ アカウントのDNSレコードを動的に登録する場合は、DNSサーバが動的DNSをサポートしている必要があります。
- セキュアなDDNSを使用するようにSVMが設定されている場合は、Active Directory統合DNSサーバを使用する必要があります。

### タスク概要

Active Directoryコンピュータ アカウントを作成するときは、次の点に留意してください。

- Active Directoryコンピュータ アカウント名は15文字以内にする必要があります。  
次の文字は使用できません。  
@、#、\*、(、)、=、+、[、]、\、;、:、"、'、<、>、\、/、?
- ドメインを指定するときはFully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を使用する必要があります。

- デフォルトでは、Active Directoryコンピュータ アカウントはCN=Computerオブジェクトに追加されます。  
コンピュータ アカウントを別のOUに追加するには、-ouオプションを使用します。OUを指定する場合は、識別名のドメイン部分は指定せず、識別名のOU部分またはCN部分のみ指定します。必須の-domainパラメータに指定した値が、-ouパラメータに指定した値に付加されて、Active Directory識別名が生成されます。この識別名は、Active Directoryコンピュータ アカウントオブジェクトの作成時に使用されます。

#### 手順

- Active Directoryコンピュータ アカウントを作成します。  
**vserver active-directory create -vserver vs1 -account-name NetBIOS\_account\_name -domain FQDN [-ou organizational\_unit]**
- vserver active-directory showコマンドを使用して、Active Directoryコンピュータ アカウントが目的のOUに作成されたことを確認します。

#### 例

次のコマンドを実行すると、SVM vs1のvs1という名前のActive Directoryコンピュータ アカウントがmyexample.comドメインに作成されます。コンピュータ アカウントはOU=eng,DC=myexample,DC=comコンテナに配置されます。

```
cluster1::> vserver active-directory create -vserver vs1 -account-name vs1 -domain myexample.com -ou OU=eng
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "OU=eng" container within the "myexample.com" domain.

Enter the user name: Admin\_user

Enter the password:

```
cluster1::> vserver active-directory show
```

| Vserver | Account Name | Domain/Workgroup Name |
|---------|--------------|-----------------------|
| vs1     | VS1          | MYEXAMPLE             |

#### 関連コンセプト

[CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する方法](#)(26ページ)

[Active Directoryコンピュータ アカウントのドメイン コントローラ接続の管理](#)(32ページ)

## SVMコンピュータ アカウントが関連付けられているActive Directoryドメインの変更

Storage Virtual Machine (SVM) コンピュータ アカウントが関連付けられているActive Directoryドメインを変更することができます。これは、アプリケーションのサービス アカウントに別のドメインのアカウントを使用する場合や、アプリケーションが使用するSVMリソースを別のドメインに移行する場合に役立ちます。

#### 開始する前に

- クラスタ ノードの時間は、SVMコンピュータ アカウントを関連付けるドメインのActive Directoryドメイン コントローラに設定された時間から5分以内に設定する必要があります。  
時刻同期に新しいActive Directoryドメインと同じNTPサーバを使用するようにクラスタNTPサービスを設定するか、新しいドメインのActive Directoryドメイン コントローラをクラスタ タイム サーバとして使用することを推奨します。

- SVMコンピュータ アカウントを関連付ける新しいドメイン内のOU(組織単位)にコンピュータ アカウントを追加する、十分な権限を保有している必要があります。
- SVM用のDNSサーバがSVMコンピュータ アカウントを関連付ける新しいドメインのActive Directory統合DNSに設定されているか、DNSサーバにドメインLDAPとドメイン コントローラ サーバのサービス ロケーション レコード(SRV)が含まれている必要があります。
- DNSサーバでSVMコンピュータ アカウントのDNSレコードを動的に登録する場合は、DNSサーバが動的DNSをサポートしている必要があります。
- セキュアなDDNSを使用するようにSVMが設定されている場合は、Active Directory統合DNSサーバを使用する必要があります。

### タスク概要

- ドメインを指定するときはFully Qualified Domain Name(FQDN;完全修飾ドメイン名)を使用する必要があります。
- Active Directoryコンピュータ アカウントが関連付けられているドメインを変更すると、新しいドメインのコンピュータ アカウントはCN=Computersコンテナに配置されます。  
ドメインを変更する際にコンピュータ アカウントを配置する場所を指定することはできません。  
コンピュータ アカウントの場所をCN=Computers以外のコンテナにするには、Active Directoryアカウントを削除してvserver active-directory createコマンドで再作成する必要があります。

### 手順

1. Active Directoryコンピュータ アカウントのドメインを変更します。  
**vserver active-directory modify -vserver *vserver\_name* -domain *FQDN***
2. vserver active-directory showコマンドで、CN=ComputerにActive Directoryコンピュータ アカウントが作成されていることを確認します。

#### 例

次のコマンドは、SVM vs1のvs1という名前のActive Directoryコンピュータ アカウントのドメインをexample.comドメインに変更します。コンピュータ アカウントはCN=Computersコンテナに配置されます。

```
cluster1::> vserver active-directory modify -vserver vs1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Admin\_user

Enter the password:

```
cluster1::> vserver active-directory show
```

| Vserver | Account Name | Domain/Workgroup Name |
|---------|--------------|-----------------------|
| vs1     | VS1          | EXAMPLE               |

## SVMのActive Directoryコンピュータ アカウントに関する情報の表示

Storage Virtual Machine (SVM) のActive Directoryコンピュータ アカウントに関する情報を表示できます。たとえば、SVMのコンピュータ アカウント名、コンピュータ アカウントが関連付けられているドメインの名前、コンピュータ アカウントがある組織単位などの情報を表示できます。

### 手順

1. `vserver active-directory show`コマンドを使用して、SVMのActive Directoryコンピュータ アカウントに関する情報を表示します。

オプションのパラメータを指定して表示をカスタマイズできます。詳細については、コマンドのマニュアル ページを参照してください。

### 例

次のコマンドを実行すると、クラスタ上のSVMのすべてのActive Directoryアカウントに関する情報が表示されます。

```
cluster1::> vserver active-directory show
```

| Vserver | Account Name | Domain/Workgroup Name |
|---------|--------------|-----------------------|
| vs1     | CIFSSERVER1  | EXAMPLE               |
| vs2     | CIFSSERVER2  | EXAMPLE2              |

次のコマンドを実行すると、クラスタ上のSVMのすべてのActive Directoryアカウントに関する詳細情報が表示されます。

```
cluster1::> vserver active-directory show -instance
```

```

                                Vserver: vs1
Active Directory account NetBIOS Name: CIFSSERVER1
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Organizational Unit: CN=Computers

                                Vserver: vs2
Active Directory account NetBIOS Name: CIFSSERVER2
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE2.COM
Organizational Unit: CN=Computers
```

## SVMのActive Directoryコンピュータ アカウントの削除

Storage Virtual Machine (SVM) でActive Directoryドメインのコンピュータ アカウントが不要になった場合や、SVMでActive Directoryコンピュータ アカウントの代わりにCIFSサーバを設定する場合は、コンピュータ アカウントを削除できます。

### 開始する前に

SVMのコンピュータ アカウントが含まれるActive DirectoryドメインのOU(組織単位)からコンピュータ アカウントを削除するための十分な権限が必要です。

### タスク概要

SVMでは、Active Directoryコンピュータ アカウントとCIFSサーバのどちらかを使用できますが、両方を使用することはできません。現在SVMでActive Directoryコンピュータ アカウントを使用してお

り、そのSVMにCIFSサーバを作成する場合は、先にActive Directoryコンピュータ アカウントを削除してからCIFSサーバを作成します。

#### 手順

1. Active Directoryコンピュータ アカウントを削除します。

```
vserver active-directory delete -vserver vserver_name
```

コンピュータ アカウントがあるOUからコンピュータ アカウントを削除するための十分な権限を持つユーザのユーザ名とパスワードを入力するように求められます。

2. コンピュータ アカウントが削除されたことを確認します。

```
vserver active-directory show
```

#### 例

次のコマンドを実行すると、SVM vs2にあるActive Directoryコンピュータ アカウントが削除されます。

```
cluster1::> vserver active-directory show

Vserver      Account      Domain/Workgroup
Name         Name         Name
-----
vs1          VS1          EXAMPLE
vs2          VS2          MYEXAMPLE

cluster1::> vserver active-directory delete -vserver vs2

In order to delete an Active Directory machine account, you must supply the
name and password of a Windows account with sufficient privileges to remove
computers from the "example.com" domain.

Enter the user name: Admin_user

Enter the password:

cluster1::> vserver active-directory show

Vserver      Account      Domain/Workgroup
Name         Name         Name
-----
vs1          VS1          EXAMPLE
```

## SVMのActive Directoryコンピュータ アカウント パスワードの変更またはリセット

セキュリティ強化のためにActive Directoryコンピュータ アカウントのパスワードを変更したり、パスワードを忘れた場合にリセットしたりできます。

#### 手順

1. 次のいずれかを実行します。

| 状況または条件                 | 使用するコマンド                                                                  |
|-------------------------|---------------------------------------------------------------------------|
| パスワードがわかっている場合に<br>変更する | <b>vserver active-directory password-change -vserver<br/>vserver_name</b> |

| 状況または条件              | 使用するコマンド                                                                                                                                                                                     |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスワードがわからない場合にリセットする | <b><code>vserver active-directory password-reset -vserver vserver_name</code></b>                                                                                                            |
|                      | パスワードのリセットは、Active Directoryドメインにマシン アカウントとともに保存されているパスワードがStorage Virtual Machine(SVM)以外によって変更またはリセットされた場合に必要になることがあります。この処理には、コンピュータ アカウントが含まれる組織単位(OU)のパスワードをリセットする権限を持つユーザのクレデンシャルが必要です。 |

-vserverは、ドメイン パスワードを変更またはリセットするActive Directoryアカウントに関連付けられたSVMの名前です。

## Active Directoryコンピュータ アカウントのドメイン コントローラ接続の管理

Active Directoryコンピュータ アカウントのドメイン コントローラ接続の管理には、検出されたActive Directoryサーバ情報の表示、Active Directoryサーバの再設定および再検出、優先ドメイン コントローラ リストの設定、優先ドメイン コントローラ リストの表示があります。

### 関連コンセプト

[Active Directoryコンピュータ アカウントの管理](#)(27ページ)

## SVMで検出されたActive Directoryサーバに関する情報の表示

Storage Virtual Machine(SVM)コンピュータ アカウントが関連付けられているドメインで検出されたLDAPサーバおよびドメイン コントローラに関する情報を表示できます。

### タスク概要

`vserver active-directory discovered-servers show`コマンドは、`vserver cifs domain discovered-servers show`コマンドのエイリアスです。どちらのコマンドを使用しても、SVMで検出されたActive Directoryサーバに関する情報を表示できます。

### 手順

1. 検出されたサーバに関する情報のすべてまたは一部を表示するには、次のコマンドを入力します。

```
vserver active-directory discovered-servers show
```

デフォルトでは、検出されたサーバに関する次の情報が表示されます。

- ノード名
- SVM名
- Active Directoryドメイン名
- サーバ タイプ
- 優先度
- ドメイン コントローラ名
- ドメイン コントローラのアドレス



- ステータス

オプションのパラメータを指定して表示をカスタマイズできます。詳細については、コマンドのマニュアル ページを参照してください。

#### 例

次のコマンドを実行すると、SVM vs1で検出されたサーバが表示されます。

```
cluster1::> vserver active-directory discovered-servers show -vserver vs1
```

Node: node1  
Vserver: vs1

| Domain Name | Type    | Preference | DC-Name        | DC-Address     | Status |
|-------------|---------|------------|----------------|----------------|--------|
| " "         | NIS     | preferred  | 192.168.10.222 | 192.168.10.222 | OK     |
| example.com | MS-LDAP | adequate   | DC-1           | 192.168.192.24 | OK     |
| example.com | MS-LDAP | adequate   | DC-2           | 192.168.192.25 | OK     |
| example.com | MS-DC   | adequate   | DC-1           | 192.168.192.24 | OK     |
| example.com | MS-DC   | adequate   | DC-2           | 192.168.192.25 | OK     |

## Active Directoryサーバのリセットと再検出

Storage Virtual Machine (SVM)でActive Directoryサーバのリセットと再検出を行うと、SVMに格納されているLDAPサーバおよびドメイン コントローラに関する情報が破棄されます。サーバの情報を破棄したあと、SVMはそれらの外部サーバに関する最新の情報を再取得します。これは、接続されているサーバが適切に応答しない場合に役立ちます。

### タスク概要

`vserver active-directory discovered-servers reset-servers`コマンドは、`vserver cifs domain discovered-servers reset-servers`コマンドのエイリアスです。SVMで、Active Directoryサーバのリセットや再検出を行うコマンドを使用できます。

### 手順

1. 次のコマンドを入力します。

```
vserver active-directory discovered-servers reset-servers -vserver  
vserver_name
```

2. 再検出されたサーバに関する新しい情報を表示します。

```
vserver active-directory discovered-servers show -vserver vserver_name
```

#### 例

次に、SVM vs1のサーバをリセットして再検出するコマンドを示します。

```
cluster1::> vserver active-directory discovered-servers reset-servers -  
vserver vs1
```

```
cluster1::> vserver active-directory discovered-servers show
```

Node: node1  
Vserver: vs1

| Domain Name | Type | Preference | DC-Name | DC-Address | Status |
|-------------|------|------------|---------|------------|--------|
| " "         | NIS  | preferred  | 1.1.3.4 | 1.1.3.4    | OK     |

|             |         |          |      |         |    |
|-------------|---------|----------|------|---------|----|
| example.com | MS-LDAP | adequate | DC-1 | 1.1.3.4 | OK |
| example.com | MS-LDAP | adequate | DC-2 | 1.1.3.5 | OK |
| example.com | MS-DC   | adequate | DC-1 | 1.1.3.4 | OK |
| example.com | MS-DC   | adequate | DC-2 | 1.1.3.5 | OK |

## 優先ドメイン コントローラの追加または削除

Data ONTAPでは、DNSを介してドメイン コントローラが自動的に検出されます。必要に応じて、Active Directoryコンピュータ アカウントが設定されているドメインのStorage Virtual Machine (SVM)に対する優先ドメイン コントローラのリストに、1つ以上のドメイン コントローラを追加することができます。

### タスク概要

`vserver active-directory preferred-dc add`および`vserver active-directory preferred-dc remove`コマンドは、それぞれ`vserver cifs domain preferred-dc add`および`vserver cifs domain preferred-dc remove`コマンドのエリアスです。どちらのコマンド セットも、Active Directoryドメイン アカウント用の優先ドメイン コントローラの管理に使用できます。

### 手順

1. 次のいずれかを実行します。

| 状況               | 使用するコマンド                                                                                                                                               |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 優先ドメイン コントローラの追加 | <code>vserver active-directory preferred-dc add -vserver <i>vserver_name</i> -domain <i>domain_name</i> -preferred-dc <i>IP_address</i>, ...</code>    |
| 優先ドメイン コントローラの削除 | <code>vserver active-directory preferred-dc remove -vserver <i>vserver_name</i> -domain <i>domain_name</i> -preferred-dc <i>IP_address</i>, ...</code> |

-vserver *vserver\_name*には、SVM名を指定します。

-domain *domain\_name*には、ドメイン コントローラが属するドメインの完全修飾名を指定します。

-preferred-dc *IP\_address*, ...には、追加または削除する優先ドメイン コントローラの1つ以上のIPアドレスをカンマで区切って指定します。優先ドメイン コントローラを追加する場合、カンマ区切りリストの順番は優先順位を示します。

### 例

次のコマンドでは、SVM vs1がexample.comへの外部アクセスを管理するために使用する優先ドメイン コントローラのリストに、ドメイン コントローラのIPアドレス10.1.1.10および10.1.1.20を追加します。example.comドメインには、SVM Active Directoryアカウントが含まれています。

```
cluster1::> vserver active-directory preferred-dc add -vserver vs1 -domain
example.com -preferred-dc 10.1.1.10,10.1.1.20
```

次のコマンドは、Storage Virtual Machine (SVM) vs1がexample.comドメインへの外部アクセスを管理するために使用する優先ドメイン コントローラのリストから、ドメイン コントローラIP アドレス10.1.1.20を削除します。

```
cluster1::> vserver active-directory preferred-dc remove -vserver vs1 -
domain example.com -preferred-dc 10.1.1.20
```

## 優先ドメイン コントローラに関する情報の表示

Storage Virtual Machine (SVM) の Active Directory コンピュータ アカウントが関連付けられているドメインの優先ドメイン コントローラのリストに関する情報を表示できます。この情報は、優先的に接続されるドメイン コントローラを確認するときに役立ちます。

### タスク概要

`vserver active-directory preferred-dc show` コマンドは、`vserver cifs domain preferred-dc show` コマンドのエイリアスです。どちらのコマンドを使用しても、Active Directory ドメイン アカウントの優先ドメイン コントローラに関する情報を表示できます。

### 手順

1. 検出された優先ドメイン コントローラに関する情報のすべてまたは一部を表示するには、次のコマンドを入力します。

**`vserver active-directory preferred-dc show`**

デフォルトでは、コマンドを実行すると優先ドメイン コントローラに関する次の情報が表示されます。

- SVM 名
- Active Directory ドメイン 名
- 優先ドメイン コントローラの IP アドレスの一覧

オプションのパラメータを指定して表示をカスタマイズできます。詳細については、コマンドのマニュアル ページを参照してください。

### 例

次のコマンドを実行すると、SVM vs1 のすべての優先ドメイン コントローラが表示されます。

```
cluster1::> vserver active-directory preferred-dc show -vserver vs1
```

| Vserver | Domain Name | Preferred Domain Controllers |
|---------|-------------|------------------------------|
| vs1     | example.com | 10.1.1.10, 10.1.1.20         |

## CIFSサーバのセットアップ

---

FlexVolを備えたStorage Virtual Machine(SVM)上でCIFSサーバを有効化して設定し、SMBクライアントがクラスタ上のファイルにアクセスできるようにすることができます。

クラスタ内のデータSVMは、それぞれ1つのActive Directoryドメインにバインドできますが、データSVMは必ずしも同じドメインにバインドする必要はありません。各データSVMを一意的なActive Directoryドメインにバインドできます。

Infinite Volumeを備えたSVM上のCIFSサーバの設定の詳細については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

## CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する方法

Active DirectoryドメインのメンバーであるCIFSサーバを使用してStorage Virtual Machine(SVM)を設定することも、CIFSのライセンスを取得していない場合は、Active DirectoryドメインにSVMのコンピュータ アカウントを作成することもできます。これらの設定の違いについて、またSVMでCIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する方法について理解する必要があります。

SVMごとに作成できるActive Directoryアカウントは1つだけです。そのため、CIFSサーバとActive Directoryコンピュータ アカウントのどちらを作成するかを選択する必要があります。

- 現在SVMにActive Directoryコンピュータ アカウントが設定されており、その後クラスタにCIFSのライセンスを設定してSVMにフル機能のCIFSサーバを作成する場合は、先にActive Directoryコンピュータ アカウントを削除する必要があります。
- 現在SVMにCIFSサーバがあるが今後はSVMでフル機能のCIFSサーバを使用する必要がなく、代わりにActive Directoryコンピュータ アカウントを設定したい場合は、先にCIFSサーバを削除する必要があります。

### CIFSサーバ

次の状況が当てはまる場合は、CIFSサーバを作成することを選択してください。

- クラスタにCIFSのライセンスがある。  
CIFSのライセンスがあるのは1つのノードでも複数のノードでも構いません。
- ファイル サービスやCIFSのその他の付加価値機能、たとえばホーム ディレクトリ、シンボリックリンクアクセスなどの機能をSMBクライアントに提供したい。

### Active Directoryコンピュータ アカウント

次の状況が当てはまる場合は、Active Directoryコンピュータ アカウントを作成することを選択してください。

- クラスタにCIFSのライセンスがない。
- SVMのActive Directoryコンピュータ アカウントを作成し、ファイル サービスやCIFSの付加価値機能以外の目的に使用したい。  
たとえば、iSCSIまたはFCプロトコル経由でデータにアクセスするアプリケーションのサービスアカウントとしてActive Directoryアカウントを使用する場合などです。

## 関連コンセプト

[Active Directoryコンピュータ アカウントの管理](#)(27ページ)

[CIFSサーバのセットアップ](#)(50ページ)

## サポート対象のSMBクライアントおよびドメイン コントローラ

Storage Virtual Machine (SVM) でSMBを使用する前に、Data ONTAPがサポートするSMBクライアントおよびドメイン コントローラを把握しておく必要があります。

Data ONTAPがサポートするSMBクライアントおよびドメイン コントローラの最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)) を参照してください。

## サポートされないWindowsの機能

ネットワークでCIFSを使用する場合は、一部のWindowsの機能がData ONTAPではサポートされないことに注意する必要があります。

Data ONTAPでは、次のWindowsの機能はサポートされません。

- Encrypted File System (EFS; 暗号化ファイルシステム)
- 変更ジャーナルでのNT File System (NTFS) イベントのロギング
- Microsoft File Replication Service (FRS; ファイル レプリケーション サービス)
- Microsoft Windows インデックス サービス
- Hierarchical Storage Management (HSM; 階層型ストレージ管理) 経由のリモート ストレージ
- Windows クライアントからのクォータ管理
- Windows のクォータのセマンティクス
- LMHOSTS ファイル
- NTFS のネイティブ圧縮

## CIFSサーバのセットアップの前提条件

CIFSサーバのセットアップ プロセスを開始する前に満たしておくべき前提条件があります。

- クラスタでCIFSのライセンスが有効になっている必要があります。
- Storage Virtual Machine (SVM) のデータLIFを外部ネットワークに接続しておく必要があります。
- SVMデータLIFの設定に、IPアドレス、サブネット マスク、デフォルト ゲートウェイのリストが必要です。
- SVMデータLIFを作成する際に使用するサブネットは、Active Directoryドメイン コントローラとNIS、DNS、NDMP、LDAPのサーバなどのサービスに必要なすべての外部サーバにルーティングできる必要があります。

**注:** clustered Data ONTAP 8.3より前のリリースでは、クラスタ管理LIFが外部サーバにルーティングできていれば、ノードとそのLIFを使用してSVM用の外部サーバに接続できました。clustered Data ONTAP 8.3以降では、ノードとクラスタ管理LIFを使用してSVM用の外部サーバに接続することはできません。

- CIFSサーバを作成する際にDNSサーバでコンピュータ アカウントのDNSレコードが動的に登録されるようにするには、DNSサーバが動的DNSをサポートしている必要があります。
- セキュアDDNSを設定する場合、SVM用に設定するDNSサーバはActive Directory統合DNSサーバである必要があります。
- CIFSサーバを作成する管理者は、ホーム ドメインまたは信頼されたドメインに属している必要があります。

#### 関連コンセプト

[CIFSサーバのセットアップ](#) (50ページ)

[CIFSサーバの管理](#) (71ページ)

## CIFSサーバの設定の計画

CIFSサーバ構成を作成する前に、構成の各ステップの設定タスクを理解する必要があります。構成に必要な設定タスクを決定し、計画ワークシートに記入する必要があります。

次の設定タスクを計画する必要があります。

- タイム サービスのセットアップ
- IPスペース、ブロードキャストドメイン、サブネットのセットアップ
- CIFSサーバを格納するStorage Virtual Machine (SVM) の作成
- SVMのネットワークのセットアップ
- SVM用のネーム サービスのセットアップ
- CIFSサーバの作成

#### 関連コンセプト

[CIFSサーバのセットアップ](#) (50ページ)

## タイム サービスを設定する前に収集する情報

CIFSサーバを作成する前に、クラスタでタイム サービスを設定する必要があります。Kerberos認証を使用する場合、クラスタ時間とCIFSサーバが所属するドメインのドメイン コントローラの時間の時間差が5分以上にならないようにする必要があります。5分以上のずれがあるとCIFSサーバの作成は失敗します。タイム サービスのIPアドレスは必ず記録してください。

NTPタイム サービスはクラスタ上で自動的に有効になりますが、タイム サービスのIPアドレスを指定する必要があります。タイム サービスは最大3つまで指定できます。

| 情報の種類                                                                   | 必須 | 値 |
|-------------------------------------------------------------------------|----|---|
| タイム サービスのIPアドレス                                                         | ○  |   |
| クラスタのタイム サービスとCIFSサーバが所属するドメインのドメイン コントローラの時間と時間差が常に5分以内になるように設定されているか。 | ○  | ○ |

クラスタ時間を手動で調整するのではなく、クラスタのタイム サービスを設定します。時間差が5分より大きいと、CIFSサーバの作成が失敗します。また、Kerberos認証を使用する場合、CIFSサーバ上にホストされている共有やその他のドメイン認証に依存するCIFSサーバ サービスへのCIFSへのアクセスも失敗します。

Kerberosクロック スキューのデフォルトの最大許容値は5分です。CIFSサーバのセットアップ後、`vserver cifs security modify`コマンド、または一元化されたActive Directory GPOを使用して、最大許容時間の設定を調整できます。

## 関連情報

[clustered Data ONTAP 8.3 システム アドミニストレーション ガイド](#)

## IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収集する情報

CIFSサーバを作成するStorage Virtual Machine (SVM)をセットアップする前に、あらかじめ決めておいた値を使用してIPspace、ブロードキャストドメイン、サブネットを作成する必要があります。

IPspaces、ブロードキャストドメイン、サブネット構成は、SVMが存在するネットワーク構造を指定するものです。

- IPspaceはクラスタ内の独立したIPアドレス空間を定義するもので、別々のネットワーク空間を割り当ててSVMで安全な管理やルーティングを実現するための手段です。
- ブロードキャストドメインは、同じレイヤ2ネットワークに属するポートをグループ化し、そのブロードキャストドメイン ポートにMTUを設定します。  
ブロードキャストドメインは、IPspaceに割り当てられます。1つのIP空間に複数のブロードキャストドメインを含むことができます。
- サブネットにはIPアドレスの特定のプールとデフォルト ゲートウェイが1つ含まれ、IPspace内に配置されたSVMで使用するLIFに割り当てることができます。

## IPspaceを作成するために収集する情報

CIFSサーバをセットアップする際には、新しいIPspaceを作成するか、デフォルトのIPspaceまたはその他の既存IPspaceを使用することができます。

| 情報の種類                                                                                                                        | 必須 | 値 |
|------------------------------------------------------------------------------------------------------------------------------|----|---|
| <i>IPspace名</i> <ul style="list-style-type: none"> <li>• IPspaceに割り当てる名前。</li> <li>• IPspace名はクラスタ内で一意である必要があります。</li> </ul> | ○  |   |

## ブロードキャストドメインを作成するために収集する情報

- ブロードキャストドメインを作成すると、同じ名前のフェイルオーバー グループが自動的に作成されます。
- フェイルオーバー グループには、ブロードキャストドメインに割り当てられたすべてのポートが含まれます。
- CIFSサーバ用のSVMを作成する際には、必要に応じて既存のIPspace内の既存のブロードキャストドメインを使用することもできます(デフォルトIPspaceのデフォルト ブロードキャストドメインも含まれます)。

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                            | 必須                     | 値 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---|
| <b>IPspace名</b> <ul style="list-style-type: none"> <li>ブロードキャストドメインを割り当てるIPspace。</li> <li>既存のIPspaceを指定する必要があります。</li> <li>指定しない場合、ブロードキャストドメインはデフォルトIPspaceに割り当てられます。</li> </ul>                                                                                                                                                                                                                                                               | ×(デフォルトIPspaceを使用する場合) |   |
| <b>ブロードキャストドメイン名</b> <ul style="list-style-type: none"> <li>ブロードキャストドメインに割り当てる名前。</li> <li>名前はIPspace内で一意である必要があります。</li> </ul>                                                                                                                                                                                                                                                                                                                  | ○                      |   |
| <b>MTU</b> <ul style="list-style-type: none"> <li>ブロードキャストドメインのMTU。</li> <li>1500または9000のどちらかを指定できます。</li> <li>MTU値は、ブロードキャストドメインのすべてのポートと、以降ブロードキャストドメインに追加されるすべてのポートに適用されます。</li> </ul> <p>注: MTU値は、ネットワークに接続されているすべてのデバイスで同じである必要があります。</p>                                                                                                                                                                                                   | ○                      |   |
| <b>ポート</b> <ul style="list-style-type: none"> <li>ブロードキャストドメインに追加するネットワーク ポート。</li> <li>ブロードキャストドメインには、物理ポート、VLAN、インターフェイス グループ(ifgroup)を割り当てることができます。VLANおよびインターフェイス グループの設定の詳細については、『clustered Data ONTAP ネットワーク管理ガイド』を参照してください。</li> <li>ポートが別のブロードキャストドメイン内にある場合は、そのドメインから削除してからブロードキャストドメインに追加する必要があります。</li> <li>ポートは、ノード名とポートの両方を指定して割り当てます。たとえば「node1:e0d」とします。</li> <li>デフォルトでは、どのポートも割り当てられません。ポートはいつでもブロードキャストドメインに追加できます。</li> </ul> | ×                      |   |

#### サブネットを作成するために収集する情報

- SVM上でLIFを作成する際には、IPアドレスとサブネットを指定する代わりにサブネット名を指定できます。
- サブネットはデフォルト ゲートウェイと一緒に設定できるため、SVMを作成する際に別途デフォルト ゲートウェイを作成する必要はありません。
- ブロードキャストドメインには、1つまたは複数のサブネットを含めることができます。1つまたは複数のサブネットをIPspaceのブロードキャストドメインと関連付けることによって、別のサブネット上にあるSVM LIFを設定できます。



- 各サブネットには、同じIPspace内の別のサブネットに割り当てられたIPアドレスと重複しないIPアドレスを含める必要があります。
- CIFSサーバを作成する際には、必要に応じて任意のIPspace内の既存サブネットを使用することができます。
- 必要に応じて、サブネットを使用する代わりに、SVMデータLIFに特定のIPアドレスを割り当ててSVM用のデフォルト ゲートウェイを作成することができます。  
この方法を使用してIPアドレスをデータLIFに割り当てる方法の詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』を参照してください。

| 情報の種類                                                                                                                                                                                                                                                | 必須                     | 値 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---|
| <b>IPspace名</b> <ul style="list-style-type: none"> <li>サブネットを割り当てる既存のIPspaceの名前。</li> <li>指定しない場合、サブネットはデフォルトIPspaceに割り当てられます。</li> </ul>                                                                                                            | ×(デフォルトIPspaceを使用する場合) |   |
| <b>サブネット名</b> <ul style="list-style-type: none"> <li>作成するサブネットの名前。</li> <li>名前はサブネットを割り当てるIPspace内で一意である必要があります。</li> </ul>                                                                                                                          | ○                      |   |
| <b>ブロードキャストドメイン名</b> <ul style="list-style-type: none"> <li>サブネットを割り当てるブロードキャストドメインの名前。</li> <li>ブロードキャストドメインは、指定されたIPspace内に存在する必要があります。</li> </ul>                                                                                                 | ○                      |   |
| <b>サブネット名とマスク</b><br>IPアドレスが存在するサブネット アドレスとマスクです。                                                                                                                                                                                                    | ○                      |   |
| <b>ゲートウェイ</b> <ul style="list-style-type: none"> <li>サブネット用のデフォルト ゲートウェイを指定できます。</li> <li>ゲートウェイはサブネットを作成する際に割り当てなくても、いつでも割り当てることができます。</li> </ul>                                                                                                   | ×                      |   |
| <b>IPアドレス範囲</b> <ul style="list-style-type: none"> <li>範囲またはサブネット内の特定のIPアドレスを指定できます。<br/>たとえば、「192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145」などの範囲を指定できます。</li> <li>IPアドレスの範囲を指定しない場合、指定したサブネット内のすべての範囲のIPアドレスがLIFに割り当て可能になります。</li> </ul> | ×                      |   |

| 情報の種類                                                                                                                                                                                                                                                                                  | 必須 | 値 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---|
| <b>LIFとの関連付けの強制アップデート</b> <ul style="list-style-type: none"> <li>既存のLIFとの関連付けを強制的にアップデートするかどうかを指定します。</li> <li>デフォルトでは、サービス プロセッサ インターフェイスやネットワーク インターフェイスが指定された範囲のIPアドレスを使用している場合、サブネットの作成は失敗します。</li> <li>このパラメータを使用すると、手動でアドレスを指定したすべてのインターフェイスがサブネットに関連付けられ、コマンドが成功します。</li> </ul> | ×  |   |

#### 関連情報

[clustered Data ONTAP 8.3 ネットワーク管理ガイド](#)

### SVMを設定する前に収集する情報

CIFSサーバを作成する前に、事前に決定した値を使用してStorage Virtual Machine (SVM)を設定する必要があります。SVM名、ルート ボリューム名とセキュリティ形式、ルート ボリュームを作成するアグリゲート名、IPspace、その他のオプション設定の値を記録する必要があります。

記録した値は、FlexVolを備えたSVMを作成するために使用します。Infinite Volumeを備えたSVMの作成の詳細については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

記録した値は、デフォルト データSVMを作成するために使用します。MetroClusterソースSVMを作成する場合は、『*clustered Data ONTAP システム アドミニストレーション ガイド(クラスタ管理)*』を参照してください。

| 情報の種類                                                                                                                                                                                                                                                                                             | 必須 | 値 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---|
| <b>SVM名</b> <ul style="list-style-type: none"> <li>SVMに割り当てる名前を指定します。</li> <li>SVMの名前には、英数字と、. (ピリオド)、-(ハイフン)、および_(アンダースコア)を使用できます。</li> <li>SVM名の先頭には、数字または特殊文字の. (ピリオド)、-(アンダースコア)は使用できません。</li> <li>SVM名で利用できる文字数は最大47文字です。</li> <li>SVM名がクラスタリーグ全体で一意になるように、完全修飾ドメイン名(FQDN)を使用します。</li> </ul> | ○  |   |
| <b>ルート ボリューム名</b> <ul style="list-style-type: none"> <li>SVMルート ボリュームの名前を指定します。</li> <li>ルート ボリュームの名前は英字(a～zまたはA～Z)で始まり、203文字以下でなければなりません。</li> </ul>                                                                                                                                             | ○  |   |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                     | 必須 | 値 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---|
| <b>アグリゲート名</b> <ul style="list-style-type: none"> <li>SVMルート ボリュームを保持するアグリゲート名を指定します。</li> <li>既存のアグリゲートを指定する必要があります。</li> </ul>                                                                                                                                                                                                                                                          | ○  |   |
| <b>セキュリティ形式</b> <ul style="list-style-type: none"> <li>SVMルート ボリュームのセキュリティ形式を指定します。</li> <li>指定できる値は、<b>ntfs</b>、<b>unix</b>、および<b>mixed</b>です。</li> </ul>                                                                                                                                                                                                                                | ○  |   |
| <b>IPspace</b> <ul style="list-style-type: none"> <li>SVMが割り当てられているIPspaceの名前を指定します。</li> <li>IPspaceが指定されていない場合、SVMはData ONTAPが自動的に作成するデフォルトIPspaceに割り当てられます。</li> <li>既存のIPspaceを指定する必要があります。</li> </ul>                                                                                                                                                                                | ×  |   |
| <b>SVMの言語設定</b> <ul style="list-style-type: none"> <li>SVMとそのボリュームで使用されるデフォルトの言語を指定します。</li> <li>ボリュームの言語を指定しなかった場合は、SVMのデフォルトの言語設定はC.UTF-8です。</li> <li>SVMの言語の設定によって、SVM内のすべてのNASボリュームのファイル名とデータの表示に使用される文字セットが決定されます。<br/>FlexVolを備えたSVMの言語は、SVMを作成した後からも変更できます。<br/>SVMの言語の設定の詳細については、『<i>clustered Data ONTAP システム アドミニストレーション ガイド</i>(クラスタ管理)』を参照してください。</li> </ul>                  | ×  |   |
| <b>Snapshotポリシー</b> <ul style="list-style-type: none"> <li>SVMに適用するSnapshotポリシーを指定します。<br/>Snapshotポリシーを指定しない場合、デフォルトのクラスタのSnapshotポリシーがSVMに適用されます。</li> <li>Snapshotポリシーは、デフォルトで有効になっています。<br/>デフォルトで、SnapshotポリシーはSVM上のボリュームへ継承されます。SVMに適用するSnapshotポリシーはいつでも変更することができます。</li> </ul> <p>Snapshotポリシーの詳細については、『<i>clustered Data ONTAP 論理ストレージ管理ガイド</i>』のSnapshotコピーのセクションを参照してください。</p> | ×  |   |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                               | 必須 | 値 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---|
| <b>クォータ ポリシー</b> <ul style="list-style-type: none"> <li>SVMに適用するクォータ ポリシーを指定します。<br/>クォータ ポリシーを指定しない場合、「default」という名前の空のクォータ ポリシーが作成され、SVMに適用されます。</li> <li>デフォルトで、クォータ ポリシーはSVM上のボリュームへ継承されます。</li> <li>SVMに適用するクォータ ポリシーはいつでも変更することができます。</li> <li>この設定は、FlexVolを備えたSVMのみサポートされます。</li> </ul> クォータ ポリシーの詳細については、『 <i>clustered Data ONTAP 論理ストレージ管理ガイド</i> 』のクォータのセクションを参照してください。 | ×  |   |
| <b>コメント</b> <ul style="list-style-type: none"> <li>SVMのコメントを指定します。</li> <li>スペースを含むコメントを入力する場合は、コメント全体を引用符で囲みます。</li> </ul>                                                                                                                                                                                                                                                         | ×  |   |

#### 関連情報

[Clustered Data ONTAP 8.3 Infinite Volumes Management Guide](#)  
[clustered Data ONTAP 8.3 システム アドミニストレーション ガイド](#)  
[clustered Data ONTAP 8.3 論理ストレージ管理ガイド](#)

### SVM上でデータLIFを作成する前に収集する情報

CIFSサーバを設定する前に、事前に決定した値を使用してStorage Virtual Machine (SVM) 用のデータLIFを作成する必要があります。SVM名と、LIF名、LIFのロール、許可されているプロトコル、LIFのホーム ノードとポート、およびサブネット名の値を記録します。

LIFを作成する際には、サブネットの代わりにIPアドレスとデフォルト ゲートウェイを使用することもできます。詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』を参照してください。

| 情報の種類                                   | 必須 | 値 |
|-----------------------------------------|----|---|
| <b>SVM名</b><br>データLIFを作成するSVMの名前を指定します。 | ○  |   |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 必須 | 値           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|-------------|
| <p><b>データLIF名</b></p> <ul style="list-style-type: none"> <li>クライアントがSVMサーバ上のデータにアクセスするときに使用する論理ネットワーク インターフェイスに付ける名前を指定します。</li> <li>ノードに利用可能なデータ ポートがある場合は、ノードごとに複数のデータLIFを割り当てたり、クラスタ内の任意のノードにLIFを割り当てたりすることができます。</li> <li>冗長性を確保するには、データ サブネットごとに2つ以上のデータLIFを作成する必要があり、特定のサブネットに割り当てられたLIFには、異なるノード上のホーム ポートを割り当てる必要があります。</li> </ul> <p><b>重要:</b> ノンストップ オペレーション ソリューション用にHyper-VまたはSQL Server over SMBをホストするCIFSサーバを設定する場合は、クラスタ内のStorage Virtual Machine (SVM)のすべてのノードに少なくとも1つのデータLIFが存在する必要があります。</p> <ul style="list-style-type: none"> <li>インターフェイスにはわかりやすい名前を指定でき、ホーム ノードとして割り当てられているノードに基づく名前をデータLIFに付けることなどが可能です。たとえば、ホーム ノードがノード1のLIFに「lif1」、ホーム ノードがノード2のLIFに「lif2」のように名前を指定できます。</li> <li>各データLIFのLIF名を記録する必要があります。</li> </ul> | ○  |             |
| <p><b>LIFのロール</b></p> <ul style="list-style-type: none"> <li>LIFのロールを指定します。</li> <li>データLIFにはデータ ロールが割り当てられます。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ○  | <b>data</b> |
| <p><b>許可されたプロトコル</b></p> <ul style="list-style-type: none"> <li>データLIFを使用できるプロトコルを指定します(CIFS、NFS、FlexCache、iSCSI、FC、なし)。</li> <li>デフォルトでは、CIFS、NFS、およびFlexCacheが許可されています。</li> </ul> <p>FlexCacheプロトコルを使用するボリュームは、7-Modeを実行しているData ONTAPが動作しているシステムのFlexCacheボリュームの元のボリュームにすることができます。</p> <p><b>注:</b> LIFを使用できるプロトコルは、LIFが作成されたあとは変更できません。将来的にデータLIF上でその他のプロトコルを許可する場合は、LIFを作成する際にそのプロトコルを許可するようLIFを設定する必要があります。</p>                                                                                                                                                                                                                                                                                                                          | ×  |             |
| <p><b>データLIFのホーム ノード</b></p> <ul style="list-style-type: none"> <li>ホーム ノードは、LIFがホーム ポートにリポートされるときに論理インターフェイスに戻るノードです。</li> <li>各データLIFのホーム ノードを記録する必要があります。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ○  |             |

| 情報の種類                                                                                                                                                                     | 必須                                   | 値 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|---|
| <b>データLIFのホーム ポート</b> <ul style="list-style-type: none"> <li>ホーム ポートは、LIFがホーム ポートにリバートされるときに論理インターフェイスが戻るポートです。</li> <li>各データLIFのホーム ポートを記録する必要があります。</li> </ul>          | ○                                    |   |
| <b>サブネット名</b> <ul style="list-style-type: none"> <li>SVMに割り当てるサブネットの名前です。</li> <li>アプリケーション サーバへの継続的な可用性が確保されたSMB接続を確立するために使用されるデータLIFはすべて、同じサブネット上にある必要があります。</li> </ul> | ○(サブネットを使用してデータLIFにネットワーク情報を割り当てる場合) |   |

## 関連情報

[clustered Data ONTAP 8.3 ネットワーク管理ガイド](#)

## ネーム サービスを設定する前に収集する情報

CIFSサーバを作成する前に、事前に決定した値を使用してDNSネーム サービスを設定する必要があります。必要に応じて、各ネーム サービスにどのソースを使用するかや、ネーム サービス データベースで情報を検索する順番を設定できます。さらに、NISまたはLDAPネーム サービスを設定することもできます。

### ネーム サービス データベース内でのネーム サービスの順番を設定するための情報(オプション)

Storage Virtual Machine (SVM) は、ネーム サービス (nsswitch) データベースを使用して、指定されたネーム サービスを検索するネーム サービス ソースの順番を決定します。デフォルトの設定を使用することも、ネーム サービスの順番をカスタマイズすることもできます。

データベース テーブルには、次の各データベース タイプについてネーム サービスのリストが格納されます。

| データベース タイプ | ネーム サービス ソースの用途 | 有効なソース         | 各ネーム サービスのデフォルト |
|------------|-----------------|----------------|-----------------|
| hosts      | ホスト名のIPアドレスへの変換 | files、dns      | files、dns       |
| group      | ユーザ グループ情報の検索   | files、nis、ldap | ファイル            |
| passwd     | ユーザ情報の検索        | files、nis、ldap | ファイル            |
| netgroup   | ネットグループ情報の検索    | files、nis、ldap | ファイル            |
| namemap    | ユーザ名のマッピング      | files、ldap     | ファイル            |

デフォルトの設定を使用する場合、ネーム サービス データベースの順番について追加の設定は必要はありません。デフォルト以外の値を使用する場合は、必要な値を入力する必要があります。

| ネーム サービス | デフォルトを使用するか<br>どうか | 値 |
|----------|--------------------|---|
| Hosts    |                    |   |

| ネーム サービス | デフォルトを使用するか<br>どうか | 値 |
|----------|--------------------|---|
| Group    |                    |   |
| Passwd   |                    |   |
| Netgroup |                    |   |
| Namemap  |                    |   |

注: NISまたはLDAPネーム サービスを設定する場合は、必要なネーム サービスを希望する順番で使用するよう適切なネーム サービス データベースを設定する必要があります。

### DNSを設定するための情報

CIFSサーバを作成する前に、SVMでDNSを設定する必要があります。

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 必須                    | 値 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---|
| <b>SVM名</b><br>CIFSサーバを作成するSVMの名前を指定します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <input type="radio"/> |   |
| <b>DNSドメイン名</b> <ul style="list-style-type: none"> <li>ホストとIPの名前解決を行う際に、ホスト名に付加するドメイン名のリストを指定します。</li> <li>ローカルドメインを最初にリストし、その後にDNSクエリが最も頻繁に行われているドメイン名を指定します。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <input type="radio"/> |   |
| <b>DNSサーバのIPアドレス</b> <ul style="list-style-type: none"> <li>CIFSサーバの名前解決を提供するDNSサーバのIPアドレスのリスト。</li> <li>これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス ロケーション レコード(SRV)が含まれている必要があります。<br/>SRVレコードは、サービスの名前を、そのサービスを提供するサーバのDNSコンピュータ名にマップするために使用されます。ローカルのDNSクエリを介してサービス ロケーション レコードを取得できない場合は、CIFSサーバの作成に失敗します。<br/>Data ONTAPがActive Directory SRVレコードを確実に見つけることができるようにする最も簡単な方法は、Active Directoryを統合したDNSサーバをSVMのDNSサーバとして構成することです。<br/>DNS管理者が手動で、Active Directoryドメイン コントローラに関する情報を含んだDNSゾーンにSRVのレコードを追加した場合は、Active Directoryを統合していないDNSサーバを使用することができます。</li> <li>Active Directoryを統合したSRVのレコードの詳細については、「<i>How DNS Support for Active Directory Works</i>」(Microsoft TechNet)を参照してください。<br/><a href="#">Microsoft TechNet: 「How DNS Support for Active Directory Works」</a></li> </ul> | <input type="radio"/> |   |

他のオプション パラメータの設定方法については、コマンドのマニュアル ページを参照してください。

### SVM上で動的DNSを設定するための情報

動的DNSを使用して自動的にActive Directory統合DNSサーバにDNSエントリを追加する前に、SVMに動的DNS(DDNS)を設定する必要があります。SVM上のDDNSの設定は、CIFSサーバを設定する前に行います。SVM上にあるすべてのデータLIFについてDNSレコードが作成されます。SVM上に複数のデータLIFを作成することによって、割り当てられたデータIPアドレスへのクライアント接続の負荷を分散することができます。DNSは、そのホスト名を使用して、割り当てられたIPアドレスへの接続をラウンドロビン方式で確立することで、接続の負荷を分散します。

| 情報の種類                                                                                                                                                                                                                                                    | 必須       | 値 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---|
| <b>SVM名</b><br>CIFSサーバを作成するSVMの名前を指定します。                                                                                                                                                                                                                 | ○        |   |
| <b>DDNSを使用するかどうか</b> <ul style="list-style-type: none"> <li>DDNSを使用するかどうかを指定します。</li> <li>SVM上で設定されているDNSサーバがDDNSをサポートしている必要があります。デフォルトではDDNSは無効になっています。</li> </ul>                                                                                      | ○(有効な場合) |   |
| <b>Secure DDNSを使用するかどうか</b> <ul style="list-style-type: none"> <li>Secure DDNSは、Active Directory統合DNSでのみサポートされています。</li> <li>Active Directory統合DNSでSecure DDNS更新のみを許可する場合、このパラメータの値をtrueに設定する必要があります。</li> <li>デフォルトでは、Secure DDNSは無効になっています。</li> </ul> | ×        |   |
| <b>DNSドメインのFQDN</b> <ul style="list-style-type: none"> <li>DNSドメインのFQDNを指定します。</li> <li>SVM上のDNSネーム サービスに設定されているドメイン名と同じ名前を使用する必要があります。</li> </ul>                                                                                                       | ×        |   |

### NISを設定するための情報(オプション)

- ネーム サービス データベースを設定する際にネーム サービス オプションとしてNISを指定した場合、SVMのNISドメイン設定を作成する必要があります。
- UNIXのユーザとグループについての情報検索やWindowsからUNIXへのユーザ名のマッピングにNISを使用する場合、正常にSMBアクセスが行えるようにNISを設定する必要があります。
- すべてのネーム マッピングにデフォルトのUNIXユーザを使用する場合は、このSVMにNISを設定しなくてもよい場合もあります。

| 情報の種類                            | 必須 | 値 |
|----------------------------------|----|---|
| <b>SVM名</b><br>NISを設定するSVMの名前です。 | ○  |   |



| 情報の種類                                                                                                                                                        | 必須                    | 値 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---|
| <b>NISドメイン名</b> <ul style="list-style-type: none"> <li>設定を作成するNISドメイン名です。</li> <li>NISドメイン名は最大64文字です。</li> </ul>                                             | <input type="radio"/> |   |
| <b>NISサーバのIPアドレス</b> <ul style="list-style-type: none"> <li>NISサーバのIPアドレスのリストです。</li> <li>複数のNISサーバをカンマで区切って指定できます。</li> </ul>                               | <input type="radio"/> |   |
| <b>NIS設定がアクティブかどうか</b> <ul style="list-style-type: none"> <li>NISドメイン設定がアクティブかどうかを指定します。</li> <li>SVMには複数のNISドメイン設定を指定できますが、アクティブにできるのは一度に1つだけです。</li> </ul> | <input type="radio"/> |   |

SVMでのLDAPの設定については、『*clustered Data ONTAP ファイル アクセス管理ガイド(NFS)*』を参照してください。

#### 関連情報

[clustered Data ONTAP 8.3 ファイル アクセス管理ガイド\(NFS\)](#)

### CIFSサーバを作成する前に収集する情報

CIFSサーバを作成する前に、CIFSサーバを作成するStorage Virtual Machine(SVM)の名前、CIFSサーバの名前、参加するドメインなどの情報を決定する必要があります。また、オプションでコンピュータ オブジェクト用のOU、コメント、NetBIOSエイリアス名も決定します。

以下で説明する値は、デフォルト データSVM上にCIFSサーバを作成するという仮定に基づいたものです。MetroClusterソースSVM上にCIFSサーバを作成する場合は、『*MetroClusterインストールオプションおよび構成ガイド*』を参照してください。

| 情報の種類                                                                                                                                                                                                                                | 必須                    | 値 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---|
| <b>SVM名</b><br>CIFSサーバをホストするSVMの名前                                                                                                                                                                                                   | <input type="radio"/> |   |
| <b>CIFSサーバ名</b> <ul style="list-style-type: none"> <li>CIFSサーバの名前。</li> <li>CIFSサーバの名前とSVMの名前は、同じであったり異なったりすることがあります。</li> <li>CIFSサーバの名前には15文字以内の名前を設定できます。次の文字は使用できません。<br/>@ # * ( ) = + [ ]   ; : " , &lt; &gt; \ / ?</li> </ul> | <input type="radio"/> |   |
| <b>ドメイン名</b> <ul style="list-style-type: none"> <li>CIFSサーバを参加させるActive DirectoryドメインのFQDN。</li> <li>CIFSサーバは、Active Directoryストア内のメンバーWindowsサーバ オブジェクトとして表示されます。</li> </ul>                                                        | <input type="radio"/> |   |

| 情報の種類                                                                                                                                                                                                                                                                                     | 必須 | 値 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---|
| <b>OU (組織単位)</b> <ul style="list-style-type: none"> <li>CIFSサーバのコンピュータ オブジェクトを配置するActive Directoryドメイン内のOU。</li> <li>デフォルトで、CIFSサーバのコンピュータ オブジェクトの格納場所は、CN=Computersです。</li> </ul>                                                                                                        | ×  |   |
| <b>コメント</b> <ul style="list-style-type: none"> <li>CIFSサーバについて説明する256文字以内のテキスト コメント。</li> <li>SMBクライアントは、ネットワーク上のサーバを参照するとき、CIFSサーバのコメントを確認できます。</li> <li>コメントにスペースが含まれる場合は、文字列全体を引用符で囲む必要があります。</li> </ul>                                                                               | ×  |   |
| <b>NetBIOS エイリアス</b> <ul style="list-style-type: none"> <li>1つまたは複数のNetBIOSエイリアスをカンマで区切って指定します。エイリアスはCIFSサーバの別名です。</li> <li>CIFSサーバには最大200個までのNetBIOSエイリアスを設定できます。</li> <li>NetBIOSエイリアス名は15文字以内で指定します。</li> <li>次の文字は使用できません。<br/>@ # * ( ) = + [ ]   ; : " , &lt; &gt; \ / ?</li> </ul> | ×  |   |

Data ONTAPは、CIFSサーバに関連付けるデフォルト サイトを特定しようとします。Data ONTAPがCIFSサーバの適切なサイトを特定できない場合、CIFSサーバを作成する際にデフォルトのサイトを指定できます。デフォルトでは、新しく作成されるCIFSサーバの初期管理ステータスはupです。CIFSサーバを作成する際、CIFSサーバの初期ステータスをdownに指定することができます。詳細については、`vserver cifs create`コマンドのマニュアル ページを参照してください。

#### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: `vserver cifs create` - Create a CIFS server](#)  
[clustered Data ONTAP 8.3 MetroCluster インストレーションおよび構成ガイド](#)

## CIFSサーバのセットアップ

CIFSサーバをセットアップするには、まずCIFSサーバ設定ワークシートに情報を記入します。そのあと、CIFS アクセス用に適切にStorage Virtual Machine (SVM)を設定し、SVM上のDNSを構成し、CIFS サーバを作成します。さらに、必要に応じて、UNIXのユーザとグループのネーム サービスをセットアップします。

CIFSサーバをセットアップするには、セットアップの実行時に選択する必要がある項目を事前に確認しておく必要があります。設定を作成する前に、SVM、DNS、およびCIFSサーバの設定について検討し、それを計画ワークシートに記入しておく、CIFSサーバを作成する際に役立ちます。

SVMの作成は、クラスタ管理者だけが実行できます。

## 手順

1. **タイム サービスの設定 (クラスタ管理者のみ)** (52ページ)  
クラスタ時間とCIFSサーバが参加するドメインのドメイン コントローラの時間のずれは5分以内である必要があります。CIFSサーバを作成する前に、クラスタでタイム サービスを設定する必要があります。
2. **SVMのIPspaceの作成 (クラスタ管理者のみ)** (52ページ)  
CIFSサーバを作成するStorage Virtual Machine (SVM)を作成する前に、SVMを配置するIPspaceを設定する必要があります。IPspaceは、ストレージ、管理、およびルーティングを保護するために使用する個別のIPアドレス スペースです。
3. **新しいブロードキャストドメインに使用できるポートの確認 (クラスタ管理者のみ)** (53ページ)  
新しいIPspaceに追加するブロードキャストドメインを設定する前に、新しいブロードキャストドメインに使用できる未使用のポートを確認する必要があります。
4. **新しいブロードキャストドメインに追加するポートの既存のブロードキャストドメインからの削除 (クラスタ管理者のみ)** (55ページ)  
新しいブロードキャストドメインに追加するポートがすでに別のブロードキャストドメインにある場合は、新しいブロードキャストドメインに割り当てる前にそのブロードキャストドメインからポートを削除する必要があります。
5. **IPspaceのブロードキャストドメインの作成 (クラスタ管理者のみ)** (56ページ)  
IPspaceのブロードキャストドメインを作成する必要があります。ブロードキャストドメインは、同じレイヤ2ネットワークにグループ化されるネットワーク ポートを定義します。ブロードキャストドメイン内のポートは、そのIPspaceに割り当てられたStorage Virtual Machine (SVM)で使用できます。
6. **IPspaceのサブネットの作成 (クラスタ管理者のみ)** (58ページ)  
ブロードキャストドメインの作成後、サブネットを作成してIPv4またはIPv6アドレスの特定のブロックを割り当てます。このサブネットは、あとでStorage Virtual Machine (SVM) のLIFを作成するときに使用します。IPアドレスとネットワーク マスクの値をLIFごとに指定しなくても、サブネット名を指定して簡単にLIFを作成できるようになります。
7. **CIFSサーバ用のFlexVolを備えたSVMの作成 (クラスタ管理者のみ)** (59ページ)  
CIFSサーバを作成する前に、CIFSサーバをホストするのに適切な設定を使用してStorage Virtual Machine (SVM)を作成する必要があります。
8. **SVMでのLIFの作成 (クラスタ管理者のみ)** (61ページ)  
CIFSサーバへのSMBアクセスを提供するためには、Storage Virtual Machine (SVM)にLIFを作成する必要があります。作成するLIFは、Active Directory (AD)ドメイン コントローラ、DNS、NIS、LDAP、NDMPなど、サービスに必要なすべての外部サーバへのルーティングが可能である必要があります。
9. **SVM用のDNSサービスの設定** (63ページ)  
CIFSサーバを作成する前に、Storage Virtual Machine (SVM)でDNSサービスを設定する必要があります。通常、DNSネーム サーバは、CIFSサーバが参加するドメインのActive Directory 統合DNSサーバです。
10. **SVMでの動的DNSの設定** (65ページ)  
Active Directoryに統合されたDNSサーバをCIFSサーバのDNSにあるDNSレコードに動的に登録する場合、CIFSサーバを作成する前にStorage Virtual Machine (SVM)上の動的DNS (DDNS)を設定する必要があります。
11. **CIFSサーバの作成** (65ページ)  
SMBクライアントがStorage Virtual Machine (SVM)にアクセスするためには、CIFSサーバが必要です。SVMでDNSサービスをセットアップしたあとで、CIFSサーバを作成できます。
12. **SVM上のNISまたはLDAPネーム サービスの設定** (68ページ)  
SMBアクセスでは、NTFSセキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIXユーザへのユーザ マッピングが常に実行されます。NISまたはLDAPディレクトリストアにその情報が格納されているUNIXユーザにWindowsユーザをマッピングする場合や、ネーム

マッピングにLDAPを使用する場合は、CIFSのセットアップ時にこのネーム サービスを設定する必要があります。

#### 関連コンセプト

[CIFSサーバのセットアップの前提条件](#)(37ページ)

[CIFSサーバの設定の計画](#)(38ページ)

[CIFSサーバの管理](#)(71ページ)

#### 関連情報

[clustered Data ONTAP 8.3 システム アドミニストレーション ガイド](#)

[clustered Data ONTAP 8.3 ネットワーク管理ガイド](#)

## タイム サービスの設定(クラスタ管理者のみ)

クラスタ時間とCIFSサーバが参加するドメインのドメイン コントローラの時間のずれは5分以内である必要があります。CIFSサーバを作成する前に、クラスタでタイム サービスを設定する必要があります。

#### タスク概要

##### 手順

1. `cluster time-service ntp server create`コマンドを使用して、タイム サービスを設定します。

##### 例

```
cluster time-service ntp server create -server 10.10.10.1
```

```
cluster time-service ntp server create -server 10.10.10.2
```

2. `cluster time-service ntp server show`コマンドを使用して、タイム サービスの設定が正しいことを確認します。

##### 例

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

| Server     | Version |
|------------|---------|
| 10.10.10.1 | auto    |
| 10.10.10.2 | auto    |

#### 関連参照情報

[タイム サービスを設定する前に収集する情報](#)(38ページ)

## SVMのIPspaceの作成(クラスタ管理者のみ)

CIFSサーバを作成するStorage Virtual Machine(SVM)を作成する前に、SVMを配置するIPspaceを設定する必要があります。IPspaceは、ストレージ、管理、およびルーティングを保護するために使用する個別のIPアドレス スペースです。

#### タスク概要

SVMを割り当てるIPspaceがすでに設定されている場合は、新規に設定する代わりにそのIPspaceを使用できます。

**手順**

1. `network ipspace create`コマンドを使用してIPspaceを作成します。

**例**

```
network ipspace create -ipspace ipspace1
```

```
network ipspace show
```

| IPspace  | Vserver List | Broadcast Domains |
|----------|--------------|-------------------|
| Cluster  | Cluster      | Cluster           |
| Default  | cluster1     | Default           |
| ipspace1 | ipspace1     | -                 |

IPspaceが、そのIPspaceのシステムSVMとともに作成されます。システムSVMは管理トラフィックを伝送します。

**終了後の操作**

IPspaceのブロードキャストドメインを設定する必要があります。

- ブロードキャストドメインに追加するポートを決定する必要があります。
- ポートが現在別のブロードキャストドメインに割り当てられている場合は、そのブロードキャストドメインから削除して未割り当ての状態にし、新しいブロードキャストドメインに追加できるようにします。
- これで新しいブロードキャストドメインを作成してポートを追加できます。

**関連参照情報**

[IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収集する情報](#) (39ページ)

**新しいブロードキャストドメインに使用できるポートの確認(クラスタ管理者のみ)**

新しいIPspaceに追加するブロードキャストドメインを設定する前に、新しいブロードキャストドメインに使用できる未使用のポートを確認する必要があります。

**開始する前に**

既存のLIFはすべてホーム ポートに関連付けられています。

**タスク概要**

- デフォルトでは、ポートはクラスタIPspaceまたはデフォルトIPspaceのどちらかに割り当てられます。
  - クラスタIPspaceには、クラスタ ブロードキャストドメインが含まれます。このドメインは、クラスタ ポートとして割り当てられたポートのコンテナです。
  - デフォルトIPspaceには、デフォルト ブロードキャストドメインが含まれます。このドメインは、ポート、サブネット、およびデータを提供するStorage Virtual Machine (SVM) のデフォルトのコンテナです。
  - デフォルトIPspaceには、クラスタ管理LIFおよびノート管理LIFに割り当てられたポートも含まれます。

- デフォルトIPspace内の未使用のポートは、非クラスタ ポートのデフォルトのコンテナであり、新しいブロードキャストドメインに使用できます。
- ポートには、物理ポート、VLAN、またはインターフェイス グループ（インターフェイス ポートの論理グループ）、別名 *ifgroup* があります。  
このCIFSサーバセットアップ ワークフロー では物理ポートを使用します。VLANまたはインターフェイス グループの設定の詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』、または `network port ifgrp` および `network port vlan` コマンド ファミリーのマニュアル ページを参照してください。
- 既存のブロードキャストドメインに割り当てられているポートを新しいブロードキャストドメインに追加することはできません。
- ブロードキャストドメインに追加するポートがすでに別のブロードキャストドメイン（たとえば、デフォルトIPspace内のデフォルト ブロードキャストドメイン）に割り当てられている場合は、そのブロードキャストドメインからポートを削除したあとで、新しいブロードキャストドメインに割り当てる必要があります。
- LIFが割り当てられているポートをブロードキャストドメインから削除することはできません。
- クラスタ管理LIFおよびノード管理LIFはデフォルトIPspace内のデフォルト ブロードキャストドメインに割り当てられるので、これらのLIFに割り当てられているポートはデフォルト ブロードキャストドメインから削除できません。

#### 手順

1. `network port show` コマンドを使用して、現在のポートの割り当てを確認します。

#### 例

##### `network port show`

| Node  | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper |
|-------|------|---------|------------------|------|------|------------|
| node1 |      |         |                  |      |      |            |
|       | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0f  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0g  | Default | Default          | up   | 1500 | auto/1000  |
| node2 |      |         |                  |      |      |            |
|       | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0f  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0g  | Default | Default          | up   | 1500 | auto/1000  |

この例では、コマンドの出力から次の情報が得られます。

- 各ノードのポート **e0c**、**e0d**、**e0e**、**e0f**、および **e0g** はデフォルト ブロードキャストドメインに割り当てられています。
  - これらのポートは、作成するIPspaceのブロードキャストドメインで使用できる可能性があります。
2. `network interface show` コマンドを使用して、デフォルト ブロードキャストドメイン内の、LIF インターフェイスに割り当てられている、したがって新しいブロードキャストドメインに移動できないポートを確認します。

**例****network interface show**

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| Cluster | node1_clus1       | up/up             | 10.0.2.40/24         | node1        | e0a          | true    |
|         | node1_clus2       | up/up             | 10.0.2.41/24         | node1        | e0b          | true    |
|         | node2_clus1       | up/up             | 10.0.2.42/24         | node2        | e0a          | true    |
|         | node2_clus2       | up/up             | 10.0.2.43/24         | node2        | e0b          | true    |
|         | cluster1          |                   |                      |              |              |         |
|         | cluster_mgmt      | up/up             | 10.0.1.41/24         | node1        | e0c          | true    |
|         | node1_mgmt        | up/up             | 10.0.1.42/24         | node1        | e0c          | true    |
|         | node2_mgmt        | up/up             | 10.0.1.43/24         | node2        | e0c          | true    |
|         |                   |                   |                      |              |              |         |
|         |                   |                   |                      |              |              |         |

この例では、コマンドの出力から次の情報が得られます。

- ノード ポートは各ノードのポートe0cに割り当てられており、クラスタ管理LIFのホーム ノードはnode1のe0cにあります。
- 各ノードのポートe0d、e0e、e0f、およびe0gはLIFをホストしていないので、デフォルトブロードキャストドメインから削除して、新しいIPspaceの新しいブロードキャストドメインに追加できます。

**終了後の操作**

新しいブロードキャストドメインを作成する前に、このタスクで得た情報を使用して既存のブロードキャストドメインからポートを削除します。

**関連参照情報**

[IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収集する情報](#) (39ページ)

## 新しいブロードキャストドメインに追加するポートの既存のブロードキャストドメインからの削除(クラスタ管理者のみ)

新しいブロードキャストドメインに追加するポートがすでに別のブロードキャストドメインにある場合は、新しいブロードキャストドメインに割り当てる前にそのブロードキャストドメインからポートを削除する必要があります。

**開始する前に**

既存のブロードキャストドメインからどのポートを削除できるかを把握しておく必要があります。

**手順**

1. network port broadcast-domain remove-portsコマンドを使用して、Defaultブロードキャストドメインから新しいブロードキャストドメインに割り当てるポートを削除します。

**例**

```
network port broadcast-domain remove-ports -ipspace Default -broadcast-domain Default -ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
```

2. `network port show`コマンドを使用して、ポートがブロードキャストドメインに割り当てられていないことを確認します。

**例**

```
network port show
```

| Node  | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper |
|-------|------|---------|------------------|------|------|------------|
| ----- |      |         |                  |      |      |            |
| node1 | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0d  | Default | -                | up   | 1500 | auto/1000  |
|       | e0e  | Default | -                | up   | 1500 | auto/1000  |
|       | e0f  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0g  | Default | Default          | up   | 1500 | auto/1000  |
| node2 | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|       | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0d  | Default | -                | up   | 1500 | auto/1000  |
|       | e0e  | Default | -                | up   | 1500 | auto/1000  |
|       | e0f  | Default | Default          | up   | 1500 | auto/1000  |
|       | e0g  | Default | Default          | up   | 1500 | auto/1000  |

**終了後の操作**

未割り当てのポートを使用して新しいブロードキャストドメインを作成することができます。

**関連参照情報**

[IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収集する情報](#) (39ページ)

**IPspaceのブロードキャストドメインの作成(クラスタ管理者のみ)**

IPspaceのブロードキャストドメインを作成する必要があります。ブロードキャストドメインは、同じレイヤ2ネットワークにグループ化されるネットワークポートを定義します。ブロードキャストドメイン内のポートは、そのIPspaceに割り当てられたStorage Virtual Machine (SVM) で使用できます。

**開始する前に**

- ブロードキャストドメインを割り当てるIPspaceが存在している必要があります。
- 未割り当てで、新しいブロードキャストドメインに追加できるポートを確認しておく必要があります。

**タスク概要**

ブロードキャストドメインを作成すると、ブロードキャストドメインのフェイルオーバーグループが自動的に作成されます。フェイルオーバーグループには、ブロードキャストドメインに割り当てられたすべてのポートが含まれます。

**手順**

1. `network port broadcast-domain create`コマンドを使用してブロードキャストドメインを作成します。

**例**

```
network port broadcast-domain create -ipspace ipspace1 -broadcast-domain
-ippace1 -mtu 1500 -ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
```

2. 次のコマンドを使用して、ブロードキャストドメインの設定が正しいことを確認します。



- a. network port broadcast-domain show
- b. network port show
- c. network interface failover-groups show

**例****network port broadcast-domain show**

| IPspace Name | Broadcast Domain Name | MTU  | Port List                                                                  | Update Status                                                        | Details |
|--------------|-----------------------|------|----------------------------------------------------------------------------|----------------------------------------------------------------------|---------|
| Cluster      | Cluster               | 1500 | node1:e0a<br>node1:e0b<br>node2:e0a<br>node2:e0b                           | complete<br>complete<br>complete<br>complete                         |         |
| Default      | Default               | 1500 | node1:e0c<br>node1:e0f<br>node1:e0g<br>node2:e0c<br>node2:e0f<br>node2:e0g | complete<br>complete<br>complete<br>complete<br>complete<br>complete |         |
| ipspace1     | ipspace1              | 1500 | node1:e0d<br>node1:e0e<br>node2:e0d<br>node2:e0e                           | complete<br>complete<br>complete<br>complete                         |         |

**network port show**

| Node  | Port | IPspace  | Broadcast Domain | Link | MTU  | Admin/Oper |
|-------|------|----------|------------------|------|------|------------|
| node1 | e0a  | Cluster  | Cluster          | up   | 1500 | auto/1000  |
|       | e0b  | Cluster  | Cluster          | up   | 1500 | auto/1000  |
|       | e0c  | Default  | Default          | up   | 1500 | auto/1000  |
|       | e0d  | ipspace1 | ipspace1         | up   | 1500 | auto/1000  |
|       | e0e  | ipspace1 | ipspace1         | up   | 1500 | auto/1000  |
|       | e0f  | Default  | Default          | up   | 1500 | auto/1000  |
|       | e0g  | Default  | Default          | up   | 1500 | auto/1000  |
| node2 | e0a  | Cluster  | Cluster          | up   | 1500 | auto/1000  |
|       | e0b  | Cluster  | Cluster          | up   | 1500 | auto/1000  |
|       | e0c  | Default  | Default          | up   | 1500 | auto/1000  |
|       | e0d  | ipspace1 | ipspace1         | up   | 1500 | auto/1000  |
|       | e0e  | ipspace1 | ipspace1         | up   | 1500 | auto/1000  |
|       | e0f  | Default  | Default          | up   | 1500 | auto/1000  |
|       | e0g  | Default  | Default          | up   | 1500 | auto/1000  |

**network interface failover-groups show**

| Vserver  | Group   | Failover Targets                                                       |
|----------|---------|------------------------------------------------------------------------|
| Cluster  | Cluster | node1:e0a, node1:e0b,<br>node2:e0a, node2:e0b                          |
| cluster1 | Default | node1:e0c, node1:e0f,<br>node1:e0g, node2:e0c,<br>node2:e0f, node2:e0g |

```

ipspace1
ipspace1
node1:e0d, node1:e0e,
node2:e0d, node2:e0e

```

### 終了後の操作

次に、ブロードキャストドメインのサブネットを作成します。

### 関連参照情報

[IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収集する情報](#) (39ページ)

## IPspaceのサブネットの作成(クラスタ管理者のみ)

ブロードキャストドメインの作成後、サブネットを作成してIPv4またはIPv6アドレスの特定のブロックを割り当てます。このサブネットは、あとでStorage Virtual Machine (SVM) のLIFを作成するときに使用します。IPアドレスとネットワーク マスクの値をLIFごとに指定しなくても、サブネット名を指定して簡単にLIFを作成できるようになります。

### 開始する前に

サブネットを追加する予定のブロードキャストドメインとIPspaceがすでに存在している必要があります。

### タスク概要

必須ではありませんが、LIFを作成するときはサブネットを使用してください。サブネットを使用することでLIFの管理が容易になります。次に示すサブネットの要件を満たしている必要があります。

- すべてのサブネット名がIPspace内で一意である必要があります。
- サブネットにIPアドレスの範囲を追加するときは、ルーティング可能なネットワーク内に重複するIPアドレスがないことを確認し、異なるサブネット、またはホストが同じIPアドレスを使用しないようにします。
- サブネットは、Active Directory (AD) ドメイン コントローラ、DNS、NIS、LDAP、NDMPなど、サービスに必要なすべての外部サーバへのルーティングが可能である必要があります。

このCIFSサーバのセットアップでは、サブネットを使用して、IPアドレス、ネットマスク、およびデフォルト ゲートウェイをデータLIFに割り当てます。もう1つの方法として、IPアドレスとネットマスクを指定してLIFを作成し、その後デフォルト ゲートウェイを別のタスクとして作成する方法があります。ネットワーク ソリューションの設定に関する選択肢の詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』を参照してください。

### 手順

1. `network subnet create` コマンドを使用してサブネットを作成します。

#### 例

```

network subnet create -broadcast-domain ipspace1 -ipspace ipspace1 -
subnet-name ipspace1 -subnet 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges
"10.0.0.128-10.0.0.130,10.0.0.132"

```

サブネット名には、「192.0.2.0/24」などのサブネットIPの値を使用することも、この例のように「ipspace1」などの文字列を使用することもできます。

2. `network subnet show` コマンドを使用して、サブネットの設定が正しいことを確認します。

**例**

この例では、「ipospace1」IPspace内の「ipospace1」という名前のサブネットに関する情報が出力に表示されます。サブネットは「ipospace1」という名前のブロードキャストドメインに属します。「ipospace1」IPspaceに作成したSVMのデータLIFに、このサブネット内のIPアドレスを割り当てることができます。

```
network subnet show -ipospace ipospace1
```

```
IPspace: ipospace1
Subnet
Name      Subnet      Broadcast
Domain    Gateway     Avail/
-----
ipospace1 10.0.0.0/24  ipospace1 10.0.0.1    4/4
Ranges
10.0.0.128-10.0.0.130,
10.0.0.132
```

**終了後の操作**

- CIFSサーバを配置するSVMを作成する必要があります。
- 次に、SVM上にLIFを作成し、作成したサブネットをLIFに関連付けます。

**関連参照情報**

[IPspace、ブロードキャストドメイン、サブネット構成を作成する前に収集する情報](#)(39ページ)

**CIFSサーバ用のFlexVolを備えたSVMの作成(クラスタ管理者のみ)**

CIFSサーバを作成する前に、CIFSサーバをホストするのに適切な設定を使用してStorage Virtual Machine(SVM)を作成する必要があります。

**開始する前に**

SVMを作成する前に、次の前提条件を満たす必要があります。

- SVMのルート ボリュームを作成するアグリゲートが存在している必要があります。
- デフォルト以外のIPspaceにSVMを作成する場合は、IPspaceがすでに存在している必要があります。
- ルート ボリュームに設定するセキュリティ形式を決めておく必要があります。  
このSVMにHyper-V over SMBまたはSQL Server over SMBソリューションを実装する予定がある場合は、ルート ボリュームにNTFSセキュリティ形式を使用してください。Hyper-VファイルまたはSQLデータベース ファイルを格納するボリュームは、作成時にNTFSセキュリティ形式に設定する必要があります。ルート ボリュームのセキュリティ形式をNTFSに設定することで、UNIXセキュリティ形式またはmixedセキュリティ形式のデータ ボリュームを誤って作成することがなくなります。

**タスク概要**

Infinite Volumeを備えたSVMの作成の詳細については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

データ保護またはMetroCluster SVMなど、他の種類のSVMの作成の詳細については、『*clustered Data ONTAP データ保護ガイド*』および『*MetroClusterインストールおよび構成ガイド*』を参照してください。

**手順**

1. ノードのルート アグリゲートを除く、クラスタ内のすべてのアグリゲートに関する情報を表示して、SVMのルート ボリュームを格納するためのアグリゲートを決定します。

```
storage aggregate show -has-mroot false
```

#### 例

```
storage aggregate show -has-mroot false
```

| Aggregate | Size    | Available | Used% | State  | #Vols | Nodes | RAID     | Status |
|-----------|---------|-----------|-------|--------|-------|-------|----------|--------|
| aggr1     | 239.0GB | 229.8GB   | 4%    | online | 4     | node1 | raid_dp, | normal |
| aggr2     | 239.0GB | 235.9GB   | 1%    | online | 2     | node2 | raid_dp, | normal |
| aggr3     | 478.1GB | 465.2GB   | 3%    | online | 1     | node2 | raid_dp, | normal |

SVMのルート ボリュームには、独立したアグリゲートを使用することを推奨します。データ ボリュームが格納されているアグリゲートにルート ボリュームを作成しないでください。

ルート ボリュームを格納するための空きスペースが1GB以上あるアグリゲートを選択する必要があります。SVMでNASの監査を設定する場合は、ルート アグリゲートに少なくとも3GBの追加の空きスペースと、監査を有効にしたときに監査ステージング ボリュームの作成に使用される追加のスペースが必要です。

注: 既存のSVMでNASの監査がすでに有効になっている場合は、アグリゲートの作成が完了したあとすぐにアグリゲートのステージング ボリュームが作成されます。

2. SVMのルート ボリュームを作成するアグリゲートの名前を控えます。
3. SVMを作成するときに言語を指定する予定があり、使用する値がわからない場合は、指定する言語の値を確認し、その値を控えます。

```
vserver create -language ?
```

4. SVMを作成するときにSnapshotポリシーを指定する予定があり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用するSnapshotポリシーの名前を確認して、その名前を控えます。

```
volume snapshot policy show -vserver vserver_name
```

5. SVMを作成するときにクォータ ポリシーを指定する予定があり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用するクォータ ポリシーの名前を確認して、その名前を控えます。

```
volume quota policy show -vserver vserver_name
```

6. SVMを作成します。

```
vserver create -vserver vserver_name -aggregate aggregate_name
-rootvolume root_volume_name -rootvolume-security-style {unix|ntfs|mixed}
[-ipspace IPspace_name] [-language language] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment
comment]
```

#### 例

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. vserver showコマンドを使用して、SVMの設定が正しいことを確認します。

**例****vserver show -vserver vs1**

```

Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID:
11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
Is Vserver with Infinite Volume: false
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false

```

この例では、コマンドを実行すると「vs1」という名前のSVMがIPspace「ipspace1」に作成されます。ルートボリュームは、「vs1\_root」という名前で、NTFSセキュリティ形式を使用してaggr3に作成されます。

**関連タスク**

[SVMのプロトコルの変更](#) (138ページ)

**関連参照情報**

[SVMを設定する前に収集する情報](#) (42ページ)

**関連情報**

[Clustered Data ONTAP 8.3 Infinite Volumes Management Guide](#)

[clustered Data ONTAP 8.3 データ保護ガイド](#)

[clustered Data ONTAP 8.3 MetroClusterインストレーションおよび構成ガイド](#)

**SVMでのLIFの作成(クラスタ管理者のみ)**

CIFSサーバへのSMBアクセスを提供するためには、Storage Virtual Machine (SVM) にLIFを作成する必要があります。作成するLIFは、Active Directory (AD) ドメイン コントローラ、DNS、NIS、LDAP、NDMPなど、サービスに必要なすべての外部サーバへのルーティングが可能である必要があります。

**開始する前に**

LIFに割り当てるサブネット名を把握しておく必要があります。

**タスク概要**

- CIFSトラフィックを伝送するLIFを、ホーム ノードに自動的にリポートするように設定しないでください。

Hyper-V over SMBまたはSQL Server over SMBでノンストップ オペレーションを実現するソリューションをCIFSサーバでホストする場合、これは必須です。

- LIFの設定のカスタマイズに使用できるさまざまなオプションのパラメータが用意されています。オプション パラメータの使用の詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』を参照してください。

#### 手順

1. `network port broadcast-domain show`コマンドを使用して、LIFに使用するIPspaceブロードキャストドメインのポートを判断します。

#### 例

```
network port broadcast-domain show -ipspace ipspace1
```

| IPspace Name | Broadcast Domain Name | MTU  | Port List                                        | Update Status                                | Details |
|--------------|-----------------------|------|--------------------------------------------------|----------------------------------------------|---------|
| ipspace1     | ipspace1              | 1500 | node1:e0d<br>node1:e0e<br>node2:e0d<br>node2:e0e | complete<br>complete<br>complete<br>complete |         |

2. `network subnet show`コマンドを使用して、LIFに使用するサブネットに未使用のIPアドレスが十分にあることを確認します。

#### 例

```
network subnet show -ipspace ipspace1
```

| IPspace: ipspace1 |             |                  |          |             |                                      |
|-------------------|-------------|------------------|----------|-------------|--------------------------------------|
| Subnet Name       | Subnet      | Broadcast Domain | Gateway  | Avail/Total | Ranges                               |
| ipspace1          | 10.0.0.0/24 | ipspace1         | 10.0.0.1 | 4/4         | 10.0.0.128-10.0.0.130,<br>10.0.0.132 |

3. `network interface create`コマンドを使用して、SMB経由でSVM上のデータにアクセスするために使用するポートに1つ以上のLIFインターフェイスを作成します。

#### 例

```
network interface create -vserver vs1 -lif lif1 -role data -data-protocol nfs,cifs -home-node node1 -home-port e0d -subnet-name ipspace1
```

```
network interface create -vserver vs1 -lif lif2 -role data -data-protocol nfs,cifs -home-node node2 -home-port e0d -subnet-name ipspace1
```

4. `network interface show`コマンドを使用して、LIFインターフェイスの設定が正しいことを確認します。

#### 例

```
network interface show -vserver vs1
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| vs1     | lif1              | up/up             | 10.0.0.128/24        | node1        | e0d          | true    |
|         | lif2              | up/up             | 10.0.0.129/24        | node2        | e0d          | true    |

5. `-failover`パラメータを指定して`network interface show`コマンドを実行し、フェイルオーバー グループの設定が適切であることを確認します。

#### 例

`network interface show -failover -vserver vs1`

| Vserver | Logical Interface | Home Node:Port                                                            | Failover Policy | Failover Group |
|---------|-------------------|---------------------------------------------------------------------------|-----------------|----------------|
| vs1     | lif1              | node1:e0d<br>Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e | system-defined  | ipspace1       |
|         | lif2              | node2:e0d<br>Failover Targets: node2:e0d, node2:e0e, node1:e0d, node1:e0e | system-defined  | ipspace1       |

#### 終了後の操作

SVMのDNSネーム サービスを設定したあとで、CIFSサーバを作成できます。

#### 関連参照情報

[SVM上でデータLIFを作成する前に収集する情報](#)(44ページ)

## SVM用のDNSサービスの設定

CIFSサーバを作成する前に、Storage Virtual Machine (SVM) でDNSサービスを設定する必要があります。通常、DNSネーム サービスは、CIFSサーバが参加するドメインのActive Directory統合DNSサーバです。

#### タスク概要

Active Directory統合DNSサーバには、ドメインLDAPおよびドメイン コントローラ サーバのサービス ロケーション レコード (SRV) が格納されます。Storage Virtual Machine (SVM) がActive Directory LDAPサーバおよびドメイン コントローラを見つけられない場合は、CIFSサーバのセットアップに失敗します。

Storage Virtual Machine (SVM) は、ホストについての情報を検索する際に、**hosts**ネーム サービス `ns-switch`データベースを使用してどのネーム サービスを使用するか、どの順番で使用するかを決定します。ホスト データベースとしてサポートされている2つのネーム サービスは、**files**および**dns**です。

CIFSサーバを作成する前に、**dns**がソースの1つであることを確認する必要があります。

#### 手順

1. `vserver services name-service ns-switch show`コマンドを使用すると、現在の**hosts**ネーム サービス データベースの設定を確認できます。

#### 例

この例では、**hosts**ネーム サービス データベースはデフォルトの設定を使用しています。

```
vserver services name-service ns-switch show -vserver vs1 -database
hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. 必要に応じて、次の操作を実行します。

- a. DNSネーム サービスを希望の順番で**hosts**ネーム サービス データベースに追加するか、`vserver services name-service ns-switch modify`コマンドを使用してソースの順番を変更します。

**例**

この例では、DNSおよびローカル ファイルをこの順番で使用するように**hosts**データベースを設定しています。

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources dns,files
```

- b. `vserver services name-service ns-switch show`コマンドでネーム サービスの設定が正しいことを確認します。

**例**

```
vserver services name-service ns-switch show -vserver vs1 -database
hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. `vserver services name-service dns create`コマンドを使用して、DNSサービスを設定します。

**例**

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```

4. `vserver services name-service dns show`コマンドを使用して、DNSの設定が正しいことと、サービスが有効になっていることを確認します。

**例**

```
vserver services name-service dns show -vserver vs1
```

```
Vserver: vs1
Domains: example.com, example2.com
Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

## 関連参照情報

[ネーム サービスを設定する前に収集する情報](#)(46ページ)



## SVMでの動的DNSの設定

Active Directoryに統合されたDNSサーバをCIFSサーバのDNSにあるDNSレコードに動的に登録する場合、CIFSサーバを作成する前にStorage Virtual Machine (SVM) 上の動的DNS (DDNS) を設定する必要があります。

### 開始する前に

SVMでは、DNSネーム サービスが設定される必要があります。セキュアDDNSを使用している場合は、Active Directoryに統合されたDNSネーム サービスを使用する必要があります。

### 手順

1. SVM上のDDNSは次のように設定します。

```
vserver services name-service dns dynamic-update modify -vserver
vserver_name -is-enabled true [-use-secure {true|false}] -domain-name
FQDN_used_for_DNS_updates
```

#### 例

```
vserver services name-service dns dynamic-update modify -vserver vs1 -
is-enabled true -use-secure true -domain-name example.com
```

2. DDNS設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

#### 例

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Domain Name | TTL |
|---------|------------|------------|-------------|-----|
| vs1     | true       | true       | example.com | 24h |

## CIFSサーバの作成

SMBクライアントがStorage Virtual Machine (SVM) にアクセスするためには、CIFSサーバが必要です。SVMでDNSサービスをセットアップしたあとで、CIFSサーバを作成できます。

### 開始する前に

- 少なくとも1つのSVM LIFがSVMに存在している必要があります。
- LIFは、SVM上に設定されたDNSサーバ、およびCIFSサーバを追加するドメインのActive Directoryドメイン コントローラに接続できる必要があります。
- DNSサーバには、Active Directoryドメイン サービスを見つけるために必要なサービス ロケーション レコードが含まれている必要があります。
- クラスタ時間とActive Directoryドメイン コントローラの時刻を、誤差が5分以内となるように同期する必要があります。  
Active Directoryドメインと同じNTPサーバを時刻の同期に使用するようにクラスタNTPサービスを設定してください。

### タスク概要

CIFSサーバを作成する場合は、次の点に注意する必要があります。

- CIFSサーバには、SVMと同じ名前、または別の名前を指定できます。
- CIFSサーバ名は15文字以内にする必要があります。  
使用できない文字としては、@、#、\*、(、)、=、+、[、]、|、;、:、"、,、<、>、\、/、?があります。
- ドメインを指定するときはFQDNを使用する必要があります。
- デフォルトでは、CIFSサーバ マシン アカウントはActive Directory CN=Computerオブジェクトに追加されます。
- -ouオプションを使用して、CIFSサーバを別の組織単位(OU)に追加することもできます。  
OUを指定する場合は、識別名のドメイン部分は指定せず、識別名のOU部分またはCN部分のみ指定します。必須の-domainパラメータに指定した値が、-ouパラメータに指定した値に付加されて、Active Directory識別名が生成されます。この識別名は、Active Directoryドメインに追加するときに使用されます。
- 必要に応じて、CIFSサーバに関する256文字以内のテキスト コメントを追加できます。  
コメントテキスト内にスペースが含まれる場合は、文字列全体を引用符で囲む必要があります。
- 必要に応じて、CIFSサーバの1つ以上のNetBIOSエイリアス(最大200個)をカンマで区切って追加できます。  
NetBIOSエイリアス名は15文字以内にする必要があります。使用できない文字としては、@、#、\*、(、)、=、+、[、]、|、;、:、"、,、<、>、\、/、?があります。
- CIFSサーバの初期の管理ステータスはupです。

## 手順

1. SVM上にCIFSサーバを作成します。

```
vserver cifs create -vserver vserver_name -domain FQDN [-ou
organizational_unit] [-comment text] [-netbios-aliases
NetBIOS_name, ...]
```

ドメインに追加する場合、このコマンドの実行には数分かかることがあります。

### 例

```
vserver cifs create -vserver vs1 -name CIFS1 -domain example.com
```

2. `vserver cifs show`コマンドを使用して、CIFSサーバの設定を確認します。

**例**

この例では、「CIFS1」という名前のCIFSサーバがSVM vs1上に作成され、example.comドメインに追加されたことがコマンド出力に示されています。

```
vserver cifs show -vserver vs1
```

```

Vserver: vs1
CIFS Server NetBIOS Name: CIFS1
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -

```

**例**

次のコマンドを実行すると、「CIFS2」という名前のCIFSサーバがSVM vs1上に作成され、example.comドメインに追加されます。マシン アカウントは、OU=eng,OU=corp,DC=example,DC=comコンテナに作成されます。CIFSサーバにはNetBIOSエイリアスが割り当てられます。

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFS2 -domain
example.com -ou OU=eng,OU=corp -netbios-aliases CIFS4

cluster1::> vserver cifs show -vserver vs1
Vserver: vs1
CIFS Server NetBIOS Name: CIFS2
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFS Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: CIFS4
```

次のコマンドを実行すると、信頼できるドメインの管理者がSVM vs1上に「CIFS3」という名前のCIFSサーバを作成できるようになります。-domainオプションには、CIFSサーバを作成するホームドメイン(DNSの設定で指定される)の名前を指定します。usernameオプションには、信頼できるドメインの管理者を指定します。

ホームドメイン: example.com  
 信頼できるドメイン: trust.lab.com  
 信頼できるドメインのユーザ名: Administrator1

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFS3 -domain
example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

**関連コンセプト**

[オプションを使用したCIFSサーバのカスタマイズ](#)(71ページ)  
[CIFSサーバのセキュリティ設定の管理](#)(81ページ)  
[CIFSサーバでのSMBの設定](#)(105ページ)  
[SMB署名を使用したネットワークセキュリティの強化](#)(87ページ)  
[SSL/TLS経由のLDAPを使用した通信の保護](#)(97ページ)  
[従来のoplockおよびoplockリリースでのクライアントパフォーマンスの向上](#)(110ページ)  
[SMBアクセスとCIFSサービスでのIPv6の使用](#)(143ページ)  
[CIFSサーバへのグループポリシー オブジェクトの適用](#)(115ページ)  
[ドメイン コントローラ接続の管理](#)(132ページ)  
[CIFSサーバのコンピュータ アカウント パスワードの変更](#)(130ページ)  
[CIFSサーバ用のNetBIOSエイリアスの管理](#)(134ページ)  
[CIFSサーバに関するその他のタスクの管理](#)(137ページ)  
[SMBアクティビティの監視](#)(305ページ)

**関連タスク**

[CIFSサーバの停止と起動](#)(139ページ)

**関連参照情報**

[CIFSサーバを作成する前に収集する情報](#)(49ページ)

## SVM上のNISまたはLDAPネーム サービスの設定

SMBアクセスでは、NTFSセキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIXユーザへのユーザ マッピングが常に行われます。NISまたはLDAPディレクトリストアにその情報が格納されているUNIXユーザにWindowsユーザをマッピングする場合や、ネーム マッピングにLDAPを使用する場合は、CIFSのセットアップ時にこのネーム サービスを設定する必要があります。

### タスク概要

Storage Virtual Machine(SVM)は、ネーム サービスns-switchデータベースを使用してソースから指定されたネーム サービス データベースを検索する順番を決定します。LDAPまたはNISネーム サービスを使用している場合、LDAPまたはNISネーム サービスを設定する前にネーム サービス データベース設定をカスタマイズしてネーム サービス インフラと一致させる必要があります。

デフォルトでは、CIFSサーバはすべてのWindowsユーザをローカルpasswdデータベースに格納されているデフォルトUNIXユーザにマッピングします。デフォルトの設定を使用する場合、SMBアクセスに対する、NISまたはLDAP UNIXユーザおよびグループのネーム サービスまたはLDAPユーザ マッピングの設定は省略可能です。

### 手順

1. オプション: UNIXユーザ、グループ、ネットグループ情報がNISネーム サービスによって管理されている場合、NISネーム サービスを次のように設定します。
  - a. `vserver services name-service ns-switch show`コマンドを使用して、ネーム サービスの現在の順番を確認します。

#### 例

この例では、`nis`をネーム サービス ソースとして使用可能な3つのデータベース(`group`、`passwd`、`netgroup`データベース)が`files`のみをソースとして使用しています。

```
vserver services name-service ns-switch show -vserver vs1
```

| Vserver | Database | Enabled | Source Order  |
|---------|----------|---------|---------------|
| vs1     | hosts    | true    | dns,<br>files |
| vs1     | group    | true    | files         |
| vs1     | passwd   | true    | files         |
| vs1     | netgroup | true    | files         |
| vs1     | namemap  | true    | files         |

`group`および`passwd`データベースに`nis`ソースを追加する必要があります。また、オプションで`netgroup`データベースにも追加できます。

- b. `vserver services name-service ns-switch modify`コマンドを使用して、ネーム サービスns-switchデータベースを希望の順番に調整します。

最高のパフォーマンスを得るには、SVMにネーム サービスを設定する計画でない場合に、そのネーム サービス データベースに`name-service`を追加しないでください。

複数のネーム サービス データベースの設定を変更する場合、変更するそれぞれのネーム サービス データベースに対して別々にコマンドを実行する必要があります。

#### 例

この例では、`nis`および`files`が`group`および`passwd`データベースのソースとしてこの順番で設定されています。その他のネーム サービス データベースは変更されていません。

```
vserver services name-service ns-switch modify -vserver vs1 -database
group -sources nis,files
```

```
vserver services name-service ns-switch modify -vserver vs1 -database
passwd -sources nis,files
```

- c. `vserver services name-service ns-switch show` コマンドを使用して、ネーム サービスの順番が正しいことを確認します。

#### 例

```
vserver services name-service ns-switch show -vserver vs1
```

| Vserver | Database | Enabled | Source Order  |
|---------|----------|---------|---------------|
| vs1     | hosts    | true    | dns,<br>files |
| vs1     | group    | true    | nis,<br>files |
| vs1     | passwd   | true    | nis,<br>files |
| vs1     | netgroup | true    | files         |
| vs1     | namemap  | true    | files         |

- d. NISネーム サービス設定を作成します。

```
vserver services name-service nis-domain create -vserver vserver_name
-domain NIS_domain_name -servers NIS_server_IPaddress,... -active true
```

#### 例

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```

- e. NISネーム サービスが正しく設定され、有効になっていることを確認します。

```
vserver services name-service nis-domain show vserver vserver_name
```

#### 例

```
vserver services name-service nis-domain show vserver vs1
```

| Vserver | Domain      | Active | Server    |
|---------|-------------|--------|-----------|
| vs1     | example.com | true   | 10.0.0.60 |

2. オプション: LDAPネーム サービスでUNIXユーザ、グループ、ネットグループ情報またはネーム マッピングの管理を行っている場合は、『*clustered Data ONTAP ファイル アクセス管理ガイド (NFS)*』の情報をを使用してLDAPネーム サービスを設定します。

#### 関連参照情報

[ネーム サービスを設定する前に収集する情報](#) (46ページ)

#### 関連情報

[clustered Data ONTAP 8.3 ファイル アクセス管理ガイド \(NFS\)](#)

## Infinite VolumeのSMBサポートに関する情報の参照先

SMBバージョンおよびInfinite Volumeがサポートする機能の詳細については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

### 関連情報

[\*Clustered Data ONTAP 8.3 Infinite Volumes Management Guide\*](#)

## CIFSサーバの管理

---

CIFSサーバの設定が完了すると、管理タスクを実行できます。実行できる管理タスクには次のようなものがあります。CIFSサーバ オプションの設定、CIFSサーバのセキュリティ管理、SMBとSMB署名の設定、LDAP over SSL/TLSの設定、oplockの管理、IPv6 SMBアクセスの設定、CIFSサーバへのGPOの適用、ドメイン コントローラのコネクションの管理、CIFSサーバのサービスの管理など。

### 関連コンセプト

[オプションを使用したCIFSサーバのカスタマイズ](#)(71ページ)  
[CIFSサーバのセキュリティ設定の管理](#)(81ページ)  
[CIFSサーバでのSMBの設定](#)(105ページ)  
[SMB署名を使用したネットワーク セキュリティの強化](#)(87ページ)  
[SSL/TLS経由のLDAPを使用した通信の保護](#)(97ページ)  
[従来のoplockおよびoplockリリースでのクライアント パフォーマンスの向上](#)(110ページ)  
[SMBアクセスとCIFSサービスでのIPv6の使用](#)(143ページ)  
[CIFSサーバへのグループ ポリシー オブジェクトの適用](#)(115ページ)  
[ドメイン コントローラ接続の管理](#)(132ページ)  
[CIFSサーバのコンピュータ アカウント パスワードの変更](#)(130ページ)  
[CIFSサーバ用のNetBIOSエイリアスの管理](#) (134ページ)  
[CIFSサーバに関するその他のタスクの管理](#)(137ページ)  
[ローカル ユーザおよびローカル グループを使用した認証と許可](#)(216ページ)  
[ファイル ロックの管理](#)(302ページ)  
[SMBアクティビティの監視](#)(305ページ)  
[UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法の管理](#)(77ページ)

### 関連タスク

[CIFSサーバの停止と起動](#)(139ページ)  
[匿名ユーザに対するアクセス制限の設定](#)(76ページ)  
[Flex VolでのSMBファイル名の変換のための文字マッピングの設定](#)(164ページ)

## オプションを使用したCIFSサーバのカスタマイズ

オプションを使用してCIFSサーバをカスタマイズし、デフォルトのUNIXユーザなどを設定することができます。また、advanced権限レベルでは、Windowsのローカル ユーザとローカル グループやローカルWindowsユーザ認証、自動ノード リファラールやリモート コピー オフロード、SMBアクセスのエクスポート ポリシーなど、各種のオプションを有効または無効にすることができます。

### 使用できるCIFSサーバ オプション

CIFSサーバのカスタマイズ方法について検討する場合は、使用できるCIFSオプションを把握しておくくと便利です。一部のオプションは汎用的なものですが、CIFSの特定の機能を有効にして設定するためのオプションも複数あります。

以下に、admin権限レベルで使用できるCIFSサーバ オプションについて説明します。

- **SMB/CIFSセッション タイムアウト値の設定**

このオプションでは、SMB/CIFSセッションがアイドルになってから切断されるまでの時間を秒数で指定できます。アイドル セッションとは、ユーザがクライアントでファイルもディレクトリも開いていないセッションのことです。デフォルト値は900秒です。

- **デフォルトのUNIXグループの設定**

このオプションでは、CIFSサーバのデフォルトのUNIXグループの名前を指定できます。デフォルト値はありません。このオプションは、Infinite Volumeを備えたSVMのみでサポートされます。

- **デフォルトのUNIXユーザの設定**

このオプションでは、CIFSサーバで使用されるデフォルトのUNIXユーザを指定できます。Data ONTAP 8.2以降では、デフォルト ユーザ「pcuser」(UIDは65534)およびグループ「pcuser」(GIDは65534)が自動的に作成され、デフォルト ユーザが「pcuser」グループに追加されます。CIFSサーバの作成時には、「pcuser」がデフォルトのUNIXユーザとして自動的に設定されます。

- **ゲストUNIXユーザの設定**

このオプションでは、信頼されていないドメインからログインしたユーザをマッピングするUNIXユーザの名前を指定できます。これにより、信頼されていないドメインのユーザがCIFSサーバに接続できるようになります。デフォルトでは、このオプションは設定されていません(デフォルト値はありません)。このため、信頼されていないドメインのユーザはCIFSサーバへの接続を許可されません。

- **読み取り権限での実行許可の有効化と無効化**

このオプションを有効または無効にすると、たとえUNIX実行可能ビットが設定されていない場合でも、UNIXモード ビットが設定された実行可能ファイルの実行を、ファイルへの読み取り権限を持つSMBクライアントに許可するかどうかを指定できます。このオプションはデフォルトで無効になっています。

- **読み取り専用ファイルをNFSクライアントから削除する機能の有効化と無効化**

このオプションを有効または無効にすると、読み取り専用属性が設定されたファイルやフォルダの削除をNFSクライアントに許可するかどうかを指定できます。NTFSの削除では、読み取り専用属性が設定されたファイルやフォルダの削除は許可されません。UNIXの削除では読み取り専用ビットが無視され、ファイルやフォルダを削除できるかどうかは親ディレクトリの権限によって判断されます。デフォルトの設定は無効で、NTFSの削除が適用されます。

- **Windows Internet Name Service (WINS) サーバ アドレスの設定**

このオプションでは、複数のWINSサーバ アドレスをカンマで区切って指定できます。IPv4アドレスを指定する必要があります。IPv6アドレスはサポートされません。デフォルト値はありません。

以下に、advanced権限レベルで使用できるCIFSサーバ オプションについて説明します。

- **SMB 2.xの有効化と無効化**

SMB 2.0は、LIFフェイルオーバーをサポートするSMBの最小バージョンです。SMB 2.xを無効にした場合、SMB 3.0も自動的に無効になります。

このオプションは、FlexVolを備えたSVMのみでサポートされます。このオプションは、FlexVolを備えたSVMではデフォルトで有効になり、Infinite Volumeを備えたSVMではデフォルトで無効になります。

- **SMB 3.0の有効化と無効化**

SMB 3.0は、継続的可用性を備えた共有をサポートするSMBの最小バージョンです。Windows Server 2012およびWindows 8は、SMB 3.0をサポートするWindowsの最小バージョンです。

このオプションは、FlexVolを備えたSVMのみでサポートされます。このオプションは、FlexVolを備えたSVMではデフォルトで有効になり、Infinite Volumeを備えたSVMではデフォルトで無効になります。

- **ODXコピー オフロードの有効化と無効化**

ODXコピー オフロードは、対応するWindowsクライアントで自動的に使用されます。このオプションは、デフォルトでは有効になっています。



- **ODXコピー オフロードの直接コピー メカニズムの有効化と無効化**  
 直接コピー メカニズムは、コピー中のファイル変更を禁止するモードでWindowsクライアントがコピー元のファイルを開こうとした場合に、コピー オフロード処理のパフォーマンスを向上させます。デフォルトでは、直接コピー メカニズムは有効になっています。
- **自動ノード リファラルの有効化と無効化**  
 自動ノード リファラルでは、CIFS サーバはクライアントに対して、要求した共有を介してアクセスするデータのホスト ノードに対してローカルなデータLIFを自動的に参照することになります。このオプションは、Hyper-V over SMB構成では無効にする必要があります。このオプションはデフォルトで無効になっています。
- **SMBのエクスポート ポリシーの有効化と無効化**  
 デフォルトでは、SMBのエクスポート ポリシーは無効になります。
- **ジャンクション ポイントのリパース ポイントとしての使用の有効化と無効化**  
 このオプションを有効にすると、CIFSサーバはジャンクション ポイントをリパース ポイントとしてSMBクライアントに公開します。このオプションは、SMB 2.x接続またはSMB 3.0接続のみで有効です。このオプションは、デフォルトでは有効になっています。  
 このオプションは、FlexVolを備えたSVMのみでサポートされます。このオプションは、FlexVolを備えたSVMではデフォルトで有効になり、Infinite Volumeを備えたSVMではデフォルトで無効になります。
- **TCP接続ごとの最大同時処理数の設定**  
 デフォルト値は255です。
- **ローカルのWindowsユーザとグループ機能の有効化と無効化**  
 このオプションは、デフォルトでは有効になっています。
- **ローカルのWindowsユーザ認証の有効化と無効化**  
 このオプションは、デフォルトでは有効になっています。
- **VSSシャドウ コピー機能の有効化と無効化**  
 Data ONTAPでは、シャドウ コピー機能によって、Hyper-V over SMBソリューションを使用して格納されたデータのリモート バックアップを実行します。  
 このオプションは、FlexVolを備えたSVM、およびHyper-V over SMB構成のみでサポートされます。このオプションは、FlexVolを備えたSVMではデフォルトで有効になり、Infinite Volumeを備えたSVMではデフォルトで無効になります。
- **シャドウ コピーのディレクトリ階層の設定**  
 このオプションを設定すると、シャドウ コピー機能を使用するときに、シャドウ コピーを作成するディレクトリの最大階層を定義できます。  
 このオプションは、FlexVolを備えたSVM、およびHyper-V over SMB構成のみでサポートされます。このオプションは、FlexVolを備えたSVMではデフォルトで有効になり、Infinite Volumeを備えたSVMではデフォルトで無効になります。
- **マルチドメイン ネーム マッピングの検索機能の有効化と無効化**  
 有効にすると、UNIXユーザがWindowsユーザ名のドメイン部分にワイルドカード(\*)を使用してWindowsドメイン ユーザにマッピングされている場合に(\*\joeなど)、Data ONTAPはホームドメインと双方向の信頼関係が確立されたすべてのドメインで、指定したユーザを検索します。ホームドメインとは、CIFSサーバのコンピュータ アカウントが含まれるドメインです。  
 双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。このオプションを有効にして、信頼できるドメインのリストを設定すると、マルチドメイン ネーム マッピングの検索はそのリストを使用して実行されます。  
 デフォルトでは、マルチドメイン ネーム マッピングの検索は有効になります。
- **ファイル システム セクター サイズの設定**  
 このオプションでは、Data ONTAPからSMBクライアントに報告されるファイル システム セクター サイズをバイト単位で設定できます。このオプションの有効な値は、4096と512の2つです。デ

フォルト値は4096です。Windowsアプリケーションが512バイトのセクター サイズしかサポートしていない場合は、この値を512に設定する必要があります。

- **ダイナミック アクセス制御 (DAC) の有効化と無効化**

このオプションを有効にすると、監査を使用した集約型アクセス ポリシーのステージングや、グループ ポリシー オブジェクトを使用した集約型アクセス ポリシーの実装を含めて、ダイナミック アクセス制御を使用してCIFSサーバのオブジェクトを保護できます。このオプションはデフォルトでは無効になっています。

このオプションは、FlexVolを備えたSVMのみでサポートされます。

- **認証されていないセッションのアクセス制限の設定 (restrict anonymous)**

このオプションでは、認証されていないセッションに適用されるアクセス制限を指定します。制限は匿名ユーザに適用されます。デフォルトでは、匿名ユーザに対するアクセス制限はありません。

- **UNIX対応のセキュリティが設定されたボリューム (UNIXセキュリティ形式のボリューム、またはUNIX対応のセキュリティが設定されたmixedセキュリティ形式のボリューム) のNTFS ACL の表示方法**

このオプションを有効または無効にして、UNIXセキュリティ形式のファイルやフォルダのファイル セキュリティがSMBクライアントに表示される方法を指定します。有効にすると、UNIXセキュリティ形式のボリューム内のファイルやフォルダは、NTFS ACLを使用するNTFSファイル セキュリティが設定されたファイルやフォルダとしてSMBクライアントに表示されます。無効にすると、UNIXセキュリティ形式のボリュームは、ファイル セキュリティのないFATボリュームとして表示されます。デフォルトでは、ボリュームはNTFS ACLを使用するNTFSファイル セキュリティが設定されたボリュームとして表示されます。

- **SMB擬似オープン機能の有効化と無効化**

この機能を有効にすると、Data ONTAPがファイルやディレクトリの属性情報を照会する際のオープン要求とクローズ要求の方法が最適化されて、SMB 2.xおよびSMB 3.0のパフォーマンスが向上します。デフォルトでは、SMB擬似オープン機能は有効になっています。このオプションは、SMB 2.x以降を使用する接続にのみ有効です。

- **UNIX拡張の有効化と無効化**

このオプションを有効にすると、CIFSサーバでUNIX拡張が有効になります。UNIX拡張を使用すると、SMBプロトコルを介してPOSIX/UNIX形式のセキュリティを表示できます。デフォルトでは、このオプションは無効になっています。

Mac OSXクライアントなど、UNIXベースのSMBクライアントが環境内にある場合は、UNIX拡張を有効にしてください。UNIX拡張を有効にすると、CIFSサーバはPOSIX/UNIXセキュリティ情報をSMB経由でUNIXベースのクライアントに送信できるようになります。クライアントは、受け取ったセキュリティ情報をPOSIX/UNIXセキュリティに変換します。

- **短縮名を使用した検索のサポートの有効化と無効化**

このオプションを有効にすると、CIFSサーバは短縮名に対して検索を実行できます。このオプションを有効にした場合の検索では、長いファイル名に加えて8.3形式のファイル名も照合されます。このパラメータのデフォルト値はfalseです。

- **DFSの機能の自動通知のサポートの有効化と無効化**

このオプションを有効または無効にして、共有に接続しているSMB 2.xおよびSMB 3.0クライアントにCIFSサーバからDFSの機能を自動的に通知するかどうかを指定します。clustered Data ONTAPでは、SMBアクセス用のシンボリック リンクの実装でDFSリファールが使用されます。有効にすると、シンボリック リンク アクセスが有効かどうかに関係なく、CIFSサーバは常にDFSの機能を通知します。無効にすると、シンボリック リンク アクセスが有効になっている共有にクライアントが接続している場合にのみ、CIFSサーバはDFSの機能を通知します。

## 関連コンセプト

[UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法の管理](#)(77ページ)

[CIFSサーバでのSMBの設定](#)(105ページ)  
[マルチドメイン ネーム マッピング検索の設定](#)(170ページ)  
[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)  
[エクスポート ポリシーを使用したSMBアクセスの保護](#)(208ページ)  
[ローカル ユーザおよびローカル グループを使用した認証と許可](#)(216ページ)  
[Microsoftリモート コピーのパフォーマンスの向上](#)(368ページ)  
[Auto LocationでSMB自動ノード リファールを提供することでクライアントの応答時間を改善](#)  
 (373ページ)  
[Microsoft Hyper-VおよびSQL Server over SMBソリューション用のData ONTAPの設定](#)(382ページ)  
[リモートVSSによる共有ベースのバックアップ](#)(387ページ)  
[UNIXシンボリックリンクへのSMBクライアント アクセスの設定](#)(338ページ)

## 関連タスク

[CIFSサーバ オプションの設定](#)(75ページ)  
[匿名ユーザに対するアクセス制限の設定](#)(76ページ)  
[UNIXセキュリティ形式のデータに対するNTFS ACLの提供の有効化と無効化](#)(78ページ)  
[デフォルトのUNIXユーザの設定](#)(101ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vservers cifs options modify - Modify CIFS options](#)  
[clustered Data ONTAP 8.3.1 マニュアル ページ: vservers cifs options modify - Modify CIFS options](#)

## CIFSサーバ オプションの設定

CIFSサーバ オプションはStorage Virtual Machine (SVM) でのCIFSサーバの作成後に随時設定できます。

### 手順

1. 次のうち必要な操作を実行します。

| CIFSサーバオプションの設定  | 入力するコマンド                                                                                                                                                        |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| admin権限レベルで設定    | <code>vservers cifs options modify -vservers vservers_name options</code>                                                                                       |
| advanced権限レベルで設定 | a. <code>set -privilege advanced</code><br>b. <code>vservers cifs options modify -vservers vservers_name options</code><br>c. <code>set -privilege admin</code> |

`options`は、1つ以上のCIFSサーバ オプションのリストです。

CIFSサーバ オプションの設定の詳細については、`vservers cifs options modify`コマンドのマニュアル ページを参照してください。

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vservers cifs options modify - Modify CIFS options](#)

## 匿名ユーザに対するアクセス制限の設定

デフォルトでは、認証されていない匿名ユーザ (*null* ユーザとも呼ばれます) は、ネットワークの特定の情報にアクセスできます。CIFS サーバ オプションを使用して匿名ユーザに対するアクセス制限を設定できます。

### タスク概要

-restrict-anonymous CIFS サーバ オプションは、Windows の **RestrictAnonymous** レジストリ エントリに相当します。

匿名ユーザは、ネットワークの Windows ホストから、ユーザ名、ユーザの詳細、アカウント ポリシー、共有名など、特定の種類のシステム情報をリストまたは列挙できます。次の3つのうち、いずれかのアクセス制限設定を指定して、匿名ユーザのアクセスを制御することができます。

| 値                         | 説明                      |
|---------------------------|-------------------------|
| no-restriction<br>(デフォルト) | 匿名ユーザに対してアクセス制限を設定しません。 |
| no-enumeration            | 匿名ユーザに対して列挙だけを制限します。    |
| no-access                 | 匿名ユーザに対してアクセスを制限します。    |

### 手順

1. 権限レベルをadvancedに設定します。  

```
set -privilege advanced
```
2. restrict anonymous オプションを設定します。  

```
vserver cifs options modify -vserver vservice_name -restrict-anonymous {no-restriction|no-enumeration|no-access}
```
3. オプションが目的の値に設定されていることを確認します。  

```
vserver cifs options show -vserver vservice_name
```
4. admin 権限レベルに戻ります。  

```
set -privilege admin
```

### 関連参照情報

[使用できるCIFSサーバオプション](#) (71 ページ)

### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vservice cifs options modify - Modify CIFS options](#)

## UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法の管理

SMBクライアントへのNTFS ACLの提供を有効または無効にすることによって、UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法を選択できます。それぞれの設定の利点を理解して、ビジネス要件に適した方を選ぶようにしてください。

デフォルトでは、UNIXセキュリティ形式のボリュームに対するUNIXアクセス権がNTFS ACLとしてSMBクライアントに提供されます。これは次のような場合に適しています。

- Windowsの[プロパティ]ボックスの[セキュリティ]タブを使用してUNIXアクセス権の表示や編集を行う場合。  
処理がUNIXシステムで許可されていなければ、Windowsクライアントからアクセス権を変更することはできません。たとえば、所有していないファイルの所有権を変更することはできません。これは、UNIXシステムではこうした処理が許可されていないためです。この制限により、SMBクライアントは、ファイルやフォルダに対して設定されたUNIXアクセス権をバイパスできないようになっています。
- UNIXセキュリティ形式のボリュームに格納されたファイルの編集や保存に特定のWindowsアプリケーション (Microsoft Officeなど) を使用しており、Data ONTAPでの保存時にUNIXアクセス権を維持する必要がある場合。
- 使用するファイルのNTFS ACLを読み取ることを想定した特定のWindowsアプリケーションが環境にある場合。

状況に応じて、NTFS ACLとしてのUNIXアクセス権の提供を無効にすることもできます。この機能を無効にすると、UNIXセキュリティ形式のボリュームがFATボリュームとしてSMBクライアントに提供されます。UNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供するのは、次のような場合です。

- UNIXアクセス権の変更は、マウントを使用してUNIXクライアントでしか行わない場合。  
UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合、[セキュリティ]タブで操作することはできません。マッピングされたドライブは、ファイル権限がない、FATファイルシステムでフォーマットされたドライブとして表示されます。
- SMBを使用するアプリケーションでアクセスするファイルやフォルダにNTFS ACLを設定しており、データがUNIXセキュリティ形式のボリュームにあると失敗する可能性がある場合。  
Data ONTAPではボリュームがFATとして報告され、アプリケーションでACLの変更は試行されません。

### 関連コンセプト

[セキュリティ形式がデータ アクセスに与える影響](#) (20ページ)

### 関連タスク

[FlexVolでのセキュリティ形式の設定](#) (149ページ)

[qtreeでのセキュリティ形式の設定](#) (149ページ)

### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver cifs options modify - Modify CIFS options](#)

## UNIXセキュリティ形式のデータに対するNTFS ACLの提供の有効化と無効化

UNIXセキュリティ形式のデータ (UNIXセキュリティ形式のボリュームとUNIX対応のセキュリティを使用するmixedセキュリティ形式のボリューム) に対するNTFS ACLのSMBクライアントへの提供を有効または無効にできます。

### タスク概要

このオプションを有効にすると、UNIX対応のセキュリティ形式を使用するボリュームのファイルおよびフォルダがSMBクライアントにNTFS ACLを通じて提供されます。このオプションを無効にした場合は、ボリュームがSMBクライアントにFATボリュームとして提供されます。デフォルトでは、NTFS ACLがSMBクライアントに提供されます。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. UNIX NTFS ACLオプションを設定します。

```
vserver cifs options modify -vserver vservice_name -is-unix-nt-acl-enabled {true|false}
```

3. オプションが目的の値に設定されていることを確認します。

```
vserver cifs options show -vserver vservice_name
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vservice cifs options modify - Modify CIFS options](#)

## Data ONTAPによるUNIXアクセス権の維持方法

UNIXアクセス権が現在設定されているFlexVol内のファイルがWindowsアプリケーションによって編集および保存されても、Data ONTAPではUNIXアクセス権が維持されます。

Windowsクライアントのアプリケーションがファイルを編集して保存するとき、アプリケーションはファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成してセキュリティプロパティをこのファイルに適用し、元のファイル名を付けます。

Windowsクライアントがセキュリティプロパティを照会すると、UNIXアクセス権を正確に反映した構築済みACLが渡されます。このACLの目的は、Windowsアプリケーションによってファイルが更新された際にファイルのUNIXアクセス権を維持し、変更後のファイルのUNIXアクセス権が同じになるようにすることです。Data ONTAPがこの構築済みACLを使用してNTFS ACLを設定することはありません。

## Windowsの[セキュリティ]タブを使用したUNIXアクセス権の管理方法

FlexVolを備えたStorage Virtual Machine (SVM) でmixedセキュリティ形式のボリュームまたはqtree内にあるファイルまたはフォルダのUNIXアクセス権を操作する場合は、Windowsクライアントの[セキュリティ]タブを使用します。または、Windows ACLを照会または設定できるアプリケーションを使用できます。

- UNIXアクセス権の変更

Windowsの[セキュリティ]タブで、mixedセキュリティ形式のボリュームまたはqtreeのUNIXアクセス権を表示および変更することができます。Windowsのメイン[セキュリティ]タブを使用して

UNIXアクセス権を変更する場合は、変更を行う前にまず、編集する既存のACEを削除する必要があります(これによりモードビットが0に設定されます)。また、高度なエディタを使用してアクセス権を変更することもできます。

モードのアクセス権を使用している場合は、リストされたUID、GID、およびその他(コンピュータにアカウントを持つその他すべてのユーザ)のモードアクセス権を直接変更できます。たとえば、表示されたUIDにr-xのアクセス権が設定されている場合、このUIDのアクセス権をrwxに変更できます。

- UNIXアクセス権からNTFSアクセス権への変更

Windowsの[セキュリティ]タブを使用して、ファイルおよびフォルダがUNIX対応のセキュリティ形式で設定されているmixed型セキュリティ形式のボリュームまたはqtree上の場合であれば、UNIXのセキュリティオブジェクトをWindowsのセキュリティオブジェクトで置き換えることができます。

その場合は、適切なWindowsのユーザおよびグループのオブジェクトで置き換える前に、リストされているUNIXアクセス権のすべてのエントリをまず削除する必要があります。次に、WindowsのユーザおよびグループのオブジェクトにNTFS-based ACLを設定します。すべてのUNIXセキュリティオブジェクトを削除し、Windowsのユーザおよびグループのみをmixedセキュリティ形式のボリュームまたはqtree上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式がUNIXからNTFSへ変換されます。

フォルダへのアクセス権を変更する際には、Windowsのデフォルトの動作により、フォルダの配下のすべてのフォルダとファイルにもアクセス権の変更が反映されます。したがって、セキュリティスタイルの変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

## CIFSサーバ オプションを使用してclustered Data ONTAPでDFSの自動通知を制御する方法

共有に接続するSMBクライアントに対してDFS対応を通知する方法を制御するCIFSサーバ オプションが追加されています。clustered Data ONTAPでは、クライアントがSMB経由でシンボリックリンクにアクセスするときにDFSリファールを使用するため、このオプションを無効または有効にしたときの影響を理解しておく必要があります。

clustered Data ONTAP 8.2～8.2.2では、Storage Virtual Machine(SVM)上のCIFSサーバは、DFSに対応していることを常にSMBクライアントに通知します。ただし、CIFSサーバはDFSに対応していることを常に通知しますが、SMBのシンボリックリンク アクセスは、共有パラメータを設定することによって共有ごとに管理されます。共有パラメータを使用すると、SMBのシンボリックリンクアクセスを次の3つのアクセス レベルのいずれかに設定できます。

- 読み取り / 書き込みアクセスに対して有効
- 読み取り専用アクセスに対して有効
- 無効。このパラメータの値を設定してシンボリックリンクを非表示にするか、パラメータをnull(「」)に設定

8.2リリース ファミリーのData ONTAP 8.2.3以降およびData ONTAP 8.3以降では、DFSに対応していることをCIFSサーバがSMBクライアントに自動通知するかどうかは、CIFSサーバ オプションで指定します。デフォルトでは、このオプションは有効になっており、CIFSサーバはDFSに対応していることを常にSMBクライアントに(たとえシンボリックリンクへのアクセスが無効になっている共有に接続する場合でも)通知します。シンボリックリンクへのアクセスが有効になっている共有にクライアントが接続する場合にのみ、DFSに対応していることをCIFSサーバがクライアントに通知するようにするには、このオプションを無効にします。

このオプションを無効にすると次のような影響があることに留意してください。

- シンボリックリンクの共有設定は変わりません。



- シンボリック リンク アクセス(読み取り / 書き込みアクセスまたは読み取り専用アクセス)を許可するように共有パラメータが設定されている場合、CIFSサーバは、その共有に接続するクライアントにDFS対応を通知します。

シンボリック リンクへのクライアントの接続とアクセスは中断せずに続行されます。

- シンボリック リンク アクセスを許可しないように共有パラメータが設定されている場合(アクセスを無効にしているか共有パラメータの値がnullの場合)、CIFSサーバは、その共有に接続するクライアントにDFS対応を通知しません。

クライアントは、CIFSサーバがDFSに対応しているというキャッシュされた情報を保持しており、CIFSサーバはそのことを通知しなくなるので、シンボリック リンク アクセスが無効になっている共有に接続されたクライアントは、CIFSサーバ オプションが無効になったあとでそれらの共有にアクセスできなくなることがあります。オプションが無効になったあとで、それらの共有に接続されたクライアントを再起動し、キャッシュされた情報を消去する必要があります。

これらの変更はSMB 1.0の接続には適用されません。

## CIFSサーバによるDFS対応の自動通知の管理

CIFSサーバ オプションを設定して、CIFSサーバが共有に接続するSMB 2.xおよびSMB 3.0クライアントに自動的にDFS対応を通知するかどうかを決定できます。DFS対応を通知する共有に接続しないアプリケーションの場合は、自動通知を無効にすることができます。

### タスク概要

clustered Data ONTAPでは、SMBアクセス用のシンボリック リンクの実装でDFSリファールが使用されます。このオプションを有効または無効にする場合は、次の点に注意する必要があります。

- 自動DFS通知を有効にすると、共有でシンボリック リンクによるCIFSへのアクセスが有効かどうかに関わらず、CIFSサーバはその共有に接続するSMB 2.xおよびSMB 3.0クライアントに常にDFS対応を通知します。  
これがデフォルト設定です。
- 自動DFS通知を無効にすると、CIFSサーバはクライアントがシンボリック リンク アクセス(読み取り / 書き込みアクセスまたは読み取り専用アクセス)が有効になっている共有に接続する場合にのみ、SMB 2.xおよびSMB 3.0クライアントにDFS対応を通知します。シンボリック リンク アクセスが無効になっている共有に接続するクライアントには、DFS対応を通知しません。

シンボリック リンク アクセスが無効になっている共有に接続しているクライアントは、CIFSサーバ オプションが無効になるとその共有にアクセスできなくなる可能性があります。これは、クライアントがCIFSサーバがDFS対応であるという情報をキャッシュしているにもかかわらず、サーバがDFSに対応していることを通知しなくなったためです。その結果、SMB共有への再接続が失敗します。これには、次の2つの対応方法があります。

- オプションを無効にする前に、すべての共有で読み取り / 書き込みまたは読み取り専用アクセスのどちらかを許可するように共有設定を変更します。
- シンボリック リンク アクセスが無効になっている共有の設定を変更できない場合は、オプションを無効にしたあとで、共有に接続していて影響を受けたクライアントをすべてリブートしてキャッシュ情報をクリアします。

### 手順

- 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- DFSリファール オプションを設定します。

```
vserver cifs options modify -vserver vserver_name -is-advertise-dfs-enabled {true|false}
```



3. オプションが目的の値に設定されていることを確認します。

```
vserver cifs options show -vserver vserver_name
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

## CIFSサーバのセキュリティ設定の管理

CIFSサーバのセキュリティ設定は、ビジネス要件に合わせてカスタマイズできます。Kerberosセキュリティ設定を変更したり、受信SMBトラフィックにSMB署名を要求するかどうか、LDAP over SSL/TLSを使用するかどうか、Kerberos通信用のAES暗号化タイプを有効にするかどうか、共有へのアクセスにSMB暗号化を要求するかどうか、ローカル ユーザに複雑なパスワードを要求するかどうかを設定したりできます。また、認証セキュリティの最低レベルも設定できます。

### SVMディザスタリカバリ構成でのCIFSサーバセキュリティ設定に関する重要な考慮事項

IDが保存されない(SnapMirrorの設定で-identity-preserveオプションをfalseに設定)ディザスタリカバリ先として設定するStorage Virtual Machine(SVM)を作成する前に、デスティネーションSVM上でのCIFSサーバのセキュリティ設定の管理方法に関する重要な考慮事項を理解しておく必要があります。

デフォルト以外のCIFSサーバセキュリティ設定はデスティネーションにレプリケーションされません。デスティネーションSVM上にCIFSサーバを作成した場合、すべてのCIFSサーバセキュリティ設定はデフォルト値に設定されます。SVMのディザスタリカバリ先を初期化、更新、再同期した場合、ソース上のCIFSサーバのセキュリティ設定はデスティネーションにレプリケーションされません。

ソースSVM上でCIFSサーバセキュリティ設定をデフォルト以外にしている場合、デスティネーションが読み書き可能になったあと(SnapMirror関係が解除されたあと)にデスティネーションSVM上で手動で同じ設定を行う必要があります。

### CIFSサーバのセキュリティ設定に関する情報の表示

Storage Virtual Machine(SVM)上のCIFSサーバのセキュリティ設定に関する情報を表示できます。この情報は、セキュリティ設定が適切かどうかを確認するときに役立ちます。

#### タスク概要

表示されるセキュリティ設定は、そのオブジェクトのデフォルト値か、Data ONTAP CLIまたはActive Directory Group Policy Object(GPO;グループ ポリシー オブジェクト)を使用して設定されたデフォルト以外の値です。

#### 手順

1. 次のいずれかを実行します。

| 表示する情報               | 入力するコマンド                                                                                                                    |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 指定したSVMのすべてのセキュリティ設定 | <code>vserver cifs security show -vserver vserver_name</code>                                                               |
| SVMの特定のセキュリティ設定      | <code>vserver cifs security show -vserver vserver_name -fields [fieldname,...]</code><br>-fields ?と入力すると、使用できるフィールドを確認できます。 |

**例**

次の例では、SVM vs1のすべてのセキュリティ設定を表示します。

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
```

次の例では、SVM vs1のKerberosのクロック スキューを表示します。

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-clock-skew

vserver kerberos-clock-skew
-----
vs1      5
```

**関連タスク**

[GPO設定に関する情報の表示](#) (122ページ)

**ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化**

パスワードの複雑さの要件はデフォルトで有効になっており、これによってStorage Virtual Machine (SVM) 上のローカルSMBユーザに対するセキュリティを強化できます。この要件の有効と無効はいつでも切り替えることができます。

**開始する前に**

CIFSサーバでローカル ユーザとローカル グループおよびローカル ユーザ認証が有効になっている必要があります。

**手順**

1. 次のいずれかを実行します。

| ローカルSMBユーザに対するパスワードの複雑さの要件の設定 | 入力するコマンド                                                                                               |
|-------------------------------|--------------------------------------------------------------------------------------------------------|
| 有効                            | <code>vserver cifs security modify -vserver vserver_name -is-password-complexity-required true</code>  |
| 無効                            | <code>vserver cifs security modify -vserver vserver_name -is-password-complexity-required false</code> |

2. パスワードの複雑さの要件についてのセキュリティ設定を確認します。

```
vserver cifs security show -vserver vserver_name
```

例

次の例では、SVM vs1でローカルSMBユーザに対するパスワードの複雑さの要件を有効にしています。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-complexity-required
vserver is-password-complexity-required
-----
vs1      true
```

関連コンセプト

- [ローカル ユーザおよびローカル グループを使用した認証と許可](#)(216ページ)
- [ローカル ユーザのパスワードの要件](#)(222ページ)

関連タスク

- [CIFSサーバのセキュリティ設定に関する情報の表示](#)(81ページ)
- [ローカル ユーザのアカウント パスワードの変更](#)(229ページ)

CIFSサーバのKerberosセキュリティ設定の変更

対象となる設定には、Kerberosクロック スキューの許容最大時間やKerberosチケットの有効期間、チケットを更新できる最長有効期間(日数)など、CIFSサーバのKerberosセキュリティ設定を変更できます。

タスク概要

vserver cifs security modifyコマンドによるCIFSサーバのKerberos設定の変更では、-vserverパラメータで指定した単一のStorage Virtual Machine(SVM)の設定のみを変更できます。Active DirectoryのGroup Policy Object(GPO;グループ ポリシー オブジェクト)を使用すると、同一のActive Directoryドメインに属するクラスタ上のSVMすべてについて、Kerberosセキュリティ設定を集中管理できます。

手順

1. 次の操作を1つ以上実行します。

| 状況                            | コマンド                                                                                                                    |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Kerberosクロック スキューの許容最大時間を分で指定 | <b>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</b><br><br>デフォルトの設定は5分です。 |
| Kerberosチケットの有効期間を時間で指定       | <b>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</b><br><br>デフォルトの設定は10時間です。 |
| チケットを更新できる最長有効期間(日数)を指定       | <b>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</b><br><br>デフォルトの設定は7日です。     |

| 状況                                                   | コマンド                                                                                                                               |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| KDCのソケットのタイムアウトを指定します。この時間を過ぎるとすべてのKDCが到達不能とマークされます。 | <b>vserver cifs security modify -vserver <i>vserver_name</i> -kerberos-kdc-timeout <i>integer_in_seconds</i></b><br>デフォルトの設定は3秒です。 |

2. 次のコマンドを実行し、Kerberosセキュリティ設定を確認します。

```
vserver cifs security show -vserver vserver_name
```

#### 例

次の例では、SVM vs1のKerberosセキュリティ設定を変更し、Kerberos Clock Skewを3分に設定し、Kerberos Ticket Ageを8時間に設定しています。

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew 3
-k Kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 3 minutes
Kerberos Ticket Age: 8 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
```

#### 関連コンセプト

[Kerberos認証](#) (22ページ)

[AES暗号化によるKerberosベースの通信の強固なセキュリティ設定](#) (85ページ)

[サポートされるGPO](#) (116ページ)

[CIFSサーバへのグループポリシー オブジェクトの適用](#) (115ページ)

#### 関連タスク

[CIFSサーバのセキュリティ設定に関する情報の表示](#) (81ページ)

## CIFSサーバの最低限の認証セキュリティレベルの設定

業務に求められるSMBアクセスのセキュリティ要件を満たすために、CIFSサーバの最低限のセキュリティレベル (*LMCompatibilityLevel*とも呼ばれます) をCIFSサーバ上に設定できます。この最低限のセキュリティレベルは、CIFSサーバによって許可されるSMBクライアントからのセキュリティトークンの最低限のレベルです。

#### タスク概要

最低限の認証セキュリティレベルをサポートされている4つのセキュリティレベルのうちの1つに設定することができます。

| 値                          | 説明                                                        |
|----------------------------|-----------------------------------------------------------|
| lm-ntlm-ntlmv2-krb (デフォルト) | SVMは、LM、NTLM、NTLMv2、Kerberos認証セキュリティを許可します。               |
| ntlm-ntlmv2-krb            | SVMは、NTLM、NTLMv2、Kerberos認証セキュリティを許可します。SVMはLM認証を拒否します。   |
| ntlmv2-krb                 | SVMは、NTLMv2とKerberos認証セキュリティを許可します。SVMはLMとNTLM認証を拒否します。   |
| krb                        | SVMは、Kerberos認証セキュリティのみを許可します。SVMはLM、NTLM、NTLMv2認証を拒否します。 |

#### 手順

1. 最低限の認証セキュリティレベルを設定します。

```
vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}
```

2. 認証セキュリティレベルが目的のレベルに設定されていることを確認します。

```
vserver cifs security show -vserver vserver_name
```

#### 関連コンセプト

[認証によってSMBアクセス セキュリティを確保する仕組み](#)(22ページ)

#### 関連タスク

[Kerberosベースの通信用のAES暗号化の有効化と無効化](#)(86ページ)

## AES暗号化によるKerberosベースの通信の強固なセキュリティ設定

Kerberosベースの通信による最も強固なセキュリティを実現するために、AES-256暗号化とAES-128暗号化をCIFSサーバで有効にすることができます。デフォルトでは、Storage Virtual Machine (SVM) でのCIFSサーバの作成時にAES暗号化は無効になっています。AES暗号化が提供する強固なセキュリティを活用するには、AES暗号化を有効にする必要があります。

CIFSのKerberos関連の通信は、SVMでCIFSサーバを作成する際や、SMBセッションの設定フェーズで使用されます。CIFSサーバはKerberos通信で次の暗号化タイプをサポートしています。

- RC4-HMAC
- DES
- AES 128
- AES 256

Kerberos通信で最高のセキュリティを持つ暗号化タイプを使用する場合は、SVMのKerberos通信でAES暗号化を有効にする必要があります。

CIFSサーバを作成すると、ドメイン コントローラによってActive Directoryにコンピュータ マシン アカウントが作成されます。この時点で、KDCは特定のマシン アカウントの暗号化機能を認識するようになっています。これ以降は、認証の際にクライアントがサーバに提示するサービス チケットを暗号化するために特定の暗号化タイプが選択されます。

#### 関連コンセプト

[Kerberos認証](#)(22ページ)

## 関連タスク

[CIFSサーバのKerberosセキュリティ設定の変更](#) (83ページ)

## Kerberosベースの通信用のAES暗号化の有効化と無効化

Kerberosベースの通信で最大限のセキュリティを確保するには、CIFSサーバでAES-256およびAES-128暗号化を有効にします。CIFSサーバでActive Directory (AD) KDCとのKerberosベースの通信にAES暗号化タイプを選択したくない場合は、AES暗号化を無効にすることができます。デフォルトでは、AES暗号化は無効になっています。

## タスク概要

セキュリティを強化するため、Storage Virtual Machine (SVM) はAESセキュリティオプションが変更されるたびに、AD内のマシン アカウントのパスワードを変更します。パスワードの変更には、マシン アカウントが所属する組織単位 (OU) の管理ADクレデンシャルが必要になることがあります。

IDが保持されないディザスタリカバリ デスティネーションとしてSVMが設定されている場合 (SnapMirror構成で `-identity-preserve` オプションが `false` に設定されている場合)、CIFSサーバのデフォルト以外のセキュリティ設定はデスティネーションにレプリケートされません。ソース SVMでAES暗号化を有効にしている場合は、デスティネーションが読み取り / 書き込み可能になったあとで (SnapMirror関係が解除されたあとで)、デスティネーションSVMでAES暗号化を手動で有効にする必要があります。

## 手順

1. 次のいずれかを実行します。

| Kerberos通信のAES暗号化<br>タイプの設定 | 入力するコマンド                                                                                             |
|-----------------------------|------------------------------------------------------------------------------------------------------|
| 有効                          | <code>vserver cifs security modify -vserver<br/>vserver_name -is-aes-encryption-enabled true</code>  |
| 無効                          | <code>vserver cifs security modify -vserver<br/>vserver_name -is-aes-encryption-enabled false</code> |

2. AES暗号化が設定どおり有効または無効になっていることを確認します。

```
vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled
```

`is-aes-encryption-enabled` フィールドに、AES暗号化が有効になっている場合は `true` が、無効になっている場合は `false` が表示されます。

## 例

次の例では、SVM vs1のCIFSサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-encryption-enabled
vserver  is-aes-encryption-enabled
-----
vs1      true
```

次の例では、SVM vs2のCIFSサーバでAES暗号化タイプを有効にします。管理者は、CIFSサーバが所属するOUの管理ADクレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes-encryption-enabled true

Info: In order to enable CIFS AES encryption, the password for the CIFS
```

```

server
machine account must be reset. Enter the username and password for the
CIFS domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled
vserver  is-aes-encryption-enabled
-----
vs2      true

```

## SMB署名を使用したネットワーク セキュリティの強化

SMB署名は、リプレイ アタックを防止することで、CIFSサーバとクライアント間のネットワークトラフィックが危険にさらされることのないようにします。デフォルトでは、クライアントから要求されたときにSMB署名がサポートされます。ストレージ管理者は、必要に応じて、CIFSサーバでSMB署名を必須にするように設定することができます。

### SMB署名ポリシーがCIFSサーバとの通信に与える影響

CIFSサーバのSMB署名セキュリティ設定に加えて、クライアントとSVMのCIFSサーバ間の通信のデジタル署名を制御するWindowsクライアント上のSMB署名ポリシーが2つあります。ビジネス要件に合わせた設定を行うことができます。

クライアントSMBポリシーは、Microsoft Management Console (MMC; Microsoft 管理コンソール) または Active Directory の GPO を使用して設定した Windows ローカル セキュリティ ポリシー 設定で制御されます。クライアントのSMB署名とセキュリティ問題の詳細については、Microsoft Windows のマニュアルを参照してください。

ここでは、Microsoft クライアントの2つのSMB署名ポリシーについて説明します。

- Microsoft network client: Digitally sign communications (if server agrees)**  
 この設定はクライアントのSMB署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定をクライアントで無効にすると、クライアントのCIFSサーバとの通信は、CIFSサーバ上のSMB署名の設定によって異なります。
- Microsoft network client: Digitally sign communications (always)**  
 この設定は、クライアントがサーバとの通信にSMB署名を必要とするかどうかを制御します。この設定はデフォルトでは無効になっています。この設定がクライアント上で無効である場合、SMB署名の動作は、「Microsoft network client: Digitally sign communications (if server agrees)」ポリシー設定とCIFSサーバ上の設定に基づきます。

**注:** ご使用の環境に、SMB署名を必要とするように設定されたWindowsクライアントが含まれる場合、CIFSサーバ上のSMB署名を有効にする必要があります。有効にしないと、CIFSサーバはこれらのシステムにデータを提供できません。

クライアントとCIFSサーバのSMB署名設定の有効な結果は、SMBセッションでSMB 1.0が使用されるかSMB 2.x以降が使用されるかによって異なります。

次の表に、セッションでSMB 1.0が使用される場合の有効なSMB署名の動作を示します。

| クライアント            | Data ONTAP—署名が不要 | Data ONTAP—署名が必要 |
|-------------------|------------------|------------------|
| 署名が無効になっており、不要である | 署名されない           | 署名される            |
| 署名が有効になっており、不要である | 署名されない           | 署名される            |

| クライアント            | Data ONTAP—署名<br>が不要 | Data ONTAP—署名が<br>必要 |
|-------------------|----------------------|----------------------|
| 署名が無効になっており、必要である | 署名される                | 署名される                |
| 署名が有効になっており、必要である | 署名される                | 署名される                |

**注:**

古いバージョンのWindowsのSMB 1クライアントや一部のWindows以外のSMB 1クライアントでは、署名がクライアントでは無効になっていてCIFSサーバでは必要な場合、接続に失敗することがあります。

次の表に、セッションでSMB 2.xまたはSMB 3.0が使用される場合の有効なSMB署名の動作を示します。

注: SMB 2.xクライアントおよびSMB 3.0クライアントでは、SMB署名は常に有効になります。無効にはできません。

| クライアント   | Data ONTAP—署名<br>が不要 | Data ONTAP—署名が<br>必要 |
|----------|----------------------|----------------------|
| 署名が不要である | 署名されない               | 署名される                |
| 署名が必要である | 署名される                | 署名される                |

次の表に、MicrosoftクライアントおよびサーバのSMB署名のデフォルト動作を示します。

| プロトコル   | ハッシュア<br>ルゴリズム  | 有効と無<br>効の切り替<br>えが可能 | 必須と不要<br>の切り替え<br>が可能 | クライ<br>アントのデ<br>フォルト | サーバの<br>デフォルト | DCのデフ<br>ォルト |
|---------|-----------------|-----------------------|-----------------------|----------------------|---------------|--------------|
| SMB 1.0 | MD5             | ○                     | ○                     | 有効(不<br>要)           | 無効(不<br>要)    | 必須           |
| SMB 2.x | HMAC<br>SHA-256 | ×                     | ○                     | 不要                   | 不要            | 必須           |
| SMB 3.0 | AES-<br>CMAC    | ×                     | ○                     | 不要                   | 不要            | 必須           |

注: Microsoftでは、「**Digitally sign communications (if client agrees)**」または「**Digitally sign communications (if server agrees)**」グループ ポリシー設定の使用を推奨していません。また、Microsoftでは、「**EnableSecuritySignature**」レジストリ設定の使用も推奨していません。これらのオプションは、SMB 1の動作にのみ影響を与え、「**Digitally sign communications (always)**」グループ ポリシー設定または「**RequireSecuritySignature**」レジストリ設定で置き換えることができます。詳細については、Microsoftのブログ「[The Basics of SMB Signing \(covering both SMB1 and SMB2\)](#)」を参照してください。

**SMB署名のパフォーマンスへの影響**

SMBセッションでSMB署名を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが著しく低下し、クライアントとサーバの両者にその影響が及びます。これは、CIFSサーバなどのStorage Virtual Machine (SVM) で動作するクラスタ上のノードが影響を受けることを意味します。

パフォーマンスの低下は、CPU使用率の増加としてクライアントとサーバの両方に表れます。ネットワークのトラフィック量は変わりません。



ネットワークとSVMの実装方法に応じてSMB署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

ほとんどのWindowsクライアントは、サーバでSMB署名が有効になっている場合は、SMB署名をデフォルトでネゴシエートします。Windowsクライアントの一部でSMB保護が必要で、SMB署名がパフォーマンスの問題を引き起こしている場合は、リプレイアタックからの保護を必要としないWindowsクライアントに対してSMB署名を無効にすることができます。WindowsクライアントでのSMB署名の無効化については、Microsoft Windowsのマニュアルを参照してください。

### SMB署名の設定に関する推奨事項

SMBクライアントとCIFSサーバの間のSMB署名の動作は、セキュリティ要件に応じて設定することができます。CIFSサーバでのSMB署名の設定は、セキュリティ要件の内容によって異なります。

SMB署名は、クライアントとCIFSサーバのどちらでも設定できます。SMB署名を設定する際の推奨事項を次に示します。

| 状況または条件                                               | 推奨事項                                                                                 |
|-------------------------------------------------------|--------------------------------------------------------------------------------------|
| クライアントとサーバの間の通信のセキュリティを強化する                           | クライアントに対して <b>[Require Option (Sign always)]</b> セキュリティ設定を有効にして、クライアントでSMB署名を必須にします。 |
| 特定のStorage Virtual Machine (SVM) へのすべてのSMBトラフィックに署名する | セキュリティ設定でSMB署名を必須にするように設定して、CIFSサーバでSMB署名を必須にします。                                    |

Windowsクライアントのセキュリティ設定の詳細については、Microsoftのドキュメントを参照してください。

### 関連タスク

[受信SMBトラフィックのSMB署名要求の有効化と無効化](#)

### 複数のデータLIFが設定されている場合の考慮事項

Storage Virtual Machine (SVM) で複数のデータLIFが設定されている場合に、CIFSサーバでSMB署名の要求を有効または無効にするときは、一定の考慮事項があります。

CIFSサーバを設定する際に、複数のデータLIFが設定されていることがあります。その場合、DNSサーバには、CIFSサーバに対するAレコードエントリが複数存在し、CIFSサーバホスト名はすべてのエントリで同じですが、IPアドレスは各エントリで異なります。たとえば、2つのデータLIFが設定されているCIFSサーバには、次のようなDNS Aレコードエントリがあります。

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

通常の動作では、SMB署名の要求の設定を変更すると、クライアントからの新しい接続だけがSMB署名の設定変更の影響を受けます。ただし、この動作には例外があります。共有への既存の接続がクライアントにあると、設定の変更後、クライアントは元の接続を維持しながら同じ共有への新しい接続を作成します。この場合、新規と既存のSMB接続の両方で新しいSMB署名の設定が適用されます。

次の例を考えてみましょう。

- Client1は、パス0:\を使用して、SMB署名を使わずに共有に接続しています。
- ストレージ管理者が、SMB署名を要求するようにCIFSサーバの設定を変更したとします。
- Client1は、パスS:\を使用して(パス0:\を使用した接続は維持したまま)、SMB署名を使って同じ共有に接続します。

4. 結果として、0:\ドライブとS:\ドライブの両方でデータ アクセス時にSMB署名が使用されます。

### 受信SMBトラフィックのSMB署名要求の有効化と無効化

SMBメッセージへのクライアントによる署名を強制するには、SMB署名要求を有効にします。有効にすると、Data ONTAPは有効な署名のあるSMBメッセージのみを受け入れます。SMB署名を許可するが要求しない場合は、SMB署名要求を無効にできます。

#### タスク概要

デフォルトでは、SMB署名要求は無効になっています。SMB署名要求は随時有効または無効にできます。

注: 次の状況では、SMB署名はデフォルトで無効になりません。

1. SMB署名要求が有効になっており、クラスタがSMB署名をサポートしていないバージョンのData ONTAPにリポートされた。
2. その後、クラスタがSMB署名をサポートするバージョンのData ONTAPにアップグレードされた。  
このような場合は、サポートされているバージョンのData ONTAPで最初に行われたSMB署名の設定が、リポートとその後のアップグレードを通して維持されます。

Storage Virtual Machine (SVM) ディザスタリカバリ関係をセットアップするときに、snapmirror createコマンドの-identity-preserveオプションに指定する値によって、デスティネーションSVMでレプリケートされる設定の詳細が決まります。

-identity-preserveオプションをtrue (ID保持) に設定すると、SMB署名のセキュリティ設定がデスティネーションにレプリケートされます。

-identity-preserveオプションをfalse (非ID保持) に設定すると、SMB署名のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションではCIFSサーバのセキュリティ設定がデフォルト値に設定されます。ソースSVMでSMB署名要求を有効にしている場合は、デスティネーションでSMB署名要求を手動で有効にする必要があります。

#### 手順

1. 次のいずれかを実行します。

| SMB署名要求の設定 | 入力するコマンド                                                                                   |
|------------|--------------------------------------------------------------------------------------------|
| 有効         | <code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>  |
| 無効         | <code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code> |

2. 次のコマンドの出力で、Is Signing Requiredフィールドの値が目的の値に設定されているかどうかを判断して、SMB署名要求が有効または無効になっていることを確認します。

```
vserver cifs security show -vserver vserver_name -fields is-signing-required
```

#### 例

次の例では、Storage Virtual Machine (SVM、旧Vserver) vs1のSMB署名要求を有効にしています。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true
cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
```

```
required
vserver  is-signing-required
-----
vs1      true
```

## SMBセッションが署名されているかどうかの確認

CIFSサーバで接続中のSMBセッションに関する情報を表示できます。この情報を使用して、SMBセッションが署名されているかどうかを確認できます。これは、必要なセキュリティ設定を使用してSMBクライアントセッションが接続されているかどうかを確認する場合に役立ちます。

### 手順

1. 次のいずれかを実行します。

| 表示する情報                                             | 入力するコマンド                                                                                           |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------|
| 指定したStorage Virtual Machine (SVM) 上の署名されたすべてのセッション | <b>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed true</b>              |
| SVM上の指定したセッションIDを持つ署名されたセッションの詳細                   | <b>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</b> |

### 例

次のコマンドを実行すると、SVM vs1上の署名されたセッションに関するセッション情報が表示されます。デフォルトの要約出力には、「Is Session Signed」出力フィールドは表示されません。

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID         ID      Workstation      Windows User      Open      Idle
-----
3151272279 1       10.1.1.1         DOMAIN\joe        2         23s
```

次のコマンドを実行すると、セッションID 2のSMBセッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node:      node1
Vserver:   vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User:   pcuser
Open Shares: 1
Open Files:  1
Open Other:  0
Connected Time: 10m 43s
Idle Time:    1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## 関連タスク

[受信SMBトラフィックのSMB署名要求の有効化と無効化](#)

[SMB署名済みセッションの統計の監視](#) (92ページ)

## SMB署名済みセッションの統計の監視

SMBセッションの統計を監視し、確立されたセッションのうち、署名されたセッションと署名されていないセッションを区別できます。

### タスク概要

advanced権限レベルでstatisticsコマンドを使用すると、signed\_sessionsカウンタで署名SMBセッションの数を監視できます。signed\_sessionsカウンタでは、次の統計オブジェクトを利用できます。

- **cifs**。このオブジェクトを使用すると、すべてのSMBセッションについてSMB署名を監視できます。
- **smb1**。このオブジェクトを使用すると、SMB 1.0セッションのSMB署名を監視できます。
- **smb2**。このオブジェクトを使用すると、SMB 2.xセッションとSMB 3.0セッションのSMB署名を監視できます。

注: SMB 3.0の統計は、smb2オブジェクトを使用して得られる出力に含まれます。

署名セッションの数をセッションの全体数と比較する場合は、signed\_sessionsカウンタの出力とestablished\_sessionsカウンタの出力を比較します。

データを取得して表示するには、統計のサンプルの収集を起動する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しなければ、以前のクエリとの比較に使用できる更新されたデータを入手できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

statisticsコマンドの詳細については、『*clustered Data ONTAP システム アドミニストレーションガイド(クラスタ管理)*』を参照してください。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のコマンドを実行し、データの収集を起動します。

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

このコマンドで-sample-idパラメータを指定しないと、サンプル識別子が生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。-sample-idの値はテキスト文字列です。同じCLIセッションでこのコマンドを実行し、-sample-idパラメータを指定しない場合、前回のデフォルト サンプルは上書きされます。

オプションで、統計情報を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

3. オプション: サンプルのデータ収集を停止するには、statistics stopコマンドを使用します。
4. 次のコマンドによりSMB署名統計を表示します。

| 表示する情報                  | コマンド                                                                                                                           |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 署名されたセッション              | <code>show -sample-id <i>sample_ID</i> -counter signed_sessions node_name [-node <i>node_name</i>]</code>                      |
| 署名されたセッションおよび確立されたセッション | <code>show -sample-id <i>sample_ID</i> -counter signed_sessions established_sessions node_name [-node <i>node_name</i>]</code> |

単一のノードの情報のみを表示する場合は、オプションの `-node` パラメータを指定します。

5. admin権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次の例では、「vs1」というStorage Virtual Machine (SVM) について、SMB 2.xとSMB 3.0のそれぞれの署名統計情報を監視する方法を示します。

次のコマンドは、advanced権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use
them only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object smb2 -sample-id
smbsigning_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbsigning_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id:
smbsigning_sample
```

次のコマンドでは、ノードが署名、確立した各SMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1
```

| Counter              | Value |
|----------------------|-------|
| -----                | ----- |
| established_sessions | 0     |
| node_name            | node1 |
| signed_sessions      | 0     |
| established_sessions | 1     |
| node_name            | node2 |
| signed_sessions      | 1     |
| established_sessions | 0     |
| node_name            | node3 |
| signed_sessions      | 0     |
| established_sessions | 0     |
| node_name            | node4 |
| signed_sessions      | 0     |

次のコマンドでは、ノード2が署名したSMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1
```

| Counter         | Value |
|-----------------|-------|
| node_name       | node2 |
| signed_sessions | 1     |

次のコマンドで、admin権限レベルに戻ります。

```
cluster1::*> set -privilege admin
```

#### 関連タスク

[受信SMBトラフィックのSMB署名要求の有効化と無効化](#)

[SMBセッションが署名されているかどうかの確認](#) (91ページ)

## CIFSサーバのSMBを介したデータ転送に必要なとなるSMB暗号化の設定

SMBを介したデータ転送でのSMB暗号化は、CIFSサーバで有効化または無効化できるセキュリティ強化です。これを有効にすると、共有プロパティ設定から共有ごとに必要なSMB暗号化を設定できます。

デフォルトでは、Storage Virtual Machine (SVM) でのCIFSサーバの作成時にSMB暗号化は無効になっています。SMB暗号化が提供する強固なセキュリティを活用するには、SMB暗号化を有効にする必要があります。

暗号化SMBセッションを作成するには、SMBクライアントがSMB暗号化をサポートしている必要があります。SMB暗号化は、Windows Server 2012およびWindows 8以降のWindowsクライアントでサポートされています。

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

- SVMの機能を有効化するCIFSサーバ セキュリティ オプション
- 共有ごとにSMB暗号化を設定するCIFS共有プロパティ

SVM上のすべてのデータへのアクセスに暗号化を要求するか、選択した共有のデータにアクセスする場合のみにSMB暗号化を要求するかを決定できます。SVMレベルの設定は、共有レベルの設定よりも優先されます。

次の表に記載された2つの設定の組み合わせを使用すると、効果的なSMB暗号化設定を行うことができます。

| CIFSサーバSMB暗号化が有効 | 共有暗号化データ設定が有効 | サーバ側の暗号化の動作                                             |
|------------------|---------------|---------------------------------------------------------|
| True             | False         | SVMのすべての共有でサーバレベルの暗号化が有効です。この設定では、SMBセッション全体で暗号化が行われます。 |

| CIFSサーバSMB暗号化が有効 | 共有暗号化データ設定が有効 | サーバ側の暗号化の動作                                                            |
|------------------|---------------|------------------------------------------------------------------------|
| True             | True          | 共有レベルの暗号化には関係なくSVMのすべての共有でサーバレベルの暗号化が有効です。この設定では、SMBセッション全体で暗号化が行われます。 |
| False            | True          | 特定の共有で共有レベルの暗号化が有効です。この設定では、ツリー接続から暗号化が行われます。                          |
| False            | False         | 暗号化は無効です。                                                              |

暗号化をサポートしないSMBクライアントは、暗号化が必要なCIFSサーバや共有には接続できません。

### 受信SMBトラフィックのSMB暗号化要求の有効化と無効化

受信SMBトラフィックに対してSMB暗号化を必須にするには、CIFSサーバ上または共有レベルでこれを有効にすることができます。デフォルトでは、SMB暗号化は必須ではありません。

#### タスク概要

CIFSサーバ上でSMB暗号化を有効にすると、その設定はCIFSサーバのすべての共有に適用されます。CIFSサーバの一部の共有でのみSMB暗号化要求を有効にする場合、または受信SMBトラフィックのSMB暗号化要求を共有ごとに有効にする場合は、CIFSサーバ上でSMB暗号化要求を無効にすることができます。

Storage Virtual Machine (SVM) ディザスタリカバリ関係をセットアップするときに、`snapmirror create` コマンドの `-identity-preserve` オプションに指定する値によって、デスティネーションSVMでレプリケートされる設定の詳細が決まります。

`-identity-preserve` オプションを `true` (ID保持) に設定すると、SMB暗号化のセキュリティ設定がデスティネーションにレプリケートされます。

`-identity-preserve` オプションを `false` (非ID保持) に設定すると、SMB暗号化のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションではCIFSサーバのセキュリティ設定がデフォルト値に設定されます。ソースSVMでSMB暗号化を有効にしている場合は、デスティネーションでCIFSサーバのSMB暗号化を手動で有効にする必要があります。

#### 手順

1. 次のいずれかを実行します。

| CIFSサーバでの受信SMBトラフィックのSMB暗号化要求の設定 | 入力するコマンド                                                                                          |
|----------------------------------|---------------------------------------------------------------------------------------------------|
| 有効                               | <code>vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true</code>  |
| 無効                               | <code>vserver cifs security modify -vserver vserver_name -is-smb-encryption-required false</code> |

2. CIFSサーバでのSMB暗号化要求が有効または無効になっていることを確認します。

```
vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required
```

CIFSサーバでSMB暗号化要求が有効になっている場合は、`is-smb-encryption-required` フィールドに `true` が表示され、無効になっている場合は `false` が表示されます。

**例**

次の例では、SVM vs1でCIFSサーバの受信SMBトラフィックのSMB暗号化要求を有効にしています。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption-
required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----
vs1      true
```

**クライアントが暗号化されたSMBセッションを使用して接続しているかどうかの確認**

接続中のSMBセッションに関する情報を表示し、クライアントが暗号化されたSMB接続を使用しているかどうかを確認できます。これは、必要なセキュリティ設定を使用してSMBクライアント セッションが接続されているかどうかを確認する場合に役立ちます。

**タスク概要**

SMBクライアント セッションには、次の3つのいずれかの暗号化レベルを設定できます。

- **unencrypted**  
SMBセッションは暗号化されません。Storage Virtual Machine (SVM)レベルの暗号化も共有レベルの暗号化も設定されません。
- **partially-encrypted**  
ツリー接続が行われたときに暗号化が開始されます。共有レベルの暗号化が設定されます。SVMレベルの暗号化は有効になりません。
- **encrypted**  
SMBセッション全体が暗号化されます。SVMレベルの暗号化が有効になります。共有レベルの暗号化は、有効になる場合とならない場合があります。SVMレベルの暗号化設定は、共有レベルの暗号化設定よりも優先されます。

**手順**

1. 次のいずれかを実行します。

| 表示する情報                             | 入力するコマンド                                                                                                            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| 指定したSVMのセッションで、指定した暗号化設定を使用するセッション | <b>vserver cifs session show -vserver <i>vserver_name</i> {unencrypted partially-encrypted encrypted} -instance</b> |
| 指定したSVMの特定のセッションIDの暗号化設定           | <b>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</b>                  |

**例**

次のコマンドを実行すると、セッションID 2のSMBセッションに関する、暗号化設定を含む詳細なセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
```



```

Windows User: DOMAIN\joe
  UNIX User: pcuser
    Open Shares: 1
    Open Files: 1
    Open Other: 0
  Connected Time: 10m 43s
    Idle Time: 1m 19s
  Protocol Version: SMB3
Continuously Available: No
  Is Session Signed: true
  User Authenticated as: domain-user
    NetBIOS Name: CIFS_ALIAS1
  SMB Encryption Status: Unencrypted

```

## SSL/TLS経由のLDAPを使用した通信の保護

SSL/TLS経由のLDAPを使用して、Storage Virtual Machine (SVM) LDAPクライアントとLDAPサーバの間の通信を保護することができます。この場合、LDAPサーバとやり取りされるすべてのトラフィックをLDAPによって暗号化できます。

### SSL/TLS経由のLDAPの概念

Data ONTAPによるSSL/TLSを使用したLDAP通信の保護方法に関する用語や概念を理解しておく必要があります。Data ONTAPでは、SSL/TLS経由のLDAPを使用して、Active Directoryに統合されたLDAPサーバ間またはUNIXベースのLDAPサーバ間の認証されたセッションを設定できます。

#### 用語

Data ONTAPでのSSL経由のLDAPを使用したLDAP通信の保護方法に関して理解しておくべき用語があります。

#### LDAP

(Lightweight Directory Access Protocol; ライトウェイト ディレクトリ アクセス プロトコル) 情報ディレクトリに対するアクセスおよび管理を行うためのプロトコルです。LDAPは、ユーザ、グループ、ネットグループのようなオブジェクトを格納するための情報ディレクトリとして使用されます。また、これらのオブジェクトを管理したりLDAPクライアントからの要求を処理するディレクトリ サービスを提供します。

#### SSL

(Secure Sockets Layer) インターネット上で情報を安全に送信するために開発されたセキュアなプロトコルです。SSLは、サーバ認証または相互 (サーバとクライアント) 認証を実現するために使用されます。SSLは暗号化の機能のみを提供します。データの整合性を保証する手段が必要な場合は、SSLを使用してアプリケーションで提供する必要があります。

#### TLS

(Transport Layer Security) それまでのSSL仕様に基づいたIETF標準の追跡プロトコルです。SSLの後継にあたります。

#### SSL/TLS経由のLDAP

(*LDAPS*) SSLまたはTLSを使用してLDAPクライアントとLDAPサーバとの間の通信を保護するプロトコルです。*SSL*と*TLS*という2つの用語は、プロトコルの具体的なバージョンを指す場合を除き、同じ意味で使用されることが少なくありません。

#### Start TLS

(*start\_tls*、*STARTTLS*、*StartTLS*とも表記) TLS/SSLプロトコルを使用してセキュアな通信を提供するメカニズムです。

### Data ONTAPでのSSL/TLS経由のLDAPの使用方法

デフォルトでは、クライアントとサーバ アプリケーション間のLDAP通信は暗号化されません。つまり、ネットワーク監視用のデバイスまたはソフトウェアを使用してLDAPクライアントとサーバ コンピュータ間の通信内容を表示することが可能です。特に問題になるのはLDAPの簡易バインドが使用されている場合で、LDAPクライアントをLDAPサーバにバインドするために使用されるクレデンシャル(ユーザ名とパスワード)が暗号化されずにネットワークを介して渡されます。

SSLおよびTLSプロトコルは、TCP/IPよりも上位、かつLDAPなどの上位プロトコルよりも下位で動作します。これらのプロトコルは上位プロトコルに代わってTCP/IPを使用し、SSL対応のサーバがSSL対応クライアントに対して自身を認証するのを許可し、双方のマシンが暗号化された接続を確立するのを許可します。こうした機能により、インターネットやその他のTCP/IPネットワーク経由の通信についての基本的なセキュリティ面での懸念は払拭されます。

Data ONTAPはSSLサーバ認証をサポートしており、Storage Virtual Machine(SVM)のLDAPクライアントは、バインド時にLDAPサーバの識別情報を確認できます。SSL/TLSに対応したLDAPクライアントは、公開鍵暗号化の標準的な技法を使用して、サーバの証明書および公開IDが有効であり、かつクライアントの信頼できるCertificate Authority(CA;認証局)のリストにあるCAによって発行されたものであるかどうかをチェックできます。

このバージョンのData ONTAPでは以下の機能をサポートしています。

- Active Directory統合LDAPサーバとSVMとの間のSMB関連トラフィックに対するSSL/TLS経由のLDAP
- ネーム マッピング用LDAPトラフィックに対するSSL/TLS経由のLDAP  
Active Directory統合LDAPサーバまたはUNIXベースLDAPサーバのどちらかを使用して、LDAPネーム マッピングの情報を格納できます。
- 自己署名ルートCA証明書  
Active-Directory統合LDAPを使用している場合、Windows Server証明書サービスがドメインにインストールされると自己署名ルート証明書が生成されます。UNIXベースのLDAPサーバをLDAPネーム マッピングに使用している場合は、該当するLDAPアプリケーションに適した手段を使用して自己署名ルート証明書が生成および保存されます。

Data ONTAPは、データの署名(整合性の保護)や封印(暗号化)をサポートしていません。

デフォルトでは、SSL/TLS経由のLDAPは無効になっています。

### Data ONTAPではSSL/TLS経由のLDAPにポート389を使用

LDAPでは、SSL/TLSを使用した通信の暗号化方式として、従来のLDAPSとSTARTTLSの2つがサポートされています。LDAPS通信は、通常は専用のポート(通常636)経由で行われます。一方STARTTLSは標準のLDAPポート(389)経由でプレーンテキスト接続として開始され、その後SSL/TLS接続にアップグレードされます。

Data ONTAPでは、LDAP通信を保護するためにSTARTTLSを使用し、デフォルトのLDAPポート(389)を使用してLDAPサーバと通信します。SVMでは、SSL/TLS経由のLDAPでポート636を使用するように設定しないでください。LDAP接続が失敗します。LDAPサーバは、LDAPポート389経由の接続を許可するように設定する必要があります。そうしないと、SVMからLDAPサーバへのLDAP SSL/TLS接続が失敗します。

## LDAP over SSL/TLSの設定

LDAP over SSL/TLSを設定するには、Storage Virtual Machine(SVM)LDAP over SSL/TLSを有効化し、自己署名ルートCA証明書のコピーをエクスポートし、エクスポートしたファイルを使用して自己署名ルートCA証明書をSVMにインストールする必要があります。

### 手順

1. [CIFSサーバでのLDAP over SSL/TLSの有効化](#) (99ページ)

CIFSサーバでActive Directory LDAPサーバへのセキュアなLDAP通信を使用するには、CIFSサーバのセキュリティ設定を変更し、Active DirectoryサーバのLDAP通信用にLDAP over SSL/TLSを有効にする必要があります。

2. [自己署名ルートCA証明書のコピーのエクスポート](#) (99ページ)  
Active Directory通信の保護にLDAP over SSL/TLSを使用するには、まずActive Directory証明書サービスの自己署名ルートCA証明書のコピーを証明書ファイルにエクスポートし、それをASCIIテキストファイルに変換する必要があります。Data ONTAPは、このテキストファイルを使用して証明書をStorage Virtual Machine (SVM) にインストールします。
3. [SVMでの自己署名ルートCA証明書のインストール](#) (100ページ)  
LDAPサーバへのバインド時にセキュアなLDAP認証を使用するには、Storage Virtual Machine (SVM) に自己署名ルートCA証明書をインストールする必要があります。

## 関連情報

[clustered Data ONTAP 8.3 システム アドミニストレーション ガイド](#)

## CIFSサーバでのLDAP over SSL/TLSの有効化

CIFSサーバでActive Directory LDAPサーバへのセキュアなLDAP通信を使用するには、CIFSサーバのセキュリティ設定を変更し、Active DirectoryサーバのLDAP通信用にLDAP over SSL/TLSを有効にする必要があります。

### 手順

1. Active Directory LDAPサーバとのセキュアなLDAP通信を可能にするCIFSサーバのセキュリティ設定を行います。  
`vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. LDAP over SSL/TLSセキュリティ設定がtrueに設定されていることを確認します。  
`vserver cifs security show -vserver vserver_name`

### 終了後の操作

Storage Virtual Machine (SVM) の証明書サービス証明書ストアからエクスポートした自己署名ルートCA証明書をインストールします。

SVMでLDAPクライアントが設定されている場合、たとえば、SVMがマルチプロトコルである場合や、ユーザ マッピングにLDAPを使用していて、LDAPクライアントでLDAP over SSLを有効にした場合は、`vserver services name-service ldap client create` コマンドまたは `vserver services name-service ldap client modify` コマンドを使用し、`-use-start-tls` オプションをtrueに設定することで、有効にすることができます。

LDAPクライアント設定の作成の詳細については、『[clustered Data ONTAP ファイル アクセス管理 ガイド \(NFS\)](#)』を参照してください。

## 自己署名ルートCA証明書のコピーのエクスポート

Active Directory通信の保護にLDAP over SSL/TLSを使用するには、まずActive Directory証明書サービスの自己署名ルートCA証明書のコピーを証明書ファイルにエクスポートし、それをASCIIテキストファイルに変換する必要があります。Data ONTAPは、このテキストファイルを使用して証明書をStorage Virtual Machine (SVM) にインストールします。

### 開始する前に

Active Directory証明書サービスがすでにインストールされ、CIFSサーバが属するドメイン用に設定されている必要があります。Active Directory証明書サービスのインストールと設定の詳細については、[Microsoft TechNetライブラリ: \*technet.microsoft.com/ja-jp/library\*](https://technet.microsoft.com/ja-jp/library) を参照してください。

### 手順

1. ドメイン コントローラのルートCA証明書を .pem テキスト形式で取得します。

詳細については、[Microsoft TechNet ライブラリ: technet.microsoft.com/ja-jp/library](https://technet.microsoft.com/ja-jp/library) を参照してください。

### 終了後の操作

SVM に証明書をインストールします。

### 関連情報

[Microsoft TechNet ライブラリ](https://technet.microsoft.com/ja-jp/library)

## SVMでの自己署名ルートCA証明書のインストール

LDAP サーバへのバインド時にセキュアなLDAP認証を使用するには、Storage Virtual Machine (SVM) に自己署名ルートCA証明書をインストールする必要があります。

### タスク概要

SSL/TLS 経由のLDAPが有効な場合、SVM上のData ONTAP LDAPクライアントでは破棄された証明書はサポートされません。LDAPクライアントでは、破棄された証明書を破棄されていないものとして扱います。

### 手順

1. 自己署名ルートCA証明書をインストールします。

- a. 証明書のインストールを開始します。

```
security certificate install -vserver vservice_name -type server-ca
```

コンソール出力に次のメッセージが表示されます。

Please enter Certificate: Press <Enter> when done

- b. 証明書の .pem ファイルをテキスト エディタで開き、-----BEGIN CERTIFICATE----- から-----END CERTIFICATE----- までの行をコピーして、コンソールに貼り付けます。
  - c. 証明書の内容がコンソール プロンプトのあとに表示されていることを確認します。
  - d. Enter キーを押して、インストールを完了します。
2. 証明書がインストールされていることを確認します。

```
security certificate show -vserver vservice_name
```

## CIFSサーバでのデフォルトWindowsユーザからUNIXユーザへのマッピングの設定

設定済みのUNIXユーザ ディレクトリ ストアで特定のユーザをマッピング (暗黙的なネーム マッピングまたは明示的なWindowsとUNIXユーザ名のマッピング設定のどちらか) していないWindows (SMB) ユーザについて、CIFSサーバでのデフォルトWindowsユーザのUNIXユーザへのマッピングを設定できます。

- デフォルトUNIXアカウントの設定すると、SMBユーザはUNIXクレデンシャルを受信します (ホームドメインまたは信頼できるドメインからのローカルSMBユーザ アカウントおよびドメイン ユーザの場合)。
- ゲストUNIXアカウントを設定すると、SMBユーザはUNIXクレデンシャルを受信します (ローカル以外のアカウントまたは信頼できるドメイン以外から接続しているユーザの場合)。

- ・ CIFSサーバ オプションを有効にすると、ホームドメインのドメイン管理者グループは、rootアカウントUNIXクレデンシャルを受信します。

### デフォルトのUNIXユーザの設定

ユーザに対する他のマッピングの試行がすべて失敗した場合や、UNIXとWindowsの間で個々のユーザをマッピングしないようにする場合に使用するデフォルトのUNIXユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする場合は、デフォルトUNIXユーザを設定しないでください。

#### タスク概要

デフォルトで、デフォルトUNIXユーザの名前は「pcuser」です。これは、デフォルトで、デフォルトUNIXユーザへのユーザ マッピングが有効になっていることを示しています。デフォルトのUNIXユーザとして使用する別の名前を指定することもできます。指定する名前は、Storage Virtual Machine (SVM) 用に設定されているネーム サービス データベース内に存在する必要があります。このオプションをnull文字列に設定すると、どのユーザもUNIXデフォルト ユーザとしてCIFSサーバにアクセスできません。つまり、CIFSサーバにアクセスするためには、各ユーザがパスワード データベースにアカウントを持つ必要があります。

ユーザがデフォルトUNIXユーザ アカウントを使用してCIFSサーバに接続するには、次の前提条件を満たす必要があります。

- ・ ユーザが認証されていること
- ・ ユーザが、CIFSサーバのローカルWindowsユーザ データベース、CIFSサーバのホームドメイン、信頼できるドメイン (CIFSサーバでマルチドメイン ネーム マッピング検索が有効な場合) のいずれかにあること
- ・ ユーザ名が明示的にnull文字列にマッピングされていないこと

#### 手順

1. デフォルトのUNIXユーザを設定します。

| 目的                               | コマンド                                                                  |
|----------------------------------|-----------------------------------------------------------------------|
| デフォルトUNIXユーザ「pcuser」を使用する        | <code>vserver cifs options modify -default-unix-user pcuser</code>    |
| デフォルト ユーザとして別のUNIXユーザ アカウントを使用する | <code>vserver cifs options modify -default-unix-user user_name</code> |
| デフォルトのUNIXユーザを無効にする              | <code>vserver cifs options modify -default-unix-user ""</code>        |

#### 例

```
vserver cifs options modify -default-unix-user pcuser
```

2. デフォルトのUNIXユーザが正しく設定されていることを確認します。

```
vserver cifs options show -vserver vserver_name
```

#### 例

次の例では、SVM vs1のデフォルトUNIXユーザとゲストUNIXユーザの両方がUNIXユーザ「pcuser」に設定されています。

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

## 関連コンセプト

[ネーム マッピングの作成](#) (167ページ)

[FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法](#) (23ページ)

## ゲストUNIXユーザの設定

ゲストUNIXユーザを設定すると、信頼されていないドメインからログインしたユーザがゲストUNIXユーザにマッピングされ、CIFSサーバに接続できるようになります。ただし、マッピングされていないユーザの認証を失敗にする場合は、デフォルトUNIXユーザを設定しないでください。デフォルトでは、信頼されていないドメインのユーザによるCIFSサーバへの接続は許可されません(ゲストUNIXアカウントは設定されません)。

### タスク概要

ゲストUNIXアカウントを設定する場合は、次の点に注意する必要があります。

- CIFSサーバがホーム ドメインまたは信頼できるドメインのドメイン コントローラ、ローカル データベースのどちらかに対してユーザを認証できず、このオプションが有効である場合、CIFSサーバはユーザをゲスト ユーザと見なし、そのユーザを指定されたUNIXユーザにマッピングします。
- このオプションがnull文字列に設定されている場合、ゲストUNIXユーザは無効になります。
- いずれかのStorage Virtual Machine (SVM) ネーム サービス データベースで、ゲストUNIXユーザとして使用するUNIXユーザを作成する必要があります。
- ゲスト ユーザとしてログインしたユーザは、自動的にCIFSサーバのBUILTIN\guestsグループのメンバーになります。
- ゲスト ユーザとしてログインしたユーザは、ホーム ディレクトリを持ちません。

### 手順

1. 次のいずれかを実行します。

| 状況               | コマンド                                                                       |
|------------------|----------------------------------------------------------------------------|
| ゲストUNIXユーザを設定する  | <code>vserver cifs options modify -guest-unix-user <i>unix_name</i></code> |
| ゲストUNIXユーザを無効化する | <code>vserver cifs options modify -guest-unix-user ""</code>               |

### 例

```
vserver cifs options modify -guest-unix-user pcuser
```

2. ゲストUNIXユーザが正しく設定されていることを確認します。

```
vserver cifs options show -vserver vserver_name
```

例

次の例では、SVM vs1のデフォルトUNIXユーザとゲストUNIXユーザの両方がUNIXユーザ「pcuser」に設定されています。

**vserver cifs options show -vserver vs1**

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

### ルートへのAdministratorsグループのマッピング

環境内のクライアントがすべてCIFSクライアントで、Storage Virtual Machine (SVM) がマルチプロトコル ストレージ システムとしてセットアップされている場合は、SVM上のファイルにアクセスするルート権限を持つアカウントが1つ以上必要です。このアカウントがないと、十分なユーザ権限がないため、SVMを管理できません。

タスク概要

ただし、ストレージ システムがNTFS専用でセットアップされている場合、/etcディレクトリにファイルレベルのACLがあり、このACLによって、AdministratorsグループはData ONTAP構成ファイルにアクセスできます。

手順

1. 権限レベルをadvancedに設定します。  
**set -privilege advanced**
2. 必要に応じて、AdministratorsグループをルートにマッピングするCIFSサーバ オプションを設定します。

| 状況                                       | 表示されるユーザ名                                                                                                                                                                                                                                                                                       |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administratorグループ メンバーをルートにマッピングする       | <b>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to-root-enabled true</b><br><br>アカウントをルートにマッピングする/etc/usermap.cfgエントリを指定していない場合でも、Administratorsグループ内のすべてのアカウントがルートとみなされます。Administratorsグループに属するアカウントを使用してファイルを作成する場合、UNIXクライアントからファイルを表示するときに、ファイルはルートによって所有されます。 |
| Administratorsグループ メンバーのルートへのマッピングを無効にする | <b>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to-root-enabled false</b><br><br>Administratorsグループ内のアカウントがルートにマッピングされなくなります。ルートへのマッピングは、単一のユーザに対して明示的にのみ実行可能です                                                                                                     |

3. オプションが目的の値に設定されていることを確認します。  
**vserver cifs options show -vserver vserver\_name**
4. admin権限レベルに戻ります。  
**set -privilege admin**

# SMBセッションを介して接続しているユーザのタイプに関する情報の表示

SMBセッションを介して接続しているユーザのタイプに関する情報を表示できます。これは、適切なタイプのユーザのみがStorage Virtual Machine(SVM)上のSMBセッションを介して接続していることを確認するのに役立ちます。

## タスク概要

SMBセッションを介して接続できるのは、次のタイプのユーザです。

- **local-user**  
ローカルCIFSユーザとして認証されている
- **domain-user**  
ドメイン ユーザとして(CIFSサーバのホームドメインまたは信頼できるドメインから)認証されている
- **guest-user**  
ゲスト ユーザとして認証されている
- **anonymous-user**  
匿名ユーザまたはnullユーザとして認証されている

## 手順

1. SMBセッションを介して接続しているユーザのタイプを確認します。

```
vserver cifs session show -vserver vs1 -windows-user windows_user_name -fields windows-user,address,lif-address,user-type
```

| 確立されたセッションのユーザタイプ情報を表示する対象 | 入力するコマンド                                                                                                                               |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 指定したユーザタイプすべてのセッション        | <code>vserver cifs session show -vserver vs1 -user-type {local-user domain-user guest-user anonymous-user}</code>                      |
| 特定のユーザ                     | <code>vserver cifs session show -vserver vs1 -windows-user windows_user_name -fields windows-user,address,lif-address,user-type</code> |

**例**  
次のコマンドを実行すると、ユーザ「iepubs\user1」によって確立されたSVM vs1上のセッションのユーザタイプに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user iepubs \user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user      user-type
-----
pub1node1 pub1      1          3439441860    10.0.0.1    10.1.1.1    IEPUBS \user1      domain-user
```



## CIFSサーバでのSMBの設定

Server Message Block (SMB; サーバ メッセージ ブロック) は、Microsoft Windows クライアントおよびサーバで使用されるリモート ファイル 共有プロトコルです。Storage Virtual Machine (SVM) に関連付けられているCIFSサーバのSMBを設定および管理できます。

### 関連コンセプト

[SMB署名を使用したネットワーク セキュリティの強化](#) (87 ページ)

### サポートされるSMBのバージョン

Data ONTAP では、データ SVM の CIFS サーバで、複数のバージョンの Server Message Block (SMB; サーバ メッセージ ブロック) プロトコルをサポートしています。サポートされる SMB のバージョンは、FlexVol を備えた SVM と Infinite Volume を備えた SVM で異なります。それぞれの種類の Storage Virtual Machine (SVM) でサポートされるバージョンを確認しておく必要があります。

FlexVol を備えた SVM と Infinite Volume を備えた SVM でサポートされる SMB のバージョンを次に示します。

| SMB のバージョン | FlexVol を備えた SVM でのサポート | Infinite Volume を備えた SVM でのサポート |
|------------|-------------------------|---------------------------------|
| SMB 1.0    | ○                       | ○                               |
| SMB 2.0    | ○                       | ×                               |
| SMB 2.1    | ○                       | ×                               |
| SMB 3.0    | ○                       | ×                               |

### サポートされる SMB 1.0 の機能

CIFS (SMB 1.0) プロトコルは、Microsoft が Windows クライアント向けに導入したプロトコルです。Data ONTAP では、clustered Data ONTAP のすべてのバージョン、および FlexVol を備えた Storage Virtual Machine (SVM) と Infinite Volume を備えた SVM で SMB 1.0 プロトコルをサポートしています。

SMB 1.0 プロトコルは、導入以降、Microsoft によって拡張が繰り返され、セキュリティ、ファイル、およびディスク管理の機能が強化されてきました。SMB 1.0 のみをサポートするレガシー Windows クライアント (Windows XP より前) や Windows 以外のクライアントでは、SMB 1.0 を使用して SVM のデータにアクセスできます。

### サポートされる SMB 2.0 の機能

clustered Data ONTAP 8.1 以降では、FlexVol を備えた Storage Virtual Machine (SVM) で SMB 2.0 プロトコルがサポートされます。SMB 2.0 は SMB プロトコルのメジャー リビジョンであり、パフォーマンスが強化されているほか、永続性ハンドルを使用してネットワークの中断に対する耐障害性も強化されています。

SMB 2.0 は、CIFS サーバを作成すると自動的に有効になります。

Data ONTAP では、SMB 2.0 の次の機能をサポートしています。

- 永続性ハンドル  
ネットワークが短時間停止した場合に、切断された SMB セッションにクライアントを透過的に再接続できます。たとえば、SMB 2.0 接続では、LIF のフェイルオーバー、LIF の移動、および LIF の移行が透過的に無停止で実行されます。
- 複合操作

複数のSMBメッセージを組み合わせ、基盤となるトランスポートに1つのネットワーク転送要求として送信できます。

- 非同期操作  
クライアントで実行するSMBのコマンドの中には、サーバで処理されるまでに時間がかかるものがあります。そのようなコマンドに対して、CIFSサーバから非同期で応答を送信できます。
- 読み取り / 書き込みバッファのサイズの増加  
遅延の多いネットワークも含め、高速なネットワークのスループットが向上しています。
- 拡張性の向上  
SMB 2.0では、SMBセッションの数や開くことができる共有接続およびファイル接続の数の上限が引き上げられています。
- SMB署名によるセキュリティの強化  
HMAC-SHA256ハッシュ アルゴリズムを使用した強力なデータ整合性保護機能がサポートされています。

Data ONTAPでは、SMB 2.0の次の機能はサポートされません。

- シンボリック リンク
- フロー制御用のクレジット システム

CIFSサーバでSMB 2.0が無効になっている場合、SMB 2.0クライアントとCIFSサーバの間の通信はSMB 1.0プロトコルにフォールバックされます(SMB 2.0クライアントのネゴシエート要求にSMB 1.0のダイレクトが含まれている場合)。

詳細については、テクニカル レポートTR-3740またはSMB 2.0プロトコルの仕様を参照してください。

#### 関連情報

テクニカル レポート:『SMB 2—Next-Generation CIFS Protocol in Data ONTAP』  
([media.netapp.com/documents/tr-3740.pdf](http://media.netapp.com/documents/tr-3740.pdf))

#### サポートされるSMB 2.1の機能

SMB 2.1プロトコルは、SMB 2.0プロトコルの機能をいくつか強化したものです。Data ONTAP 8.1以降では、FlexVolを備えたStorage Virtual Machine (SVM)でSMB 2.1がサポートされます。SMB 2.1は、CIFSサーバでSMB 2.0プロトコルを有効にすると自動的に有効になります。

SMB 2.0およびSMB 2.1は、CIFSサーバを作成すると自動的に有効になります。SMB 2.0とSMB 2.1は常に一緒に有効または無効になります。SMB 2.0とSMB 2.1を別々に有効または無効にすることはできません。

Data ONTAPでは、SMB 2.1の次の機能をサポートしています。

- oplockリリース  
Data ONTAPでは、SMB 2.1のoplockリリースが使用されます。これは、従来のoplockよりも優れた新しいoplockモデルです。oplockリリースを使用すると、より詳しく柔軟にクライアントのキャッシュを制御できます。これにより、遅延の多い不安定なネットワークにおけるパフォーマンスが大幅に向上します。
- BranchCacheバージョン1  
BranchCacheは、リモート オフィスでクライアント側キャッシュを使用することで、WAN帯域幅を最適化し、ファイル アクセス パフォーマンスを向上させる機能です。SMB 2.1には、コンテンツ ハッシュを管理するために必要な拡張機能が備わっています。BranchCache対応のCIFSサーバでは、このコンテンツ ハッシュを使用して、キャッシュされたコンテンツに関する情報をクライアントに提供します。

Data ONTAPでは、SMB 2.1の次の機能はサポートされません。

- Large MTU
- 永続性ハンドル

詳細については、テクニカル レポートTR-3740またはSMB 2.1プロトコルの仕様を参照してください。

#### 関連情報

テクニカル レポート:『SMB 2—Next-Generation CIFS Protocol in Data ONTAP』  
([media.netapp.com/documents/tr-3740.pdf](http://media.netapp.com/documents/tr-3740.pdf))

#### サポートされるSMB 3.0の機能

clustered Data ONTAP 8.2以降では、FlexVolを備えたStorage Virtual Machine(SVM)でSMB 3.0プロトコルがサポートされます。SMB 3.0には、重要な拡張機能として、透過的なフェイルオーバーとギブバック、およびその他のノンストップ オペレーションを円滑に実行するための機能などが含まれています。

SMB 3.0は、CIFSサーバを作成すると自動的に有効になります。

Data ONTAPでは、SMB 3.0の次の機能をサポートしています。

- 共有の継続的な可用性  
継続的な可用性を確保するように共有を設定すると、その共有に接続されたSMBクライアントは、永続的なハンドルを使用して、フェイルオーバー処理やギブバック処理などでシステムが停止した場合にCIFSサーバに透過的に再接続することができます。
- 永続的ハンドル  
システムが停止した場合に、切断されたSMBセッションにクライアントを透過的に再接続できます。永続的なハンドルは切断後も維持され、再接続されるまで他のファイルが開かれなようにブロックします。永続的なハンドルと共有の継続的な可用性を組み合わせることにより、特定のノンストップ オペレーションがサポートされます。
- SMB共有に対するリモートVSS  
SMBに対するリモートVSS(ボリューム シャドウ コピー サービス)を使用すると、VSSに対応したバックアップ サービスで、SMB 3.0共有を介して格納されたデータにアクセスするVSS対応アプリケーションについて、アプリケーションと整合性のあるボリューム シャドウ コピーを作成できます。
- 監視  
ネットワークで障害が発生した場合に、Hyper-VおよびSQLアプリケーション サーバにSMB共有を提供するCIFSサーバから、その情報をすぐにアプリケーション サーバに通知できます。
- ODXコピー オフロード  
ODXを使用すると、ODX対応のストレージ サーバ内やストレージ サーバ間で、Windowsクライアントを介さずにデータを転送できます。
- BranchCacheバージョン2  
いくつかの機能が拡張されています。たとえば、より細かい任意のサイズのセグメントにコンテンツを分割できるようになったため、キャッシュされている既存のコンテンツを再利用しやすくなりました。
- SMB暗号化  
ネットワーク上のSMBデータをエンドツーエンドで暗号化し、クライアントSMB接続のセキュリティを強化します。

Data ONTAPでは、SMB 3.0の次の機能はサポートされません。

- SMBマルチチャネル

- SMBダイレクト
- SMBディレクトリ リース

詳細については、SMB 3.0プロトコルの仕様を参照してください。

#### 関連コンセプト

[SMBアクティビティの監視](#)(305ページ)

#### 関連タスク

[SMB 3.0の有効化と無効化](#)(109ページ)

[oplockステータスの監視](#)(113ページ)

[CIFSサーバでのSMB共有の作成](#)(180ページ)

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#)(403ページ)

## SMB 2.xの有効化と無効化

SMB 2.xは、FlexVolを備えたStorage Virtual Machine(SVM)上のCIFSサーバでデフォルトで有効になっています。これにより、クライアントからSMB 2.xを使用してCIFSサーバに接続できるようになります。SMB 2.xは、CIFSサーバ オプションを使用していつでも有効または無効にできます。

#### タスク概要

-smb2-enabledオプションにより、SMB 2.0とSMB 2.1を有効にします。

#### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| SMB 2.xの設定 | 入力するコマンド                                                                           |
|------------|------------------------------------------------------------------------------------|
| 有効         | <code>vserver cifs options modify -vserver vserver_name -smb2-enabled true</code>  |
| 無効         | <code>vserver cifs options modify -vserver vserver_name -smb2-enabled false</code> |

3. admin権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次の例では、SVM vs1でSMB 2.xを有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -smb2-enabled true

cluster1::*> set -privilege admin
```

関連コンセプト

- [サポートされるSMB 2.0の機能](#)(105ページ)
- [サポートされるSMB 2.1の機能](#)(106ページ)

SMB 3.0の有効化と無効化

SMB 3.0は、FlexVolを備えたStorage Virtual Machine(SVM)上のCIFSサーバでデフォルトで有効になっています。これにより、SMB 3.0をサポートするクライアントからSMB 3.0を使用してCIFSサーバに接続できるようになります。SMB 3.0は、CIFSサーバ オプションを使用していつでも有効または無効にできます。

タスク概要

このオプションは、共有の継続的可用性を設定する場合に有効にする必要があります。

ODXコピー オフロードを使用するには、SMB 3.0が有効になっている必要があります。ODXコピー オフロードが有効になっている場合にSMB 3.0を無効にすると、ODXコピー オフロードは自動的に無効になります。同様に、ODXコピー オフロードを有効にすると、SMB 3.0は自動的に有効になります(有効になっていない場合)。

手順

- 権限レベルをadvancedに設定します。  
`set -privilege advanced`
- 次のいずれかを実行します。

| SMB 3.0の設定 | 入力するコマンド                                                                           |
|------------|------------------------------------------------------------------------------------|
| 有効         | <code>vserver cifs options modify -vserver vserver_name -smb3-enabled true</code>  |
| 無効         | <code>vserver cifs options modify -vserver vserver_name -smb3-enabled false</code> |

- admin権限レベルに戻ります。  
`set -privilege admin`

例

次のコマンドを実行すると、SVM vs1でSMB 3.0が有効になります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -smb3-enabled true

cluster1::*> set -privilege admin
```

関連コンセプト

- [サポートされるSMB 3.0の機能](#)(107ページ)

## 従来のoplockおよびoplockリリースでのクライアント パフォーマンスの向上

従来のoplock(便宜的ロック)とoplockリリースでは、先読み、あと書き、ロックの各情報をSMBクライアント側でキャッシングできるよう、特定のファイル共有シナリオでそのクライアントを有効にします。これによりクライアントは、目的のファイルへのアクセス要求をサーバに定期的に通知しなくても、ファイルの読み書きを実行できます。この処理によって、ネットワークトラフィックが軽減し、パフォーマンスが向上します。

oplockリリースはoplockを強化したもので、SMB 2.1以降のプロトコルで使用できます。oplockリリースでは、クライアントが、自身による複数のSMBオープンにおいてキャッシュ状態を取得、保持できます。

oplockリリースは、Infinite Volumeを備えたStorage Virtual Machine(SVM)ではサポートされません。

### oplockを使用するときの書き込みキャッシュ データ消失に関する考慮事項

状況によっては、あるプロセスがファイルに対して排他的なoplockを保持している場合に、別のプロセスがそのファイルを開こうとすると、最初のプロセスは、キャッシュされたデータを無効にし、書き込みとロックをフラッシュする必要があります。クライアントはoplockを放棄し、ファイルにアクセスする必要があります。このフラッシュ時にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われることがあります。

- データ消失の可能性  
データの書き込みがキャッシュされるアプリケーションでは、次の場合にそのデータを失う可能性があります。
  - 接続はSMB 1.0を使用して確立されます。
  - ファイルに対して排他的なoplockを使用している場合
  - そのoplockを破棄するか、ファイルを閉じるように指示された場合
  - 書き込みキャッシュをフラッシュするプロセスで、ネットワークまたはターゲット システムにエラーが発生した場合
- エラー処理および書き込みの完了  
キャッシュ自体にはエラー処理機能がありません。アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行うと、書き込みは必ず完了します。またキャッシュがネットワークを介してターゲット システムに書き込みを行う場合、書き込みは正常に終了することを前提とする必要があります。このような前提でないと、後続のプロセスでデータが失われるからです。

### SMB共有の作成時におけるoplockの有効化と無効化

oplockを使用すると、クライアントによりファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスを向上できます。FlexVolを備えたStorage Virtual Machine(SVM)上にあるSMB共有では、oplockがデフォルトで有効になっています。場合によっては、oplockの無効化が必要になることがあります。oplockは共有ごとに有効または無効にできます。

#### タスク概要

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームのoplockの設定よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリリースの両方が無効になります。

oplock共有プロパティに加えて、その他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する処理を実行します。

| 状況                     | 表示されるユーザ名                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 共有の作成時に共有でoplockを有効にする | <p>次のコマンドを入力します。</p> <pre><b>vserver cifs share create -vserver vserver_name -share-name share_name -path path_to_share -share-properties [oplocks,...]</b></pre> <p>注: 共有でデフォルトの共有プロパティ<b>oplocks</b>、<b>browsable</b>、および<b>changenotify</b>のみを有効にする場合は、SMB共有の作成時に<b>-share-properties</b>パラメータを指定する必要はありません。デフォルト以外の共有プロパティを組み合わせで使用する場合は、<b>-share-properties</b>パラメータとその共有で使用する共有プロパティのリストを指定する必要があります。</p> |
| 共有の作成時に共有でoplockを無効にする | <p>次のコマンドを入力します。</p> <pre><b>vserver cifs share create -vserver vserver_name -share-name share_name -path path_to_share -share-properties [other_share_property,...]</b></pre> <p>注: oplockを無効にする場合は、共有の作成時に共有プロパティのリストを指定する必要がありますが、<b>oplocks</b>プロパティは指定しないでください。</p>                                                                                                                                         |

関連タスク

[既存のSMB共有でのoplockの有効化と無効化](#)(111ページ)

[oplockステータスの監視](#)(113ページ)

[CIFSサーバでのSMB共有の作成](#)(180ページ)

## 既存のSMB共有でのoplockの有効化と無効化

FlexVolを備えたStorage Virtual Machine(SVM)上のSMB共有では、oplockがデフォルトで有効になっています。場合によっては、oplockの無効化が必要になることがあります。または、以前に共有でoplockを無効にした場合に、oplockを再度有効にすることもあります。

タスク概要

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームでのoplockの有効化よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。既存の共有でのoplockの有効化と無効化はいつでも実行できます。

手順

1. 該当する処理を実行します。



| 状況                        | 表示されるユーザ名                                                                                                                                                                                                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 既存の共有を変更して共有でoplockを有効にする | <p>次のコマンドを入力します。</p> <pre><b>vserver share properties add -vserver<br/>vserver_name -share-name share_name -share-<br/>properties oplocks</b></pre> <p><b>注:</b> 追加する共有プロパティをカンマで区切って追加指定できます。</p> <p>新たに追加したプロパティは、共有プロパティの既存のリストに追加されます。以前に指定した共有プロパティは有効なままです。</p>           |
| 既存の共有を変更して共有でoplockを無効にする | <p>次のコマンドを入力します。</p> <pre><b>vserver share properties remove -vserver<br/>vserver_name -share-name share_name -share-<br/>properties oplocks</b></pre> <p><b>注:</b> 削除する共有プロパティをカンマで区切って追加指定できます。</p> <p>削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しなかった設定済みの共有プロパティは有効なままになります。</p> |

**例**

次のコマンドを実行すると、Storage Virtual Machine (SVM、旧Vserver) vs1上の「Engineering」という名前の共有でoplockが有効になります。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name  
Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

| Vserver | Share       | Properties                                           |
|---------|-------------|------------------------------------------------------|
| vs1     | Engineering | oplocks<br>browsable<br>changenotify<br>showsnapshot |

次のコマンドを実行すると、SVM vs1上の「Engineering」という名前の共有でoplockが無効になります。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name  
Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

| Vserver | Share       | Properties                                |
|---------|-------------|-------------------------------------------|
| vs1     | Engineering | browsable<br>changenotify<br>showsnapshot |

**関連タスク**

[SMB共有の作成時におけるoplockの有効化と無効化](#)(110ページ)

[oplockステータスの監視](#)(113ページ)

[既存のSMB共有に対する共有プロパティの追加または削除](#)(187ページ)

**ボリュームおよびqtreeでoplockを有効または無効にするコマンド**

oplockを使用すると、クライアントによりファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスを向上できます。ボリュームやqtreeのoplockを有効また



は無効にするためのコマンドを理解しておく必要があります。また、いつボリュームおよびqtreeでoplockを有効化または無効化できるかについても理解しておく必要があります。

- ボリュームではデフォルトでoplockが有効になっています。
- ボリュームを作成する際にoplockを無効化することはできません。
- 既存のFlexVolを備えたSVMボリュームでのoplockの有効化と無効化はいつでも実行できます。
- Infinite Volumeを備えたSVMのボリュームでは、いったん有効になったoplockを無効にすることはできません。
- FlexVolを備えたSVMでは、qtreeのoplockを有効にできます。  
qtreeの作成時にoplock設定を指定しない場合、qtreeは親ボリュームのoplock設定を継承します。一方、qtreeのoplock設定を指定すると、親ボリュームのoplock設定に優先して、その設定が適用されます。

| 状況                     | 使用するコマンド                                                      |
|------------------------|---------------------------------------------------------------|
| ボリュームやqtreeのoplockの有効化 | volume qtree oplocksコマンドを実行。この際、-oplock-modeパラメータをenableに設定。  |
| ボリュームやqtreeのoplockの無効化 | volume qtree oplocksコマンドを実行。この際、-oplock-modeパラメータをdisableに設定。 |

関連タスク

[oplockステータスの監視](#)(113ページ)

oplockステータスの監視

oplockステータスについて、情報を監視、表示することができます。この情報を使用すると、oplockが設定されたファイル、oplockのレベルやoplockの状態レベルのほか、oplockリースの使用の有無を特定できます。また、手動での解除が必要となる可能性のあるロックについて、情報を取得することもできます。

タスク概要

すべてのoplockについての情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、クライアントのIPアドレスやパスを指定して、該当するロックのみを返すように指定できます。

従来のoplockおよびoplockリースについて、次の情報を表示できます。

- oplockが有効なSVM、ノード、ボリューム、LIF
- ロックUUID
- oplockが有効なクライアントのIPアドレス
- oplockが有効なパス
- ロックのプロトコル(SMB)およびロックのタイプ(oplock)
- ロックの状態  
ロックは次のいずれかの状態になります。

| ロックの状態  | 説明        |
|---------|-----------|
| granted | ロックは有効です。 |

| ロックの状態   | 説明                                        |
|----------|-------------------------------------------|
| revoking | ロックの状態を変更するために、サーバがクライアントと調整中です。          |
| revoked  | ダウングレードまたはリリースのために、ロックの解除を実行中です。          |
| adjusted | 現在のロックと同等かまたは弱いロックで置き換えるために、ロックの解除を実行中です。 |
| subsumed | 解除中のロックに置き換わる一連のロックのうちのひとつです。             |
| waiting  | 別のロックと競合しているため許可待ちの状態です。                  |
| denied   | ロックは拒否されています。                             |
| timeout  | 待機中でしたがタイムアウトしました。                        |
| gone     | リリースされようとしています。                           |
| unused   | ロックは割り当てられていますが、どの状態にもなっていません。            |

- oplockレベル  
ロックは次のいずれかのoplockレベルになります。

| oplockレベル  | 説明                                   |
|------------|--------------------------------------|
| batch      | クライアントは、対象のファイルの操作すべてをキャッシュできます。     |
| exclusive  | クライアントは、対象のファイルの読み取りと書き込みをキャッシュできます。 |
| read-batch | クライアントは、対象のファイルの読み取りとオープンをキャッシュできます。 |
| level2     | クライアントは、対象のファイルの読み取りをキャッシュできます。      |
| null       | クライアントは、対象のファイルのいずれの操作もキャッシュできません。   |

- 接続の状態およびSMBの有効期限
- oplockリリースが有効な場合のOpen Group ID

## 手順

1. vserver locks showコマンドを使用してoplockの状態を表示します。

### 例

次のコマンドでは、すべてのロックについてデフォルトの情報を表示します。表示するファイルのoplockには**read-batch**のoplockレベルが許可されています。

```
cluster1::> vserver locks show
```

```
Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
vol1    /vol1/notes.txt          node1_data1  cifs      share-level 192.168.1.5
Sharelock Mode: read_write-deny_delete
Oplock Level: read-batch
op-lock    192.168.1.5
```

次の例では、/data2/data2\_2/intro.pptxのパスを持つファイルのロックについて、詳細の情報が表示されています。このファイルでは、**10.3.1.3**のIPアドレスのクライアントに対して**batch**のoplockレベルでoplockリリースが有効になっています。

**注:** 詳細情報を表示する場合に、このコマンドを使用すると、oplockの情報と共有ロックの情報を別々に表示できます。この例では、oplockの情報のみが表示されています。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
Lock Protocol: cifs
Lock Type: op-lock
Node Holding Lock State: node3
Lock State: granted
ByteLock Starting Offset: -
Number of Bytes Locked: -
ByteLock is Mandatory: -
ByteLock is Exclusive: -
ByteLock is Superlock: -
ByteLock is Soft: -
Oplock Level: batch
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

#### 関連タスク

[SMB共有の作成時におけるoplockの有効化と無効化](#)(110ページ)

[既存のSMB共有でのoplockの有効化と無効化](#)(111ページ)

#### 関連参照情報

[ボリュームおよびqtreeでoplockを有効または無効にするコマンド](#)(112ページ)

## CIFSサーバへのグループ ポリシー オブジェクトの適用

SVMのCIFSサーバでは、グループ ポリシー オブジェクト(GPO)をサポートしています。GPOは、Active Directory環境のコンピュータに適用される一連のルール(グループポリシー属性)です。GPOを使用して、同じActive Directoryドメインに属するクラスター上のすべてのStorage Virtual Machine(SVM)の設定を一元管理できます。

Data ONTAPは、CIFSサーバでGPOが有効になっている場合、Active DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。Active Directoryサーバは、CIFSサーバに適用できるGPO定義がある場合、次のGPO情報を返します。

- GPO名
- 現在のGPOバージョン
- GPO定義の場所
- GPOポリシー セットのUniversally Unique Identifier(UUID)一覧

#### 関連コンセプト

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)

[FlexVolを備えたSVMでのNASイベントの監査](#)(432ページ)

## サポートされるGPO

すべてのグループ ポリシー オブジェクト(GPO)をCIFS対応のStorage Virtual Machine(SVM)に適用できるわけではありませんが、SVMでは関連するGPOを認識して処理することができます。

FlexVolを備えたSVMで現在サポートされているGPOは次のとおりです。

- 高度な監査ポリシー構成の設定:  
オブジェクト アクセス: 集約型アクセス ポリシーのステージング  
次の設定を含む集約型アクセス ポリシー(CAP)のステージングで監査対象となるイベントの種類を指定します。

- 監査しない
- 成功イベントのみ監査
- 失敗イベントのみ監査
- 成功イベントと失敗イベントの両方を監査

注: 3つの監査オプション(成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査)のいずれかが設定されている場合、clustered Data ONTAPは成功イベントと失敗イベントの両方を監査します。

**Advanced Audit Policy Configuration/Audit Policies/Object Access GPO内の Audit Central Access Policy Staging**設定を使用して設定します。

注: 高度な監査ポリシー構成GPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- レジストリ設定:
  - CIFS対応のSVMのグループ ポリシーの更新間隔  
**Registry GPO**を使用して設定します。
  - グループ ポリシーの更新間隔のランダム オフセット  
**Registry GPO**を使用して設定します。
  - BranchCacheのハッシュの発行  
BranchCacheのハッシュの発行GPOは、BranchCacheの動作モードに対応します。次の3つの動作モードがサポートされています。
    - Per-share
    - All-shares
    - 無効**Registry GPO**を使用して設定します。
  - BranchCacheのハッシュ バージョン サポート  
次の3つのハッシュ バージョン設定がサポートされています。
    - BranchCacheバージョン1
    - BranchCacheバージョン2
    - BranchCacheバージョン1および2**Registry GPO**を使用して設定します。

**注:** BranchCache GPO設定を使用するには、その設定を適用するCIFS対応のSVM上でBranchCacheを構成する必要があります。SVMでBranchCacheが構成されていない場合、GPO設定は適用されず、破棄されます。

- セキュリティ設定

- 監査ポリシーおよびイベント ログ

- ログオン イベントの監査

次の設定を含む監査対象となるログオン イベントの種類を指定します。

- 監査しない
- 成功イベントのみ監査
- 失敗イベントの監査
- 成功イベントと失敗イベントの両方を監査

**Audit logon events** GPO内の**Local Policies/Audit Policy**設定を使用して設定します。

**注:** 3つの監査オプション(成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査)のいずれかが設定されている場合、clustered Data ONTAPは成功イベントと失敗イベントの両方を監査します。

- オブジェクトへのアクセスの監査

次の設定を含む監査対象となるオブジェクト アクセスの種類を指定します。

- 監査しない
- 成功イベントのみ監査
- 失敗イベントの監査
- 成功イベントと失敗イベントの両方を監査

**Audit object access** GPO内の**Local Policies/Audit Policy**設定を使用して設定します。

**注:** 3つの監査オプション(成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査)のいずれかが設定されている場合、clustered Data ONTAPは成功イベントと失敗イベントの両方を監査します。

- ログの保持方法

次の設定を含む監査ログ保持方法を指定します。

- ログ ファイルのサイズが最大ログ サイズを超えた場合、イベント ログを上書き
- イベント ログを上書きしない(手動でログを消去)

**Retention method for security log** GPO内の**Event Log**設定を使用して設定します。

- 最大ログ サイズ

監査ログの最大サイズを指定します。

**Maximum security log size** GPO内の**Event Log**設定を使用して設定します。

**注:** 監査ポリシーとイベント ログGPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- ファイルシステムのセキュリティ  
GPOを通してファイル セキュリティを適用するファイルまたはディレクトリのリストを指定します。  
**File System** GPOを使用して設定します。  
  
注: SVM内にファイル システム セキュリティGPOを構成するボリューム パスが存在している必要があります。
- Kerberosポリシー
  - 最大クロック スキュー  
コンピュータ クロックの同期の許容最大誤差を分単位で指定します。  
**Maximum tolerance for computer clock synchronization** GPO内の**Account Policies/Kerberos Policy**設定を使用して設定します。
  - チケットの有効期間  
ユーザ チケットの最有効期間を時間単位で指定します。  
**Maximum lifetime for user ticket** GPO内の**Account Policies/Kerberos Policy**設定を使用して設定します。
  - チケットの更新の有効期間  
ユーザ チケットの更新の最大有効期間を日単位で指定します。  
**Maximum lifetime for user ticket renewal** GPO内の**Account Policies/Kerberos Policy**設定を使用して設定します。
- ユーザ権限割り当て(権限)
  - 所有権の取得  
セキュリティ保護が可能なオブジェクトの所有権を持つユーザとグループのリストを指定します。  
**Take ownership of files or other objects** GPO内の**Local Policies/User Rights Assignment**設定を使用して設定します。
  - セキュリティ権限  
ファイル、フォルダ、Active Directoryオブジェクトなどの個々のリソースへのオブジェクトアクセスの監査オプションを指定できるユーザとグループのリストを指定します。  
**Manage auditing and security log** GPO内の**Local Policies/User Rights Assignment**設定を使用して設定します。
  - 通知権限の変更(トラバース チェックのバイパス)  
ユーザやグループがトラバースするディレクトリに対する権限を持っていなくても、ディレクトリ ツリーをトラバースできるユーザとグループのリストを指定します。  
ファイルやディレクトリの変更通知を受け取るユーザにも同じ権限が必要です。**Bypass traverse checking** GPO内の**Local Policies/User Rights Assignment**設定を使用して設定します。
- レジストリ値
  - 署名要求設定  
SMB署名要求を有効にするか無効にするかを指定します。  
**Microsoft network server: Digitally sign communications (always)** GPO内の**Security Options**設定を使用して設定します。
- 匿名の制限  
匿名ユーザの制限内容に次の3つのGPO設定を指定します。
  - Security Account Manager (SAM) アカウントを列挙しない:

このセキュリティ設定で、コンピュータへの匿名接続に対して許可を行う追加権限の内容を決定します。このオプションが有効である場合、Data ONTAPで**no-enumeration**と表示されます。

**Local Policies/Security Options GPOでNetwork access: Do not allow anonymous enumeration of SAM accounts** 設定を使用して設定します。

- SAMアカウントと共有を列挙しない  
このセキュリティ設定で、匿名によるSAMアカウントと共有の列挙を許可するかどうかを決定します。このオプションが有効である場合、Data ONTAPで**no-enumeration**と表示されます。  
**Local Policies/Security Options GPOでNetwork access: Do not allow anonymous enumeration of SAM accounts and shares**設定を使用して設定します。
- 共有と名前付きパイプへの匿名アクセスを制限  
このセキュリティ設定で、共有とパイプへの匿名アクセスを制限します。このオプションが有効である場合、Data ONTAPで**no-access**と表示されます。  
**Network access: Restrict anonymous access to Named Pipes and Shares GPO内のLocal Policies/Security Options**設定を使用して設定します。

定義済みや適用されているグループ ポリシーについての情報を表示すると、**Resultant restriction for anonymous user**出力フィールドに3つの匿名制限GPO設定による制限結果に関する情報が表示されます。表示される可能性がある制限結果は、次のとおりです。

- **no-access**  
匿名ユーザによる指定された共有や名前付きパイプへのアクセスは拒否され、SAMアカウントや共有の列挙は使用できません。**Network access: Restrict anonymous access to Named Pipes and Shares GPO**が有効な場合、この制限結果になります。
- **no-enumeration**  
匿名ユーザは指定された共有や名前付きパイプにアクセスできますが、SAMアカウントや共有の列挙は使用できません。次の両方の条件が満たされている場合、この制限結果になります。
  - **Network access: Restrict anonymous access to Named Pipes and Shares GPO**が無効
  - **Network access: Do not allow anonymous enumeration of SAM accounts GPO**または**Network access: Do not allow anonymous enumeration of SAM accounts and shares GPO**が有効
- **no-restriction**  
匿名ユーザは、フル アクセスが可能で、列挙も使用できます。次の両方の条件が満たされている場合、この制限結果になります。
  - **Network access: Restrict anonymous access to Named Pipes and Shares GPO**が無効
  - **Network access: Do not allow anonymous enumeration of SAM accounts GPO**と**Network access: Do not allow anonymous enumeration of SAM accounts and shares GPO**の両方が無効
- **制限されたグループ**  
制限されたグループを設定して、組込みグループやユーザ定義グループのメンバーを集中管理することができます。グループ ポリシーを通して制限されたグループを適用する場合、CIFSサーバ ローカル グループのメンバーは、適用されるグループ ポリシーで定義されているメンバー リスト設定に一致するように自動的に設定されます。

**Restricted Groups** GPOを使用して設定します。

- 集約型アクセス ポリシーの設定  
集約型アクセス ポリシーのリストを指定します。集約型アクセス ポリシーと関連付けられた集約型アクセス ポリシー ルールによって、SVM上の複数のファイルに対するアクセス権が決定されます。

#### 関連コンセプト

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)  
[FlexVolを備えたSVMでのNASイベントの監査](#)(432ページ)  
[Kerberos認証](#)(22ページ)  
[BranchCacheを使用したブランチ オフィスでのSMB共有のコンテンツのキャッシュ](#)(344ページ)  
[SMB署名を使用したネットワーク セキュリティの強化](#)(87ページ)  
[トラバース チェックのバイパスの設定](#)(242ページ)

#### 関連タスク

[CIFSサーバ上でのGPOサポートの有効化と無効化](#)(120ページ)  
[CIFSサーバのKerberosセキュリティ設定の変更](#)(83ページ)  
[匿名ユーザに対するアクセス制限の設定](#)(76ページ)

### CIFSサーバでGPOを使用するための要件

CIFSサーバでグループ ポリシー オブジェクト(GPO)を使用するには、いくつかの要件を満たしている必要があります。

- クラスタでCIFSのライセンスが有効になっている必要があります。
- CIFSサーバが設定され、Windows Active Directoryドメインに追加されている必要があります。
- CIFSサーバ管理ステータスがオンである必要があります。
- GPOが設定され、CIFSサーバ コンピュータ オブジェクトを含むWindows Active Directoryの組織単位(OU)に適用されている必要があります。
- CIFSサーバでGPOのサポートが有効になっている必要があります。

### CIFSサーバ上でのGPOサポートの有効化と無効化

CIFSサーバ上でGroup Policy Object(GPO;グループ ポリシー オブジェクト)のサポートを有効または無効にできます。CIFSサーバ上でGPOのサポートを有効にすると、グループ ポリシーで定義されている該当するGPO(この場合は、CIFSサーバ コンピュータ オブジェクトを含むOUに適用されるポリシー)がCIFSサーバに適用されます。

#### 手順

1. 次のいずれかを実行します。

| 状況        | 入力するコマンド                                                                             |
|-----------|--------------------------------------------------------------------------------------|
| GPOを有効にする | <code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>  |
| GPOを無効にする | <code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code> |

2. GPOサポートが指定した状態になっていることを確認します。

```
vserver cifs group-policy show -vserver vserver_name
```



**例**

次の例では、Storage Virtual Machine (SVM、旧Vserver) vs1上でGPOサポートを有効にします。

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled
cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```

**関連コンセプト**

- [サポートされるGPO\(116ページ\)](#)
- [CIFSサーバでGPOを使用するための要件\(120ページ\)](#)
- [CIFSサーバでのGPOの更新方法\(121ページ\)](#)

**関連タスク**

- [CIFSサーバでのGPO設定の手動更新\(122ページ\)](#)
- [GPO設定に関する情報の表示\(122ページ\)](#)

**CIFSサーバでのGPOの更新方法**

デフォルトでは、Data ONTAPはGroup Policy Object (GPO; グループ ポリシー オブジェクト) の変更を90分に1回取得して適用します。セキュリティ設定は16時間に1回更新されます。Data ONTAPで自動的に更新される前にGPOを更新し、新しいGPOポリシー設定を適用するには、Data ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーします。

- デフォルトで、すべてのGPOを90分に1回確認し、必要に応じて更新。  
この間隔は設定可能で、「**更新間隔**」および「**ランダム オフセット**」GPO設定を使用して設定できます。

Data ONTAPは、GPOの変更がないかどうかをActive Directoryに照会します。Active Directoryに記録されているGPOのバージョン番号がCIFSサーバ上のGPOのバージョン番号より大きい場合、Data ONTAPは新しいGPOを取得して適用します。バージョン番号が同じ場合、CIFSサーバ上のGPOは更新されません。
- セキュリティ設定のGPOを16時間に1回更新。  
Data ONTAPは、変更の有無にかかわらず、16時間に1回セキュリティ設定のGPOを取得して適用します。

**注:** デフォルト値の16時間は、現在のData ONTAPバージョンでは変更できません。これはWindowsクライアントのデフォルト設定です。
- Data ONTAPコマンドを使用して手動ですべてのGPOを更新。  
このコマンドは、Windowsのgpupdate.exe /forceコマンドの出力結果を模しています。

**関連タスク**

- [CIFSサーバでのGPO設定の手動更新\(122ページ\)](#)

**GPOの更新が失敗した場合の対応**

一部の環境下では、Windows Server 2012ドメイン コントローラからのグループ ポリシー オブジェクト (GPO) の更新が失敗し、vserver cifs group-policy show-definedコマンドの出力

Cental Access Policy Settingsセクションに何も表示されない場合があります。この問題が発生した場合の修正方法を知っておく必要があります。

| 原因                                                                                                                                                                                                                                                                                                                                                           | 対処方法                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>clustered Data ONTAPがGPOの更新のためにWindows Server 2012ドメイン コントローラに接続する際に、error 0xc000000bd (NT STATUS_DUPLICATE_NAME)エラーが発生して接続が失敗する場合があります。</p> <p>このエラーは、接続するサーバの名前がCIFSサーバのNetBIOS名と異なる場合に発生します。これは、エイリアスを使用しているなど、さまざまな理由で発生します。また、clustered Data ONTAPは、ドメイン コントローラに接続する際に、NetBIOS名を名前の長さが15文字になるように空白を追加します。これによって、CIFSサーバ名とNetBIOS名が違ってしまう場合があります。</p> | <ol style="list-style-type: none"> <li>1. Windowsサーバで次のレジストリ キーに値1を設定し、NetBIOS名のチェックを無効にします。<br/> "HKEY_LOCAL_MACHINE\System<br/> \CurrentControlSet\Services<br/> \LanmanServer\Parameters<br/> \DisableStrictNameChecking"<br/> このレジストリ キーの設定について詳しくは、Microsoft KBの記事281308をご覧ください。<br/> <a href="#">Microsoftのサポート記事281308:「Connecting to SMB share on a Windows 2000-based computer or a Windows Server 2003-based computer may not work with an alias name」</a></li> <li>2. ドメイン コントローラをリブートします。</li> </ol> |

## CIFSサーバでのGPO設定の手動更新

CIFSサーバのGroup Policy Object (GPO; グループ ポリシー オブジェクト) 設定を直ちに更新するには、設定を手動で更新します。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

### 手順

1. 適切な操作を実行します。

| 更新する項目    | 入力するコマンド                                                                                             |
|-----------|------------------------------------------------------------------------------------------------------|
| 変更したGPO設定 | <code>vserver cifs group-policy update -vserver vserver_name</code>                                  |
| すべてのGPO設定 | <code>vserver cifs group-policy update -vserver vserver_name -force-reapply-all-settings true</code> |

### 関連コンセプト

[CIFSサーバでのGPOの更新方法](#) (121ページ)

## GPO設定に関する情報の表示

Active Directoryで定義されているグループ ポリシー オブジェクト (GPO) 設定およびCIFSサーバに適用されているGPO設定に関する情報を表示できます。

### タスク概要

CIFSサーバが属するドメインのActive Directoryで定義されているすべてのGPO設定に関する情報を表示するか、またはCIFSサーバに適用されているGPO設定のみにに関する情報を表示することができます。

### 手順

1. 次のいずれかの操作を実行し、GPO設定に関する情報を表示します。

---

**情報を表示するグループポリシー設定    入力するコマンド**


---

Active Directoryで定義されている    **vserver cifs group-policy show-defined -vserver vserver\_name**

---

CIFS対応のStorage Virtual Machine (SVM)に適用されている    **vserver cifs group-policy show-applied -vserver vserver\_name**

---

**例**

次の例では、FlexVolを備えたCIFS対応のvs1という名前のSVMが属するActive Directoryで定義されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----
      GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache : version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
  Central Access Policy Settings:
    Policies: cap1
              cap2

      GPO Name: Resultant Set of Policy
      Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication for Mode BranchCache: per-share
  Hash Version Support for BranchCache: version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
```

```

        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age: 7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
    Central Access Policy Settings:
        Policies: cap1
        cap2

```

次の例では、CIFS対応のSVM vs1に適用されているGPO設定を表示します。

```

cluster1::> vsriver cifs group-policy show-applied -vsriver vs1

Vserver: vs1
-----
    GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
    Advanced Audit Settings:
        Object Access:
            Central Access Policy Staging: failure
    Registry Settings:
        Refresh Time Interval: 22
        Refresh Random Offset: 8
        Hash Publication Mode for BranchCache: per-share
        Hash Version Support for BranchCache: all-versions
    Security Settings:
        Event Audit and Event Log:
            Audit Logon Events: none
            Audit Object Access: success
            Log Retention Method: overwrite-as-needed
            Max Log Size: 16384
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age: 7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
        cap2

    GPO Name: Resultant Set of Policy
    Level: RSOP
    Advanced Audit Settings:

```

```

Object Access:
  Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

```

## 関連タスク

[CIFSサーバ上でのGPOサポートの有効化と無効化](#) (120ページ)

## 制限されたグループのGPOに関する詳細情報の表示

Active DirectoryでGroup Policy Object (GPO; グループ ポリシー オブジェクト)として定義されている制限されたグループ、およびCIFSサーバに適用されている制限されたグループに関する詳細情報を表示できます。

### タスク概要

デフォルトでは、次の情報が表示されます。

- グループ ポリシー名
- グループ ポリシー バージョン
- リンク

グループ ポリシーが設定されているレベルを示します。次の値が出力されます。

- **Local**: グループ ポリシーがData ONTAPで設定されているとき
- **Site**: グループ ポリシーがドメイン コントローラのサイトレベルで設定されているとき
- **Domain**: グループ ポリシーがドメイン コントローラのドメイン レベルで設定されているとき
- **OrganizationalUnit**: グループ ポリシーがドメイン コントローラのOrganizational Unit (OU; 組織単位)レベルで設定されているとき

- **RSOP**:さまざまなレベルで定義されたすべてのグループ ポリシーから派生した一連のポリシー
- 制限されたグループ名
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ
- 制限されたグループが追加されているグループの一覧  
グループはここに示されたグループ以外のグループのメンバーになることもできます。

#### 手順

1. 次のいずれかの操作を実行し、制限されたグループのすべてのGPOに関する情報を表示します。

| 情報を表示する制限されたグループのすべてのGPO | 入力するコマンド                                                                                    |
|--------------------------|---------------------------------------------------------------------------------------------|
| Active Directoryで定義されている | <b>vserver cifs group-policy restricted-group show-defined -vserver <i>vserver_name</i></b> |
| CIFSサーバに適用されている          | <b>vserver cifs group-policy restricted-group show-applied -vserver <i>vserver_name</i></b> |

#### 例

次の例では、CIFS対応のvs1という名前のSVMが属するActive Directoryドメインで定義されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-defined -vserver vs1

Vserver: vs1
-----

Group Policy Name: gpo1
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9

Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

次の例では、CIFS対応のSVM vs1に適用されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-applied -vserver vs1

Vserver: vs1
-----

Group Policy Name: gpo1
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9

Group Policy Name: Resultant Set of Policy
Version: 0
```

```

Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9

```

## 関連タスク

[GPO設定に関する情報の表示](#) (122ページ)

## 集約型アクセス ポリシーに関する情報の表示

Active Directoryで定義されている集約型アクセス ポリシーに関する詳細情報を表示できます。また、GPO(グループ ポリシー オブジェクト)を介してCIFSサーバに適用されている集約型アクセス ポリシーに関する情報も表示できます。

### タスク概要

デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセス ポリシーの名前
- SID
- 説明
- 作成時間
- 更新日時
- メンバー ルール

### 手順

1. 次のいずれかの操作を実行し、集約型アクセス ポリシーに関する情報を表示します。

情報を表示するすべての集約型アクセス ポリシー

入力するコマンド

Active Directoryで定義されている

```
vserver cifs group-policy central-access-policy
show-defined -vserver vserver_name
```

CIFSサーバに適用されている

```
vserver cifs group-policy central-access-policy
show-applied -vserver vserver_name
```

### 例

次の例では、Active Directoryで定義されているすべての集約型アクセス ポリシーの情報を表示します。

```

cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                               SID
-----
vs1      p1                                     S-1-17-3386172923-1132988875-3044489393-3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                                     S-1-17-1885229282-1100162114-134354072-822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                  r2

```

次の例では、クラスタ上のStorage Virtual Machine(SVM)に適用されているすべての集約型アクセス ポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver      Name      SID
-----
vs1          p1        S-1-17-3386172923-1132988875-3044489393-3993546205
  Description: policy #1
  Creation Time: Tue Oct 22 09:34:13 2013
  Modification Time: Wed Oct 23 08:59:15 2013
  Member Rules: r1

vs1          p2        S-1-17-1885229282-1100162114-134354072-822349040
  Description: policy #2
  Creation Time: Tue Oct 22 10:28:20 2013
  Modification Time: Thu Oct 31 10:25:32 2013
  Member Rules: r1
               r2
```

## 関連コンセプト

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)

## 関連タスク

[GPO設定に関する情報の表示](#)(122ページ)

[集約型アクセス ポリシー ルールに関する情報の表示](#)(128ページ)

## 集約型アクセス ポリシー ルールに関する情報の表示

Active Directoryで定義されている集約型アクセス ポリシーに関連付けられた集約型アクセス ポリシー ルールに関する詳細情報を表示できます。また、集約型アクセス ポリシーのGPO(グループ ポリシー オブジェクト)を介してCIFSサーバに適用されている集約型アクセス ポリシー ルールに関する情報も表示できます。

### タスク概要

定義されているか適用されている集約型アクセス ポリシー ルールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセス ポリシー ルールの名前
- 説明
- 作成時間
- 更新日時
- 現在の権限
- 推奨される権限
- ターゲット リソース

### 手順

1. 次のいずれかの操作を実行し、すべての集約型アクセス ポリシー ルールに関する情報を表示します。



集約型アクセス ポリシーに関連付けられた、情報を表示するすべての集約型アクセス ポリシー ルール

入力するコマンド

Active Directoryで定義されている

**vserver cifs group-policy central-access-rule show-defined -vserver vserver\_name**

CIFSサーバに適用されている

**vserver cifs group-policy central-access-rule show-applied -vserver vserver\_name**

## 例

次の例では、Active Directoryで定義されている集約型アクセス ポリシーに関連付けられたすべての集約型アクセス ポリシー ルールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: 0:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: 0:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: 0:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: 0:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

次の例では、クラスタ上でStorage Virtual Machine(SVM)に適用されている集約型アクセス ポリシーに関連付けられたすべての集約型アクセス ポリシー ルールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: 0:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: 0:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: 0:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: 0:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

## 関連コンセプト

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)

## 関連タスク

[GPO設定に関する情報の表示](#)(122ページ)

[集約型アクセス ポリシーに関する情報の表示](#)(127ページ)

## CIFSサーバのコンピュータ アカウント パスワードの変更

CIFSサーバのコンピュータ アカウント パスワードは、手動で変更することも、リセットして変更することもできます。また、パスワードを自動的に更新するようにCIFSサーバでスケジュールを設定することもできます。

### 関連タスク

[コンピュータ アカウント パスワードの自動変更のためのCIFSサーバの設定](#) (130ページ)

## ドメイン アカウント パスワードの変更またはリセット

Storage Virtual Machine (SVM) 上のCIFSサーバには、Active Directoryドメイン アカウントが割り当てられています。セキュリティ強化のためにこのアカウントのパスワードを変更したり、パスワードを忘れた場合にパスワードをリセットしたりできます。

### 手順

1. 次のいずれかの操作を実行します。

| 状況または条件                  | 使用するコマンド                                         |
|--------------------------|--------------------------------------------------|
| パスワードがわかっている場合に<br>変更する  | <code>vserver cifs domain password change</code> |
| パスワードがわからない場合に<br>リセットする | <code>vserver cifs domain password reset</code>  |

詳細については、各コマンドのマニュアル ページを参照してください。

## コンピュータ アカウント パスワードの自動変更のためのCIFSサーバの設定

セキュリティを強化するために、Windows Active Directoryのコンピュータ アカウント パスワードをスケジュールに従って自動的に変更するようにCIFSサーバを設定することができます。デフォルトでは、パスワード変更スケジュールは無効になっています。

### 手順

1. スケジュールを設定して自動コンピュータ アカウント パスワード変更を有効にするには、次を実行します。

```
vserver cifs domain password schedule modify -vserver vserver_name -is-schedule-enabled true -schedule-weekly-interval integer -schedule-randomized-minute integer -schedule-day-of-week cron_dayofweek -schedule-time-of-day HH:MM:SS
```

-schedule-weekly-intervalは、何週間後にスケジュールされたドメイン アカウント パスワードの変更を実行するかを指定します。

-schedule-randomized-minuteは、何分後にスケジュールされたドメイン アカウント パスワードの変更を開始するかを指定します。

-schedule-day-of-weekは、何曜日にスケジュールされたドメイン アカウント パスワードの変更を実行するかを設定します。

-schedule-time-of-dayは、スケジュールされたドメイン アカウント パスワードの変更を開始する時間をHH:MM:SSで設定します。

**例**

```
vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled true -schedule-randomized-minute 120 -schedule-weekly-interval 4 -schedule-day-of-week sunday -schedule-time-of-day 23:00:00
```

2. パスワードのスケジュールが正しく設定され、有効になっていることを確認します。

```
vserver cifs domain password schedule show -vserver vserver_name
```

**例**

```
vserver cifs domain password schedule show -vserver vs1
```

```

Vserver: vs1
Is Password Change Schedule Enabled: true
Interval in Weeks for Password Change Schedule: 4
Minutes Within Which Schedule Start Can be Randomized: 120
Last Successful Password Change/Reset Time: -
Schedule Description: Sun@23:00
Warning Message in Case Job Is Deleted: -

```

**関連コンセプト**

[CIFSサーバのコンピュータアカウントパスワードの変更](#)(130ページ)

**関連タスク**

[CIFSサーバでのコンピュータアカウントパスワードの自動変更の無効化](#)(131ページ)

**CIFSサーバでのコンピュータ アカウント パスワードの自動変更の無効化**

CIFSサーバのコンピュータ アカウント パスワードの自動変更を停止するには、スケジュールされた変更を無効にします。

**手順**

1. vserver cifs domain password schedule modifyコマンドを使用して、コンピュータ アカウント パスワードの自動変更を無効にします。

**例**

```
vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled false
```

2. vserver cifs domain password schedule showコマンドを使用して、パスワードのスケジュールが無効になったことを確認します。

**例**

```
vserver cifs domain password schedule show -vserver vs1
```

```

Vserver: vs1
Is Password Change Schedule Enabled: false
Interval in Weeks for Password Change Schedule: 4
Minutes Within Which Schedule Start Can be Randomized: 120
Last Successful Password Change/Reset Time: -
Schedule Description: Sun@23:00
Warning Message in Case Job Is Deleted: -

```

## ドメイン コントローラ接続の管理

ドメイン コントローラ接続の管理では、次のような作業を実行できます。現在検出されているLDAPサーバとドメイン コントローラサーバに関する情報の表示、LDAPサーバとドメイン コントローラサーバの再設定および再検出、推奨するドメイン コントローラについてのリストの管理、現在構成されている推奨するドメイン コントローラについての情報の表示。

### 検出されたサーバに関する情報の表示

CIFSサーバで検出されたLDAPサーバおよびドメイン コントローラに関する情報を表示できます。

#### 手順

1. 検出されたサーバに関する情報を表示するには、次のコマンドを入力します。

```
vserver cifs domain discovered-servers show
```

#### 例

次の例では、SVM vs1で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

| Domain Name | Type    | Preference | DC-Name | DC-Address | Status |
|-------------|---------|------------|---------|------------|--------|
| example.com | MS-LDAP | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-LDAP | adequate   | DC-2    | 1.1.3.5    | OK     |
| example.com | MS-DC   | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-DC   | adequate   | DC-2    | 1.1.3.5    | OK     |

#### 関連タスク

[サーバのリセットおよび再検出](#) (132ページ)

[CIFSサーバの停止と起動](#) (139ページ)

### サーバのリセットおよび再検出

CIFSサーバでサーバのリセットと再検出を行うと、LDAPサーバおよびドメイン コントローラに関するCIFSサーバに格納されている情報が破棄されます。サーバの情報が破棄されたあと、それらの外部サーバに関する最新の情報が再取得されます。これは、接続されているサーバが適切に応答しない場合に役立ちます。

#### 手順

1. 次のコマンドを入力します。

```
vserver cifs domain discovered-servers reset-servers -vserver  
vserver_name
```

2. 再検出されたサーバに関する新しい情報を表示します。

```
vserver cifs domain discovered-servers show -vserver vserver_name
```

**例**

次の例では、Storage Virtual Machine (SVM、旧Vserver) vs1のサーバをリセットして再検出します。

```
cluster1::> vserver cifs domain discovered-servers reset-servers -
vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
Vserver: vs1
```

| Domain Name | Type    | Preference | DC-Name | DC-Address | Status |
|-------------|---------|------------|---------|------------|--------|
| example.com | MS-LDAP | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-LDAP | adequate   | DC-2    | 1.1.3.5    | OK     |
| example.com | MS-DC   | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-DC   | adequate   | DC-2    | 1.1.3.5    | OK     |

**関連タスク**

[検出されたサーバに関する情報の表示](#) (132ページ)

[CIFSサーバの停止と起動](#) (139ページ)

**優先ドメイン コントローラの追加**

Data ONTAPでは、DNSを介してドメイン コントローラが自動的に検出されます。必要に応じて、特定のドメインに対する優先ドメイン コントローラのリストに、1つ以上のドメイン コントローラを追加できます。

**タスク概要**

優先ドメイン コントローラ リストがすでに特定のドメインに存在する場合、新しいリストが既存のリストに統合されます。

**手順**

1. 優先ドメイン コントローラのリストに追加するには、次のコマンドを入力します。

```
vserver cifs domain preferred-dc add -vserver vserver_name -domain
domain_name -preferred-dc IP_address, ...
```

-vserver *vserver\_name*には、Storage Virtual Machine (SVM) 名を指定します。

-domain *domain\_name*には、特定のドメイン コントローラが属するドメインの完全修飾Active Directory名を指定します。

-preferred-dc *IP\_address,...*には、優先ドメイン コントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

**例**

次のコマンドでは、cifs.lab.example.comドメインへの外部アクセスを管理するためにSVM vs1上のCIFSサーバで使用する優先ドメイン コントローラのリストに、ドメイン コントローラ 172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

**関連参照情報**

[優先されるドメイン コントローラの管理用コマンド](#)(134ページ)

**優先されるドメイン コントローラの管理用コマンド**

優先ドメインコントローラの追加、表示、削除を行うコマンドについて説明します。

| 状況                | 使用するコマンド                                             |
|-------------------|------------------------------------------------------|
| 優先ドメインコントローラを追加する | <code>vserver cifs domain preferred-dc add</code>    |
| 優先ドメインコントローラを表示する | <code>vserver cifs domain preferred-dc show</code>   |
| 優先ドメインコントローラを削除する | <code>vserver cifs domain preferred-dc remove</code> |

詳細については、各コマンドのマニュアル ページを参照してください。

**関連タスク**

[優先ドメイン コントローラの追加](#)(133ページ)

**CIFSサーバ用のNetBIOSエイリアスの管理**

NetBIOSエイリアスは、SMBクライアントがCIFSサーバに接続する際に使用できるCIFSサーバの別名です。CIFSサーバのNetBIOSエイリアスを設定すると、他のファイル サーバのデータをCIFSサーバに統合して、CIFSサーバが元のファイル サーバの名前に応答するようにする場合に役立ちます。

CIFSサーバの作成時またはCIFSサーバ作成後の任意の時点で、NetBIOSエイリアスのリストを指定できます。リストへのNetBIOSエイリアスの追加や削除は、いつでも行うことができます。CIFSサーバにはNetBIOSエイリアス リスト内のどの名前を使用しても接続できます。

**関連コンセプト**

[CIFSサーバのセットアップ](#)(50ページ)

**関連タスク**

[NetBIOS over TCP接続に関する情報の表示](#)(142ページ)

**CIFSサーバへのNetBIOSエイリアスのリストの追加**

エイリアスを使用してSMBクライアントをCIFSサーバに接続する場合、NetBIOSエイリアスのリストを作成するか、NetBIOSエイリアスの既存のリストにNetBIOSエイリアスを追加します。

**タスク概要**

- NetBIOSエイリアス名は15文字以内にする必要があります。
- CIFSサーバには最大200個までのNetBIOSエイリアスを設定できます。
- 次の文字は使用できません。

@ # \* ( ) = + [ ] | ; : " , < > \ / ?

手順

1. NetBIOSエイリアスを追加します。

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases  
NetBIOS_alias,...
```

例

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- 各エイリアスをカンマで区切り、1つまたは複数のNetBIOSエイリアスを指定します。
- 指定したNetBIOSエイリアスが既存のリストに追加されます。
- 現在のリストが空である場合、NetBIOSエイリアスの新しいリストが作成されます。

2. NetBIOSエイリアスが正しく追加されたことを確認します。

```
vserver cifs show -vserver vserver_name -display-netbios-aliases
```

例

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1  
  
Server Name: CIFS_SERVER  
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

関連タスク

[NetBIOSエイリアス リストからのNetBIOSエイリアスの削除](#)(135ページ)

[CIFSサーバのNetBIOSエイリアスのリストの表示](#)(136ページ)

## NetBIOSエイリアス リストからのNetBIOSエイリアスの削除

CIFSサーバで特定のNetBIOSエイリアスが不要な場合、そのNetBIOSエイリアスをリストから削除できます。リストからすべてのNetBIOSエイリアスを削除することもできます。

タスク概要

カンマで区切ったリストを使用して複数のNetBIOSエイリアスを削除することもできます。`-netbios-aliases`パラメータの値に`-`を指定すると、CIFSサーバのすべてのNetBIOSエイリアスを削除できます。

手順

1. 次のいずれかを実行します。

| 削除する項目                | コマンド                                                                                                    |
|-----------------------|---------------------------------------------------------------------------------------------------------|
| リスト内の特定のNetBIOSエイリアス  | <b>vserver cifs remove-netbios-aliases -vserver<br/>vserver_name -netbios-aliases NetBIOS_alias,...</b> |
| リスト内のすべてのNetBIOSエイリアス | <b>vserver cifs remove-netbios-aliases -vserver<br/>vserver_name -netbios-aliases -</b>                 |

例

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1
```

2. 指定したNetBIOSエイリアスが削除されたことを確認します。

```
vserver cifs show -vserver vserver_name -display-netbios-aliases
```

#### 例

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
    Server Name: CIFS_SERVER
    NetBIOS Aliases: ALIAS_2, ALIAS_3
```

## CIFSサーバのNetBIOSエイリアスのリストの表示

NetBIOSエイリアスのリストを表示できます。これは、SMBクライアントがCIFSサーバへの接続に使用できる名前を確認するときに役立ちます。

#### 手順

1. 次のいずれかを実行します。

| 表示する情報                          | コマンド                                              |
|---------------------------------|---------------------------------------------------|
| CIFSサーバのNetBIOSエイリアス            | <b>vserver cifs show -display-netbios-aliases</b> |
| NetBIOSエイリアスのリストを含む詳細なCIFSサーバ情報 | <b>vserver cifs show -instance</b>                |

#### 例

次の例では、CIFSサーバのNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1
    Server Name: CIFS_SERVER
    NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

次の例では、NetBIOSエイリアスのリストを含む詳細なCIFSサーバ情報を表示します。

```
vserver cifs show -instance
```

```
Vserver: vs1
    CIFS Server NetBIOS Name: CIFS_SERVER
    NetBIOS Domain/Workgroup Name: EXAMPLE
    Fully Qualified Domain Name: EXAMPLE.COM
    Default Site Used by LIFs Without Site Membership:
        Authentication Style: domain
    CIFS Server Administrative Status: up
    CIFS Server Description:
        List of NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

詳細については、各コマンドのマニュアル ページを参照してください。

#### 関連タスク

[CIFSサーバへのNetBIOSエイリアスのリストの追加](#) (134ページ)



## 関連参照情報

[CIFSサーバの管理用コマンド](#) (142ページ)

## SMBクライアントがNetBIOSエイリアスを使用して接続しているかどうかの確認

SMBクライアントがNetBIOSエイリアスを使用して接続しているかどうか、また、使用している場合はそのNetBIOSエイリアスを確認できます。この情報は、接続の問題のトラブルシューティングを行う場合に役立ちます。

### タスク概要

SMB接続に関連付けられたNetBIOSエイリアスを表示するには、`-instance`パラメータを使用します。CIFSサーバ名またはIPアドレスを使用してSMB接続を行っている場合、NetBIOS Nameフィールドの出力は`-`(ハイフン)になります。

### 手順

1. 次のうち必要な操作を実行します。

| 表示するNetBIOS情報             | コマンド                                                                                |
|---------------------------|-------------------------------------------------------------------------------------|
| SMB接続                     | <code>vserver cifs sessions show -instance</code>                                   |
| 指定したNetBIOSエイリアスを使用している接続 | <code>vserver cifs sessions show -instance -netbios-name <i>netbios_name</i></code> |

### 例

次の例では、セッションID 1のSMB接続に使用されているNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

## CIFSサーバに関するその他のタスクの管理

CIFSサーバへのSMBアクセスの終了や再開、ドメイン アカウント パスワードの変更やリセット、CIFSサーバの別のOUへの移動、CIFSサーバのドメインの変更、NetBIOS over TCP接続の情報の表示、CIFSサーバについての情報の変更や表示、CIFSサーバの削除を行うことができます。

また、デフォルトUNIXユーザも設定できます。

## SVMのプロトコルの変更

Storage Virtual Machine (SVM) の NFS や SMB を構成して使用する前に、SVM のプロトコルを有効にする必要があります。この作業は通常、SVM のセットアップ時に実行します。ただし、セットアップ時に SVM のプロトコルを有効にしなかった場合でも、`vserver add-protocols` コマンドを使用して、あとからこのプロトコルを有効にできます。

### タスク概要

`vserver remove-protocols` コマンドを使用して、SVM 上のプロトコルを無効にすることもできます。

### 手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルをチェックします。

```
vserver show -vserver vserver_name -protocols
```

`vserver show-protocols` コマンドを使用して、クラスタ内のすべての SVM で現在有効になっているプロトコルを表示することもできます。

2. 次のいずれかを実行します。

| 状況          | 入力するコマンド                                                                                           |
|-------------|----------------------------------------------------------------------------------------------------|
| プロトコルを有効にする | <b>vserver add-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]</b>    |
| プロトコルを無効にする | <b>vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]</b> |

詳細については、各コマンドのマニュアル ページを参照してください。

3. 許可するプロトコルと許可しないプロトコルが正しく更新されたことを確認します。

```
vserver show -vserver vserver_name -protocols
```

### 例

次のコマンドは、`vs1` という SVM で現在有効になっているプロトコルと無効になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1 -protocols
Vserver      Allowed Protocols      Disallowed Protocols
-----
vs1          nfs                     cifs, fcp, iscsi, ndmp
```

次のコマンドは、`vs1` という SVM で有効になっているプロトコルのリストに `cifs` を追加することで、SMB 経由のアクセスを許可します。

```
vs1::> vserver add-protocols -vserver vs1 -protocols cifs
```

### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver add-protocols - Add protocols to the Vserver](#)

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver remove-protocols - Remove protocols from the Vserver](#)

# CIFSサーバの停止と起動

ユーザがSMB共有を介してデータにアクセスしていない間に作業を行う場合は、SVM上のCIFSサーバを停止すると便利です。SMBアクセスを再開するときは、CIFSサーバを起動します。CIFSサーバを停止することによって、Storage Virtual Machine (SVM) で許可されているプロトコルを変更できます。

## タスク概要

注: CIFSサーバを停止すると、確立していたSMBセッションは終了され、開いていたファイルが閉じられます。ワークステーションにデータがキャッシュされている場合、それらの変更を保存できなくなるため、データが失われる可能性があります。

## 手順

1. 次のいずれかを実行します。

| 状況           | 入力するコマンド                                                                         |
|--------------|----------------------------------------------------------------------------------|
| CIFSサーバを停止する | <code>vserver cifs stop -vserver vserver_name [-foreground {true false}]</code>  |
| CIFSサーバを起動する | <code>vserver cifs start -vserver vserver_name [-foreground {true false}]</code> |

-foregroundは、コマンドをフォアグラウンドとバックグラウンドのどちらで実行するかを指定するパラメータです。省略した場合、このパラメータは trueに設定され、フォアグラウンドでコマンドが実行されます。

2. `vserver cifs show`コマンドを使用して、CIFSサーバの管理ステータスが正しいことを確認します。

### 例

次に、SVM vs1でCIFSサーバを起動するコマンドの例を示します。

```
cluster1::> vserver start -vserver vs1
cluster1::> vserver cifs show -vserver vs1
Vserver: vs1
CIFS Server NetBIOS Name: VS1
NetBIOS Domain/Workgroup Name: DOMAIN
Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
```

## 関連タスク

- [検出されたサーバに関する情報の表示](#)(132ページ)
- [サーバのリセットおよび再検出](#)(132ページ)

## 別のOUへのCIFSサーバの移動

CIFSサーバのcreateプロセスでは、別のOrganizational Unit (OU;組織単位)を指定しないかぎり、セットアップ時のデフォルトのOUであるCN=Computersが使用されます。CIFSサーバはセットアップ後でも別のOUに移動できます。

### 手順

1. Windowsサーバ上で、[Active Directoryユーザーとコンピュータ]ツリーを開きます。
2. Storage Virtual Machine (SVM) のActive Directoryオブジェクトを見つけます。
3. 該当オブジェクトを右クリックし、[移動]を選択します。
4. SVMに関連付けるOUを選択します。

### タスクの結果

選択したOUに、SVMオブジェクトが移動します。

### 関連コンセプト

[CIFSサーバのセットアップ](#) (50ページ)

## CIFSサーバ移動前のSVM上の動的DNSドメインの変更

CIFSサーバを別のドメインに移動する際に、CIFSサーバのDNSレコードがActive Directoryに統合されたDNSサーバによってDNSに動的に登録されるようにするには、CIFSサーバを移動する前にStorage Virtual Machine (SVM) 上の動的DNS (DDNS) を変更する必要があります。

### 開始する前に

新しいドメイン (CIFSサーバコンピュータ アカウントの移動先) のサービス ロケーション レコードを含むDNSドメインを使用するよう、SVM上のDNSネーム サービスを変更する必要があります。セキュアDDNSを使用している場合は、Active Directoryに統合されたDNSネーム サービスを使用する必要があります。

### タスク概要

DDNS (SVM上で設定されている場合) はデータLIFのDNSレコードを新しいドメインに自動的に追加しますが、元のドメインのDNSレコードは元のDNSサーバから自動的に削除されません。手動で削除する必要があります。

### 手順

1. SVM上のDDNSドメインを変更します。

```
vserver services name-service dns dynamic-update modify -vserver
vserver_name -is-enabled true -use-secure {true|false} -domain-name
FQDN_used_for_DNS_updates
```

#### 例

```
vserver services name-service dns dynamic-update modify -vserver vs1 -
is-enabled true -use-secure true -domain-name example2.com
```

2. DDNS設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

**例**

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Domain Name  | TTL |
|---------|------------|------------|--------------|-----|
| vs1     | true       | true       | example2.com | 24h |

**SVMのActive Directoryドメインへの参加**

vserver cifs modifyコマンドでドメインを変更すると、既存のCIFSサーバを削除することなく Storage Virtual Machine (SVM) を Active Directoryドメインに参加させることができます。現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

**開始する前に**

- SVMのDNS設定が完了している必要があります。
- SVMを新しいドメインに追加する前に、対象のドメインでSVMのDNS設定が行われていることを確認する必要があります。  
DNSサーバに、ドメインLDAPおよびドメイン コントローラ サーバのサービス ロケーション レコード (SRV) が格納されている必要があります。

**タスク概要**

- Active Directoryドメインの変更を実行するには、CIFSサーバの管理ステータスが「down」に設定されている必要があります。
- コマンドの実行が成功すると、管理ステータスが自動的に「up」に設定されます。
- ドメインに追加する場合、このコマンドの実行には数分かかることがあります。

**手順**

1. 次のコマンドを実行し、SVMをCIFSサーバドメインに追加します。

```
vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down
```

詳細については、vserver cifs modifyコマンドのマニュアル ページを参照してください。新しいドメイン用にDNSを再設定する必要がある場合は、vserver dns modifyコマンドのマニュアル ページを参照してください。

2. 次のコマンドで、CIFSサーバが目的のActive Directoryドメイン内にあることを確認します。

```
vserver cifs show
```

**例**

次の例では、SVM vs1上にあるCIFSサーバ「CIFSSERVER1」をexample2.comドメインに追加します。

```
cluster1::> vserver cifs modify -vserver vs1 -domain example2.com -status-admin down
cluster1::> vserver cifs show
```

| Vserver | Server Name | Status Admin | Domain/Workgroup Name | Authentication Style |
|---------|-------------|--------------|-----------------------|----------------------|
| vs1     | CIFSSERVER1 | up           | EXAMPLE2              | domain               |

## 関連コンセプト

[CIFSサーバのセットアップ](#)(50ページ)

## NetBIOS over TCP接続に関する情報の表示

NetBIOS over TCP (NBT) 接続に関する情報を表示できます。この情報は、NetBIOSに関連する問題のトラブルシューティングを行う場合に役立ちます。

### 手順

1. `vserver cifs nbtstat` コマンドを使用して、NetBIOS over TCP 接続に関する情報を表示します。

注: IPv6経由のNetBIOSネーム サービス(NBNS)はサポートされていません。

### 例

次の例では、「cluster1」のNetBIOSネーム サービスに関する情報を表示します。

```
cluster1::> vserver cifs nbtstat

Vserver: vs1
Node:    cluster1-01
Interfaces:
    10.10.10.32
    10.10.10.33

Servers:
    17.17.1.2 (active )
NBT Scope:
[ ]
NBT Mode:
[h]
NBT Name  NetBIOS Suffix  State  Time Left  Type
-----
CLUSTER_1  00              wins   57          -----
CLUSTER_1  20              wins   57

Vserver: vs1
Node:    cluster1-02
Interfaces:
    10.10.10.35
Servers:
    17.17.1.2 (active )
CLUSTER_1  00              wins   58
CLUSTER_1  20              wins   58
4 entries were displayed.
```

## CIFSサーバの管理用コマンド

CIFSサーバを作成、表示、変更、停止、開始、削除するコマンドを知っておく必要があります。また、サーバのリセットと再検出、マシン アカウント パスワードの変更またはリセット、マシン アカウント パスワードのスケジュール変更、NetBIOSエイリアスの追加や削除を行うコマンドもあります。

| 状況                 | 使用するコマンド                         |
|--------------------|----------------------------------|
| CIFSサーバを作成する       | <code>vserver cifs create</code> |
| CIFSサーバに関する情報を表示する | <code>vserver cifs show</code>   |

| 状況                                   | 使用するコマンド                                                          |
|--------------------------------------|-------------------------------------------------------------------|
| CIFSサーバを変更する                         | <code>vserver cifs modify</code>                                  |
| CIFSサーバを別のドメインに移動する                  | <code>vserver cifs modify</code>                                  |
| CIFSサーバを停止する                         | <code>vserver cifs stop</code>                                    |
| CIFSサーバを開始する                         | <code>vserver cifs start</code>                                   |
| CIFSサーバを削除する                         | <code>vserver cifs delete</code>                                  |
| CIFSサーバ用にサーバをリセットおよび再検出する            | <code>vserver cifs domain discovered-servers reset-servers</code> |
| CIFSサーバのマシン アカウント パスワードを変更する         | <code>vserver cifs domain password change</code>                  |
| CIFSサーバのマシン アカウント パスワードをリセットする       | <code>vserver cifs domain password reset</code>                   |
| CIFSサーバのマシン アカウントの自動パスワード変更をスケジュールする | <code>vserver cifs domain password schedule modify</code>         |
| CIFSサーバ用のNetBIOSエイリアスを追加する           | <code>vserver cifs add-netbios-aliases</code>                     |
| CIFSサーバ用のNetBIOSエイリアスを削除する           | <code>vserver cifs remove-netbios-aliases</code>                  |

詳細については、各コマンドのマニュアル ページを参照してください。

#### 関連コンセプト

[CIFSサーバのセットアップ](#)(50ページ)

[CIFSサーバを削除したときにローカル ユーザとローカル グループが受ける影響](#)(219ページ)

## SMBアクセスとCIFSサービスでのIPv6の使用

Data ONTAP 8.2以降では、SMBクライアントからIPv6ネットワーク経由でStorage Virtual Machine (SVM) のファイルにアクセスでき、IPv6ネットワークでCIFSサービス通信を使用できます。

クラスタでIPv6を有効にし、データLIFを適切に設定すると、IPv6がすぐに有効になります。SVMの設定やCIFSサーバ オプションを有効化する必要はありません。

### IPv6を使用するための要件

CIFSサーバでIPv6を使用する前に、この機能をサポートするData ONTAPおよびSMBのバージョンとライセンスの要件について確認しておく必要があります。

#### Data ONTAPのバージョンとライセンスの要件

- IPv6は、Data ONTAP 8.2以降でサポートされます。  
CIFSサーバ、SMBアクセス、およびCIFSサービスの設定やIPv6をサポートする機能の設定に使用するコマンドで、パラメータとしてIPアドレスがサポートされている場合は、IPv4またはIPv6のアドレスを使用できます。同様に、IPアドレスに関する情報を表示するためのIPv6でサポートされるコマンドでは、IPv4とIPv6の両方のアドレスが表示されます。
- SMBアクセスやCIFSサービスでIPv6を使用するために特別なライセンスは必要ありませんが、CIFSのライセンスが有効になっていて、Storage Virtual Machine (SVM) にCIFSサーバが配置されている必要があります。

### SMBプロトコルのバージョン

- FlexVolを備えたSVMについては、すべてのバージョンのSMBプロトコルでIPv6がサポートされます。
- Infinite Volumeを備えたSVMについては、SMB 1.0でIPv6がサポートされます。  
Infinite Volumeを備えたSVMではSMB 2.xおよびSMB 3.0がサポートされないためです。

注: IPv6経由のNetBIOSネーム サービス (NBNS)はサポートされません。

### SMBアクセスとCIFSサービスでのIPv6のサポート

CIFSサーバ上でIPv6を使用する場合は、Data ONTAPによるSMBアクセスやCIFSサービスとのネットワーク通信でのIPv6のサポートについて確認しておく必要があります。

#### Windowsクライアントおよびサーバのサポート

Data ONTAPでは、IPv6をサポートするWindowsサーバおよびクライアントをサポートしています。  
Microsoft WindowsクライアントおよびサーバによるIPv6のサポートは次のとおりです。

- Windows XPおよびWindows 2003では、SMBファイル共有でIPv6がサポートされます。  
これらのバージョンでのIPv6のサポートは限定的なものです。
- Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012、およびそれ以降のリリースでは、SMBファイル共有とActive Directoryサービス(DNS、LDAP、CLDAP、Kerberosなどのサービス)の両方でIPv6がサポートされます。  
IPv6アドレスが設定されている場合、Windows 7、Windows Server 2008、およびそれ以降のリリースでは、Active Directoryサービスに対してデフォルトでIPv6が使用されます。IPv6接続によるNTLM認証とKerberos認証の両方がサポートされます。  
Data ONTAPでサポートされるWindowsクライアントでは、いずれもIPv6アドレスを使用してSMB共有にアクセスできます。

Data ONTAPでサポートされるWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix))を参照してください。

注: NTドメインはIPv6ではサポートされません。

#### その他のCIFSサービスのサポート

Data ONTAPでは、SMBファイル共有とActive Directoryサービスに加え、以下に対してもIPv6をサポートしています。

- クライアント側のサービス: オフライン フォルダ、移動プロファイル、フォルダ リダイレクト、以前のバージョン機能など
- サーバ側のサービス: 動的ホーム ディレクトリの有効化(ホーム ディレクトリ機能)、シンボリックリンクとワイドリンク、BranchCache、ODXコピー オフロード、自動ノード リファール、以前のバージョン機能など
- ファイル アクセス管理用のサービス: Windowsのローカル ユーザやローカル グループを使用したアクセス制御と権限の管理、CLIを使用したファイル権限や監査ポリシーの設定、セキュリティトレース、ファイル ロックの管理、SMBアクティビティの監視など
- NASのマルチプロトコルの監査
- FPolicy
- 共有の継続的な可用性、監視プロトコル、およびリモートVSS(Hyper-V over SMB構成で使用)



## ネーム サービスと認証サービスのサポート

次のネーム サービスを使用した通信がIPv6でサポートされます。

- ドメイン コントローラ
- DNSサーバ
- LDAPサーバ
- KDCサーバ
- NISサーバ

## IPv6を使用したCIFSサーバから外部サーバへの接続

要件に対応した設定を作成するには、CIFSサーバが外部サーバへの接続を確立するときにIPv6がどのように使用されるかを確認しておく必要があります。

- 送信元アドレスの選択  
外部サーバへの接続を試行する場合は、選択する送信元アドレスが宛先アドレスと同じタイプでなければなりません。たとえば、IPv6アドレスに接続する場合、CIFSサーバをホストするStorage Virtual Machine(SVM)には、送信元アドレスとして使用するIPv6アドレスを持つデータLIFまたは管理LIFが必要です。同様に、IPv4アドレスに接続する場合、SVMには、送信元アドレスとして使用するIPv4アドレスを持つデータLIFまたは管理LIFが必要です。
- DNSを使用して動的に検出されるサーバの場合、サーバ検出は次のように実行されます。
  - クラスタでIPv6が無効になっている場合は、IPv4サーバアドレスのみが検出されます。
  - クラスタでIPv6が有効になっている場合は、IPv4とIPv6の両方のサーバアドレスが検出されます。アドレスが属するサーバが適切かどうかと、IPv6またはIPv4のデータLIFまたは管理LIFが利用可能かどうかに応じて、いずれかのタイプが使用されます。

動的なサーバ検出は、ドメイン コントローラとそれに関連するサービス(LSA、NETLOGON、Kerberos、LDAPなど)を検出するために使用されます。

- DNSサーバへの接続  
SVMがDNSサーバに接続するときにIPv6を使用するかどうかは、DNSネーム サービスの設定によって決まります。IPv6アドレスを使用するようにDNSサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、DNSサーバへの接続に引き続きIPv4アドレスが使用されるようにするため、DNSネーム サービスの設定でIPv4アドレスを使用できます。DNSネーム サービスの設定時に、IPv4アドレスとIPv6アドレスを組み合わせで指定できます。
- LDAPサーバへの接続  
SVMがLDAPサーバに接続するときにIPv6を使用するかどうかは、LDAPクライアントの設定によって決まります。IPv6アドレスを使用するようにLDAPクライアントが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、LDAPサーバへの接続に引き続きIPv4アドレスが使用されるようにするため、LDAPクライアントの設定でIPv4アドレスを使用できます。LDAPクライアントの設定時に、IPv4アドレスとIPv6アドレスを組み合わせで指定できます。

**注:** LDAPクライアントの設定は、UNIXユーザ、グループ、およびネットグループのネーム サービス用にLDAPを設定するときに使用されます。

- NISサーバへの接続  
SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネーム サービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、NISサーバへの接続に引き続きIPv4アドレスが使用されるようにするため、NISネーム サービスの設定でIPv4アドレスを使用できます。NISネーム サービスの設定時に、IPv4アドレスとIPv6アドレスを組み合わせで指定できます。

注: NISネーム サービスは、UNIXユーザ、グループ、ネットグループ、およびホスト名オブジェクトを格納および管理するために使用されます。

#### 関連タスク

[SMBでのIPv6の有効化\(クラスタ管理者のみ\)](#)(146ページ)

[IPv6 SMBセッション情報の監視および表示](#)(146ページ)

## SMBでのIPv6の有効化(クラスタ管理者のみ)

IPv6ネットワークはクラスタのセットアップ時には有効になりません。SMBでIPv6を使用するには、クラスタのセットアップ後にクラスタ管理者がIPv6を有効にする必要があります。クラスタ管理者がIPv6を有効にすると、IPv6はクラスタ全体で有効になります。

#### 手順

1. IPv6を有効にします。

```
network options ipv6 modify -enabled true
```

クラスタでのIPv6の有効化、およびIPv6のLIFの設定の詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』を参照してください。

IPv6が有効になります。SMBアクセス用のIPv6データLIFを設定できます。

#### 関連タスク

[IPv6 SMBセッション情報の監視および表示](#)(146ページ)

## SMBでのIPv6の無効化方法

クラスタでIPv6を有効にするにはネットワーク オプションを使用しますが、同じコマンドを使用してSMBでのIPv6を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後にIPv6を有効にしたインターフェイスを無効にすると、IPv6は無効になります。IPv6を有効にしたインターフェイスの管理については、クラスタ管理者と連絡を取り合う必要があります。

クラスタでのIPv6の無効化の詳細については、『*clustered Data ONTAP ネットワーク管理ガイド*』を参照してください。

## IPv6 SMBセッション情報の監視および表示

IPv6ネットワークで接続されているSMBセッション情報を監視および表示できます。この情報は、IPv6 SMBセッションに関する他の有用な情報と同様、IPv6を使用して接続するクライアントを決定する上で役に立ちます。

#### 手順

1. 次のうち必要な操作を実行します。

| 目的の処理                                                 | 入力するコマンド                                                                                                                                     |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Virtual Machine (SVM) へのSMBセッションは、IPv6を使用して接続 | <pre>vserver cifs session show -vserver vserver_name -instance</pre>                                                                         |
| 特定のLIFアドレスにより、SMBセッションにIPv6を使用                        | <pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre><br><i>LIF_IP_addressはデータLIFのIPv6アドレスです。</i> |

## SMBを使用したファイル アクセスの設定

クライアントがSMBを使用してCIFS対応のStorage Virtual Machine(SVM)のファイルにアクセスできるようにするには、いくつかの手順を実行する必要があります。

### マルチプロトコル環境でのファイルとディレクトリの命名規則

ファイルとディレクトリの命名規則は、ネットワーク クライアントのオペレーティング システムとそのファイル共有のプロトコルによって異なります。

オペレーティング システムとそのファイル共有のプロトコルの種類によって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

### ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティング システムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティング システムでも有効な文字を使用します。

たとえば、UNIXを使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン(:)を使用しないでください。コロンは、MS-DOSファイル名やディレクトリ名では無効な文字となります。文字の制約はオペレーティング システムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティング システムのマニュアルを参照してください。

### clustered Data ONTAPでファイル名とディレクトリ名が作成される仕組み

clustered Data ONTAPでは、SMBクライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して2つの名前が作成され、保持されます。元の長い名前と8.3形式の名前です。

名前が8文字を超える、または拡張子が3文字を超える(ファイルの場合)ファイル名やディレクトリ名については、clustered Data ONTAPによって次のように8.3形式の名前が生成されます。

- 名前が6文字を超える場合は、元のファイル名またはディレクトリ名が6文字に切り捨てられます。
- 切り捨てによって一意でなくなったファイル名またはディレクトリ名には、チルダ(~)と1~5の数字が追加されます。  
同様の名前が6つ以上あって数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。
- ファイルの場合は、ファイル名の拡張子が3文字に切り捨てられます。

たとえば、NFSクライアントがspecifications.htmlという名前のファイルを作成すると、clustered Data ONTAPによってspecif~1.htmという8.3形式のファイル名が作成されます。この名前がすでに存在する場合は、ファイル名の最後の番号が別の番号になります。たとえば、NFSクライアントがspecifications\_new.htmlという別の名前のファイルを作成すると、specifications\_new.htmlの8.3形式の名前はspecif~2.htmになります。

### マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名について、NFSクライアントでは大文字と小文字が区別されますが、CIFSクライアントでは大文字と小文字が区別されず、同じ文字として扱われます。この違いがマル

チプロトコル環境に及ぼす影響、およびSMB共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにはどのように対処すべきかを理解しておく必要があります。

SMBクライアントでtestdirという名前のディレクトリを作成すると、SMBクライアントとNFSクライアントのどちらでもディレクトリ名はtestdirと表示されます。ただし、SMBユーザがあとでTESTDIRという名前のディレクトリを作成しようとしても、SMBクライアントではその名前がすでに存在しているとみなされるため作成できません。NFSユーザがあとでTESTDIRという名前のディレクトリを作成すると、このディレクトリ名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

NFSクライアントでは、ディレクトリ名の大文字と小文字が区別されるため、両方のディレクトリ名が作成したとおりに、testdirおよびTESTDIRと表示されます。

SMBクライアントでは、2つのディレクトリを区別するために8.3形式の名前が使用されます。1つのディレクトリには基本ファイル名が付けられます。以降のディレクトリには8.3形式の名前が割り当てられます。

- SMBクライアントでは、testdirとTESTDI~1という名前が表示されます。
- clustered Data ONTAPは、2つのディレクトリを区別するためにTESTDI~1というディレクトリ名を作成します。  
この場合、Storage Virtual Machine(SVM)での共有の作成時または変更時に共有パスを指定するときは、8.3形式の名前を使用する必要があります。

ファイルの場合も同様に、SMBクライアントでtest.txtというファイルを作成すると、SMBクライアントとNFSクライアントのどちらでもファイル名はtest.txtと表示されます。ただし、SMBユーザがあとでTest.txtというファイルを作成しようとしても、SMBクライアントではその名前がすでに存在しているとみなされるため作成できません。NFSユーザがあとでTest.txtという名前のファイルを作成すると、このファイル名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

NFSクライアントでは、ファイル名の大文字と小文字が区別されるため、両方のファイル名が作成したとおりにtest.txtおよびText.txtと表示されます。

SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。一方のファイルには基本ファイル名が付けられます。追加のファイルには、8.3形式のファイル名が割り当てられます。

- SMBクライアントでは、test.txtとTEST~1.TXTという名前が表示されます。
- clustered Data ONTAPは、2つのファイルを区別するためにTEST~1.TXTというファイル名を作成します。

## セキュリティ形式の設定

FlexVolボリュームおよびqtreeのセキュリティ形式を設定することで、アクセスを制御するためにData ONTAPが使用するアクセス権のタイプや、そのアクセス権を変更できるクライアントタイプを決定できます。

Infinite Volumeのセキュリティ形式については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

### 関連コンセプト

[セキュリティ形式とその影響とは](#)(20ページ)

[セキュリティ形式を設定する場所とタイミング](#)(21ページ)

[FlexVolを備えたSVMで使用するセキュリティ形式を決定する方法](#)(21ページ)

[セキュリティ形式の継承の仕組み](#)(21ページ)

[UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法の管理](#)(77ページ)

SVMルート ボリュームでのセキュリティ形式の設定

Storage Virtual Machine (SVM) のルート ボリューム上のデータに使用するアクセス権のタイプを決定するには、SVMルート ボリュームのセキュリティ形式を設定します。

手順

- 1. セキュリティ形式を定義するには、`vserver create`コマンドで`-rootvolume-security-style`パラメータを使用します。

ルート ボリュームのセキュリティ形式に使用できるオプションは、`unix`、`ntfs`、または`mixed`です。`unified`セキュリティ形式は、Infinite Volumeにしか適用されないため、使用できません。

`vserver create`コマンドの詳細については、『*clustered Data ONTAP システム アドミニストレーション ガイド*(クラスタ管理)』を参照してください。

- 2. 作成したSVMのルート ボリューム セキュリティ形式を含む設定を表示して確認します。

```
vserver show -vserver vserver_name
```

FlexVolでのセキュリティ形式の設定

Storage Virtual Machine (SVM) のFlexVol上のデータに使用するアクセス権のタイプを決定するには、FlexVolのセキュリティ形式を設定します。

手順

- 1. 次のいずれかを実行します。

| FlexVolの有無 | 使用するコマンド                                                                                  |
|------------|-------------------------------------------------------------------------------------------|
| まだ存在しない    | セキュリティ形式を指定する <code>-security-style</code> パラメータを付加して、 <code>volume create</code> を入力します。 |
| すでに存在する    | セキュリティ形式を指定する <code>-security-style</code> パラメータを付加して、 <code>volume modify</code> を入力します。 |

FlexVolのセキュリティ形式に使用できるオプションは、`unix`、`ntfs`、または`mixed`です。`unified`セキュリティ形式は、Infinite Volumeにしか適用されないため、使用できません。

FlexVolの作成時にセキュリティ形式を指定しない場合、ボリュームはルート ボリュームのセキュリティ形式を継承します。

`volume create`コマンドまたは`volume modify`コマンドの詳細については、『*clustered Data ONTAP 論理ストレージ管理ガイド*』を参照してください。

- 2. 作成したFlexVolのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume show -volume volume_name -instance
```

qtreeでのセキュリティ形式の設定

qtree上のデータに使用するアクセス権のタイプを決定するには、qtreeのセキュリティ形式を設定します。

手順

- 1. 次のいずれかを実行します。

| qtreeの有無 | 使用するコマンド                                                          |
|----------|-------------------------------------------------------------------|
| まだ存在しない  | セキュリティ形式を指定する-security-styleパラメータを付加して、volume qtree createを入力します。 |
| すでに存在する  | セキュリティ形式を指定する-security-styleパラメータを付加して、volume qtree modifyを入力します。 |

qtreeのセキュリティ形式に使用できるオプションは、**unix**、**ntfs**、または**mixed**です。**unified**セキュリティ形式は、Infinite Volumeにしか適用されないため、使用できません。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトセキュリティ形式の**mixed**になります。

volume qtree createコマンドまたはvolume qtree modifyコマンドの詳細については、『*clustered Data ONTAP 論理ストレージ管理ガイド*』を参照してください。

- 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume qtree show -qtree qtree_name -instance
```

## NASネームスペースでのデータ ボリュームの作成と管理

NAS環境でファイル アクセスを管理するには、FlexVolを備えたStorage Virtual Machine(SVM)上でデータ ボリュームおよびジャンクション ポイントを管理する必要があります。これには、ネームスペース アーキテクチャの計画、ジャンクション ポイントが設定されたボリュームまたは設定されていないボリュームの作成、ボリュームのマウントまたはアンマウント、およびデータ ボリュームやNFSサーバまたはCIFSサーバのネームスペースに関する情報の表示が含まれます。

### 関連コンセプト

[FlexVolを備えたSVMのネームスペースとは](#)(15ページ)

[ボリューム ジャンクションの使用に関するルール](#)(15ページ)

[SMBおよびNFSネームスペースでのボリューム ジャンクションの使用方法](#)(16ページ)

[一般的なNASネームスペース アーキテクチャとは](#)(16ページ)

### 関連タスク

[FlexVolでのSMBファイル名の変換のための文字マッピングの設定](#)(164ページ)

## ジャンクション ポイントを指定したボリュームの作成

データ ボリュームを作成する際にジャンクション ポイントを指定できます。作成したボリュームはジャンクション ポイントに自動的にマウントされ、NASアクセス用の設定にすぐに使用できます。

### 開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

### 手順

- ジャンクション ポイントを備えたボリュームを作成します。

```
volume create -vserver vservers_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|
unix|mixed} -junction-path junction_path
```

ジャンクション パスはルート(/)で始まる必要があり、ディレクトリおよびジャンクションされたボリュームを含むことができます。ジャンクション パスにボリュームの名前を含める必要はありません。ジャンクション パスはボリューム名に依存しません。

ボリュームのセキュリティ形式の指定は省略可能です。セキュリティ形式を指定しない場合、Data ONTAPは、Storage Virtual Machine(SVM)のルート ボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルート ボリュームのセキュリティ形式が、作成するデータ ボリュームには適切でないセキュリティ形式である場合もあります。解決が困難なファイル アクセスの問題ができるだけ発生しないように、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

ジャンクション パスでは大文字と小文字は区別されず、/ENGは/engと同じものとみなされます。CIFS共有を作成すると、Windowsはそのジャンクション パスを大文字と小文字の区別があるかのように扱います。たとえば、ジャンクションが/ENGの場合、CIFS共有のパスは、/engではなく、/ENGで始まる必要があります。

データ ボリュームは、各種のパラメータを使用してカスタマイズできます。これらのパラメータの詳細については、volume createコマンドのマニュアル ページを参照してください。

2. 目的のジャンクション ポイントが設定されたボリュームが作成されたことを確認します。

```
volume show -vserver vs1 -volume volume_name -junction
```

#### 例

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

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

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

| Vserver | Volume | Junction Active | Junction Path | Junction Path Source |
|---------|--------|-----------------|---------------|----------------------|
| vs1     | home4  | true            | /eng/home     | RW_volume            |

## ジャンクション ポイントが指定されていないデータ ボリュームの作成

ジャンクション ポイントを指定せずにデータ ボリュームを作成できます。作成したボリュームは自動的にマウントされず、NASアクセス用の設定に使用することはできません。このボリュームに対してSMB共有またはNFSエクスポートを設定するには、まず、ボリュームをマウントする必要があります。

### 開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

### 手順

1. 次のコマンドを使用して、ジャンクション ポイントが設定されていないボリュームを作成します。

```
volume create -vserver vs1 -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|
unix|mixed}
```

ボリュームのセキュリティ形式の指定は省略可能です。セキュリティ形式を指定しない場合、Data ONTAPは、Storage Virtual Machine(SVM)のルート ボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルート ボリュームのセキュリティ形式が、データ ボリュームには適切でないセキュリティ形式である場合もあります。解決が困難なファイル アクセスの問題ができるだけ発生しないように、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

データ ボリュームは、各種のパラメータを使用してカスタマイズできます。これらのパラメータの詳細については、volume createコマンドのマニュアル ページを参照してください。

2. ジャンクション ポイントが設定されていないボリュームが作成されたことを確認します。

```
volume show -vserver vs1 -volume volume_name -junction
```

#### 例

次の例は、ジャンクション ポイントにマウントされない「sales」という名前のボリュームをSVM vs1上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3 -size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Junction Active | Junction Path | Junction Path Source |
|---------|----------|-----------------|---------------|----------------------|
| vs1     | data     | true            | /data         | RW_volume            |
| vs1     | home4    | true            | /eng/home     | RW_volume            |
| vs1     | vs1_root | -               | /             | -                    |
| vs1     | sales    | -               | -             | -                    |

## NASネームスペースでの既存のボリュームのマウントまたはアンマウント

Storage Virtual Machine (SVM) ボリュームに含まれているデータへのNASクライアントのアクセスを設定するには、ボリュームがNASネームスペースにマウントされている必要があります。ボリュームがマウントされていない場合、ジャンクション ポイントにボリュームをマウントできます。また、ボリュームはアンマウントすることもできます。

### タスク概要

ボリュームをアンマウントすると、ジャンクション ポイント内のすべてのデータにNASクライアントからアクセスできなくなります。アンマウントしたボリュームのネームスペース内にジャンクション ポイントが含まれるボリューム内のデータもこれに該当します。ボリュームをアンマウントしても、ボリューム内のデータは失われません。また、既存のボリューム エクスポート ポリシーおよびボリュームまたはディレクトリ上に作成されたSMB共有、およびアンマウントされたボリューム内のジャンクション ポイントもそのままです。アンマウントしたボリュームを再マウントすれば、NASは、既存のエクスポート ポリシーとSMB共有を使用してボリューム内のデータにアクセスできるようになります。

### 手順

1. 次のうち必要な操作を実行します。

| 状況           | 入力するコマンド                                                                                |
|--------------|-----------------------------------------------------------------------------------------|
| ボリュームのマウント   | <code>volume mount -vserver vs1 -volume volume_name -junction-path junction_path</code> |
| ボリュームのアンマウント | <code>volume unmount -vserver vs1 -volume volume_name</code>                            |

2. ボリュームが次のようなマウント状態になっていることを確認します。

```
volume show -vserver vs1 -volume volume_name -junction
```

#### 例

次に、vs1というSVM内の「sales」という名前のボリュームをジャンクション ポイント/salesにマウントする例を示します。



```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Junction<br>Active | Junction Path | Junction<br>Path Source |
|---------|----------|--------------------|---------------|-------------------------|
| vs1     | data     | true               | /data         | RW_volume               |
| vs1     | home4    | true               | /eng/home     | RW_volume               |
| vs1     | vs1_root | -                  | /             | -                       |
| vs1     | sales    | true               | /sales        | RW_volume               |

次に、vs1というSVM内の「data」という名前のボリュームをアンマウントする例を示します。

```
cluster1::> volume unmount -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Junction<br>Active | Junction Path | Junction<br>Path Source |
|---------|----------|--------------------|---------------|-------------------------|
| vs1     | data     | -                  | -             | -                       |
| vs1     | home4    | true               | /eng/home     | RW_volume               |
| vs1     | vs1_root | -                  | /             | -                       |
| vs1     | sales    | true               | /sales        | RW_volume               |

## ボリューム マウント ポイントとジャンクション ポイントに関する情報の表示

Storage Virtual Machine (SVM) のマウントされたボリューム、およびボリュームがマウントされているジャンクション ポイントに関する情報を表示できます。また、ジャンクション ポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVMネームスペースを把握し、管理することができます。

### 手順

1. 次のうち必要な操作を実行します。

| 表示する項目                          | 入力するコマンド                                                                                                                                                                                                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SVMのマウントされた / されていないボリュームの概要情報  | <b>volume show -vserver <i>vserver_name</i> -junction</b>                                                                                                                                                                                                          |
| SVMのマウントされた / されていないボリュームの詳細情報  | <b>volume show -vserver <i>vserver_name</i> -volume <i>volume_name</i> -instance</b>                                                                                                                                                                               |
| SVMのマウントされた / されていないボリュームの特定の情報 | <ol style="list-style-type: none"> <li>a. 必要に応じて、次のコマンドを使用して、-fieldsパラメータの有効なフィールドを表示できます。<br/><b>volume show -fields ?</b></li> <li>b. -fieldsパラメータを使用して、必要な情報を表示します。<br/><b>volume show -vserver <i>vserver_name</i> -fields <i>fieldname</i>,...</b></li> </ol> |

### 例

次の例では、SVM vs1のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Junction<br>Active | Junction Path | Junction<br>Path Source |
|---------|----------|--------------------|---------------|-------------------------|
| vs1     | data     | true               | /data         | RW_volume               |
| vs1     | home4    | true               | /eng/home     | RW_volume               |
| vs1     | vs1_root | -                  | /             | -                       |
| vs1     | sales    | true               | /sales        | RW_volume               |

|     |          |      |           |           |
|-----|----------|------|-----------|-----------|
| vs1 | data     | true | /data     | RW_volume |
| vs1 | home4    | true | /eng/home | RW_volume |
| vs1 | vs1_root | -    | /         | -         |
| vs1 | sales    | true | /sales    | RW_volume |

次の例では、SVM vs2上のボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields vsserver,volume,aggregate,size,state,type,security-
style,junction-path,junction-parent,node
vsserver volume aggregate size state type security-style junction-path junction-parent node
-----
vs2 data1 aggr3 2GB online RW unix - - node3
vs2 data2 aggr3 1GB online RW ntfs /data2 vs2_root node3
vs2 data2_1 aggr3 8GB online RW ntfs /data2/d2_1 data2 node3
vs2 data2_2 aggr3 8GB online RW ntfs /data2/d2_2 data2 node3
vs2 pubs aggr1 1GB online RW unix /publications vs2_root node1
vs2 images aggr3 2TB online RW ntfs /images vs2_root node3
vs2 logs aggr1 1GB online RW unix /logs vs2_root node1
vs2 vs2_root aggr3 1GB online RW ntfs / - node3
```

## ストレージレベルのアクセス保護を使用したファイル アクセスの保護

ネイティブ ファイルレベルのセキュリティとエクスポートおよび共有のセキュリティを使用したアクセスの保護に加えて、ボリューム レベルでData ONTAPによって適用される第3のセキュリティレイヤとしてストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護は、すべてのNASプロトコルからその適用先となるストレージ オブジェクトへのアクセスに適用されます。

### ストレージレベルのアクセス保護の動作

- ストレージレベルのアクセス保護は、ストレージ オブジェクト内のすべてのファイルまたはすべてのディレクトリに適用されます。  
ボリューム内のすべてのファイルまたはディレクトリがストレージレベルのアクセス保護設定の影響を受けるため、伝播による継承は必要ありません。
- ストレージレベルのアクセス保護は、ボリューム内にある、ファイルのみ、ディレクトリのみ、またはファイルとディレクトリの両方に適用されるように設定できます。
  - ファイルとディレクトリのセキュリティ  
ストレージ オブジェクト内のすべてのディレクトリおよびファイルに適用されます。これがデフォルト設定です。
  - ファイル セキュリティ  
ストレージ オブジェクト内のすべてのファイルに適用されます。このセキュリティを適用しても、ディレクトリへのアクセスとディレクトリの監査は影響を受けません。
  - ディレクトリ セキュリティ  
ストレージ オブジェクト内のすべてのディレクトリに適用されます。このセキュリティを適用しても、ファイルへのアクセスとファイルの監査は影響を受けません。
- ストレージレベルのアクセス保護は、アクセス権を制限するために使用されます。  
追加のアクセス権限を与えることはありません。
- NFSまたはSMBクライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。  
このセキュリティは、有効な権限を決定するために、ストレージ オブジェクトレベルで適用され、メタデータ内に格納されます。
- システム (WindowsまたはUNIX) 管理者であっても、ストレージレベルのセキュリティをクライアントから取り消すことはできません。  
このセキュリティは、ストレージ管理者のみが変更できるように設計されています。
- ストレージレベルのアクセス保護は、NTFSまたはmixedセキュリティ形式のボリュームに適用できます。

- ストレージレベルのアクセス保護をUNIXセキュリティ形式のボリュームに適用できるのは、そのボリュームが含まれているStorage Virtual Machine (SVM) でCIFSサーバが設定されている場合に限られます。
- ボリュームがあるボリューム ジャンクション パスの下にマウントされていて、ストレージレベルのアクセス保護がそのパス上にある場合、ストレージレベルのアクセス保護はそのパスの下にマウントされているボリュームには伝播されません。
- ストレージレベルのアクセス保護のセキュリティ記述子は、SnapMirrorデータレプリケーションおよびStorage Virtual Machine (SVM) レプリケーションによってレプリケートされます。
- ウィルス スキャンについては特別な免除があります。  
ファイルやディレクトリのスクリーニングを行うこうしたサーバに対しては、ストレージレベルのアクセス保護によってそのオブジェクトへのアクセスが拒否されている場合でも、例外的なアクセスが許可されます。
- ストレージレベルのアクセス保護によってアクセスが拒否された場合、FPolicy通知は送信されません。

### NFSアクセスに対するストレージレベルのアクセス保護

ストレージレベルのアクセス保護では、NTFSのアクセス権限のみがサポートされています。Data ONTAPでUNIXユーザに対するセキュリティ チェックを実行している場合、ストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスするには、UNIXユーザをそのボリュームを所有しているSVM上のWindowsユーザにマッピングする必要があります。

ストレージレベルのアクセス保護は、UNIX専用のSVMやCIFSサーバが含まれていないSVMには適用されません。

### アクセス チェックの順序

ファイルまたはディレクトリへのアクセスは、エクスポートまたは共有の権限、ボリュームで設定されているストレージレベルのアクセス保護権限、ファイルやディレクトリに適用されるネイティブのファイル アクセス権の各影響の組み合わせによって決定されます。すべてのレベルのセキュリティが評価されて、ファイルまたはディレクトリの有効な権限が決定されます。セキュリティアクセス チェックは、次の順序で実行されます。

1. SMB共有またはNFSエクスポートレベルの権限
2. ストレージレベルのアクセス保護
3. NTFSのファイルやフォルダのAccess Control List (ACL; アクセス 制御リスト)、NFSv4 ACL、またはUNIXモードのビット

ストレージレベルのアクセス保護の設定の詳細については、『*clustered Data ONTAP ファイル アクセス管理ガイド(CIFS)*』を参照してください。

### 関連コンセプト

[Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み](#)(24ページ)

[ファイル セキュリティと監査ポリシーに関する情報の表示](#)(246ページ)

[CLIを使用したSVMのNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理](#)(257ページ)

### 関連タスク

[ストレージレベルのアクセス保護の設定](#)(157ページ)

[セキュリティトレースの実行](#)(292ページ)

## ストレージレベルのアクセス保護の使用のユースケース

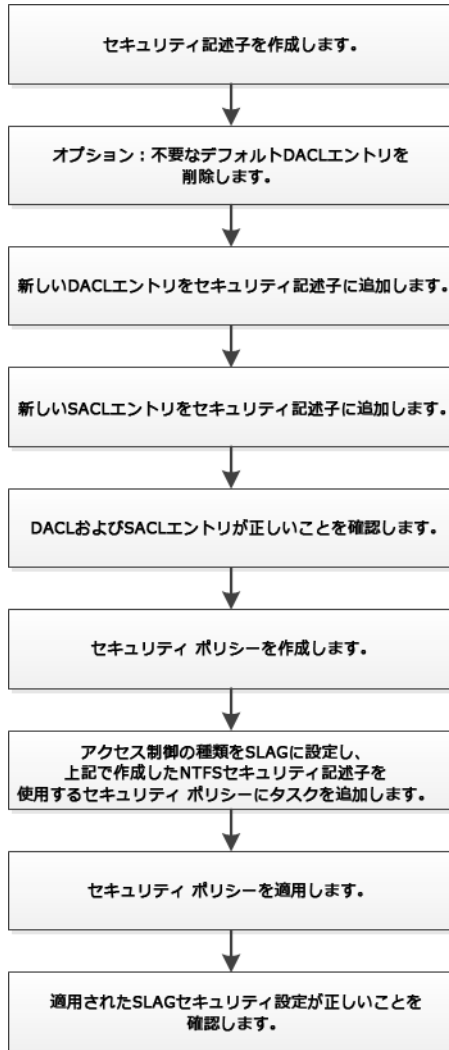
ストレージレベルのアクセス保護は、ストレージレベルでの追加セキュリティを提供します。これはクライアントサイドからは見えないため、ユーザや管理者がデスクトップから取り消すことはできません。あるユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

この機能は、次のようなシナリオで一般的に使用されるユースケースです。

- すべてのユーザ アクセスをストレージレベルで監査、制御することによって知的財産を保護する場合
- 銀行業務を行うグループと証券業務の両方を行うグループを抱えた金融サービス企業のストレージの場合
- 部門ごとにそれぞれ個別のファイル ストレージを持つ行政サービスの場合
- すべての学生のファイルを保護する必要がある大学の場合

## ストレージレベルのアクセス保護の設定ワークフロー

ストレージレベルのアクセス保護(SLAG)を設定するワークフローでは、NTFSファイル権限や監査ポリシーを設定する際に使用するData ONTAP CLIコマンドと同じコマンドを使用します。対象のファイルやディレクトリのアクセスを設定する代わりに、対象のStorage Virtual Machine(SVM)ボリュームのSLAGを設定します。



#### 関連タスク

[ストレージレベルのアクセス保護の設定](#) (157ページ)

## ストレージレベルのアクセス保護の設定

ボリュームまたはqtreeのストレージレベルのアクセス保護を設定するには、多くの手順に従う必要があります。ストレージレベルのアクセス保護は、ストレージレベルで設定するアクセス セキュリティを提供します。すべてのNASプロトコルからの適用対象のストレージ オブジェクトへのすべてのアクセスにセキュリティが適用されます。

#### 手順

1. `vserver security file-directory ntfs create`コマンドを使用して、セキュリティ記述子を作成します。

#### 例

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1
vserver security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name
-----
sd1 -
```

セキュリティ記述子は、次の4つのデフォルトDACLアクセス制御エントリ(ACE)を持った状態で作成されます。

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name           | Access Type | Access Rights | Apply To                        |
|------------------------|-------------|---------------|---------------------------------|
| BUILTIN\Administrators | allow       | full-control  | this-folder, sub-folders, files |
| BUILTIN\Users          | allow       | full-control  | this-folder, sub-folders, files |
| CREATOR OWNER          | allow       | full-control  | this-folder, sub-folders, files |
| NT AUTHORITY\SYSTEM    | allow       | full-control  | this-folder, sub-folders, files |

ストレージレベルのアクセス保護を設定する際にデフォルトのエントリを使用しない場合は、セキュリティ記述子に独自のACEを作成して追加する前に、デフォルトのエントリを削除できます。

2. オプション: セキュリティ記述子から、ストレージレベルのアクセス保護セキュリティに設定したくないデフォルトのDACL ACEを削除します。
  - a. `vserver security file-directory ntfs dacl remove`コマンドを使用して、不要なDACL ACEを削除します。

#### 例

この例では、セキュリティ記述子からBUILTIN\Administrators、BUILTIN\Users、CREATOR OWNERの3つのデフォルトDACL ACEを削除しています。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account builtin\users
```

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account builtin\administrators
```

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. `vserver security file-directory ntfs dacl show`コマンドを使用して、ストレージレベルのアクセス保護セキュリティに使用しないDACL ACEがセキュリティ記述子から削除されたことを確認します。

#### 例

この例では、コマンドからの出力より、セキュリティ記述子から3つのデフォルトDACL ACEが削除され、NT AUTHORITY\SYSTEMのデフォルトDACL ACEエントリのみが残されていることを確認できます。

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name        | Access Type | Access Rights | Apply To                        |
|---------------------|-------------|---------------|---------------------------------|
| NT AUTHORITY\SYSTEM | allow       | full-control  | this-folder, sub-folders, files |

3. `vserver security file-directory ntfs dacl add`コマンドを使用して、セキュリティ記述子に1つまたは複数のDACLエントリを追加します。

#### 例

この例では、セキュリティ記述子に2つのDACL ACEを追加しています。

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -
apply-to this-folder,sub-folders,files
```

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account "example\Domain Users" -rights read -apply-
to this-folder,sub-folders,files
```

4. オプション: `vserver security file-directory ntfs sacl add`コマンドを使用して、セキュリティ記述子に1つまたは複数のSACLエントリを追加します。

#### 例

この例では、セキュリティ記述子に2つのSACL ACEを追加しています。

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -
apply-to this-folder,sub-folders,files
```

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type success -account example\engineering -rights full-control -
apply-to this-folder,sub-folders,files
```

5. `vserver security file-directory ntfs dacl show`および `vserver security file-directory ntfs sacl show`コマンドを使用して、DACLおよびSACL ACEがそれぞれ正しく設定されていることを確認します。

#### 例

この例では、次のコマンドでセキュリティ記述子「sd1」のDACLエントリ情報を表示しています。

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name         | Access Type | Access Rights | Apply To                        |
|----------------------|-------------|---------------|---------------------------------|
| EXAMPLE\Domain Users | allow       | read          | this-folder, sub-folders, files |
| EXAMPLE\engineering  | allow       | full-control  | this-folder, sub-folders, files |
| NT AUTHORITY\SYSTEM  | allow       | full-control  | this-folder, sub-folders, files |

この例では、次のコマンドでセキュリティ記述子「sd1」のSACLエントリ情報を表示しています。

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name         | Access Type | Access Rights | Apply To                        |
|----------------------|-------------|---------------|---------------------------------|
| EXAMPLE\Domain Users | failure     | read          | this-folder, sub-folders, files |
| EXAMPLE\engineering  | success     | full-control  | this-folder, sub-folders, files |

6. `vserver security file-directory policy create`コマンドを使用して、セキュリティ ポリシーを作成します。

#### 例

次の例では、「policy1」という名前のポリシーを作成しています。

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. `vserver security file-directory policy show`コマンドを使用して、ポリシーが正しく設定されていることを確認します。

#### 例

```
vserver security file-directory policy show
```

| Vserver | Policy Name |
|---------|-------------|
| -----   | -----       |
| vs1     | policy1     |

8. `-access-control`パラメータに**slag**を設定して `vserver security file-directory policy-task add`コマンドを使用し、関連するセキュリティ記述子のタスクをセキュリティ ポリシーに追加します。

ポリシーには複数のストレージレベルのアクセス保護タスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

#### 例

この例では、「policy1」という名前のポリシーにタスクを追加しています。このポリシーは、セキュリティ記述子「sd1」に割り当てられています。これは、アクセス制御の種類が「slag」に設定されたバス/datavol1に割り当てられています。

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. `vserver security file-directory policy task show`コマンドを使用して、タスクが正しく設定されていることを確認します。

#### 例

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

| Vserver: vs1    |                  |                |               |           |                               |
|-----------------|------------------|----------------|---------------|-----------|-------------------------------|
| Policy: policy1 |                  |                |               |           |                               |
| Index           | File/Folder Path | Access Control | Security Type | NTFS Mode | NTFS Security Descriptor Name |
| -----           | -----            | -----          | -----         | -----     | -----                         |
| 1               | /datavol1        | slag           | ntfs          | propagate | sd1                           |

10. `vserver security file-directory policy apply`コマンドを使用して、ストレージレベルのアクセス保護セキュリティ ポリシーを適用します。

#### 例

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```



セキュリティ ポリシーを適用するジョブがスケジュールされます。

11. `vserver security file-directory show` コマンドを使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認します。

#### 例

この例では、コマンドからの出力により、ストレージレベルのアクセス保護セキュリティがNTFS ボリューム/`datavol1`に適用されていることがわかります。EveryoneにFull Controlを許可するデフォルトDACLは残っていますが、ストレージレベルのアクセス保護セキュリティによって、ストレージレベルのアクセス保護設定で定義されたグループにアクセスが制限(および監査)されます。

**`vserver security file-directory show -vserver vs1 -path /datavol1`**

```

Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ---D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
      Control:0x8004
      Owner: BUILTIN\Administrators
      Group: BUILTIN\Administrators
      DACL - ACEs
        ALLOW-Everyone-0x1f01ff
        ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

#### 関連コンセプト

[CLIを使用したSVMのNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理](#) (257ページ)

[ストレージレベルのアクセス保護の設定ワークフロー](#) (156ページ)

#### 関連タスク

[ストレージレベルのアクセス保護に関する情報の表示](#) (162ページ)

[ストレージレベルのアクセス保護の削除](#) (163ページ)

#### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver security file-directory show - Display file/folder security information](#)

## ストレージレベルのアクセス保護に関する情報の表示

ストレージレベルのアクセス保護は、ボリュームまたはqtreeに適用される3番目のセキュリティレイヤです。ストレージレベルのアクセス保護の設定は、Windowsの[プロパティ]ウィンドウには表示されません。ストレージレベルのアクセス保護セキュリティに関する情報を表示するには、Data ONTAP CLIを使用する必要があります。この情報を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine(SVM)の名前、およびストレージレベルのアクセス保護セキュリティ情報を表示するボリュームまたはqtreeのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

### 手順

1. ストレージレベルのアクセス保護セキュリティ設定を必要な詳細レベルで表示します。

| 表示する情報 | 入力するコマンド                                                                                             |
|--------|------------------------------------------------------------------------------------------------------|
| 要約形式   | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| 詳細を表示  | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

### 例

次の例では、SVM vs1のパス/datavol1にあるNTFSセキュリティ形式のボリュームのストレージレベルのアクセス保護セキュリティ情報を表示します。

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
              ALLOW-Everyone-0x1f01ff
              ALLOW-Everyone-0x10000000-OI|CI|IO

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

次の例では、SVM vs1のパス/datavol5にあるmixedセキュリティ形式のボリュームに関するストレージレベルのアクセス保護の情報を表示します。このボリュームの最上位には、

UNIX対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /
datavol5
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

## ストレージレベルのアクセス保護の削除

ストレージレベルのアクセス セキュリティの設定が不要になった場合は、ボリュームやqtreeからストレージレベルのアクセス保護を削除できます。ストレージレベルのアクセス保護を削除しても、通常のNTFSのファイルやディレクトリのセキュリティは変更されたり削除されたりしません。

### 手順

1. vserver security file-directory showコマンドを使用して、ボリュームまたはqtreeにストレージレベルのアクセス保護が設定されていることを確認します。

### 例

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
      Vserver: vs1
      File Path: /datavol2
      File Inode Number: 99
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0xbf14
      Owner: BUILTIN\Administrators
      Group: BUILTIN\Administrators
      SACL - ACES
        AUDIT-EXAMPLE\Domain Users-0xf01ff-0I|CI|FA
      DACL - ACES
        ALLOW-EXAMPLE\Domain Admins-0x1f01ff-0I|CI
        ALLOW-EXAMPLE\Domain Users-0x1301bf-0I|CI
```

```
Storage-Level Access Guard security
DACL (Applies to Directories):
  ALLOW-BUILTIN\Administrators-0x1f01ff
  ALLOW-CREATOR OWNER-0x1f01ff
  ALLOW-EXAMPLE\Domain Admins-0x1f01ff
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
  ALLOW-BUILTIN\Administrators-0x1f01ff
  ALLOW-CREATOR OWNER-0x1f01ff
  ALLOW-EXAMPLE\Domain Admins-0x1f01ff
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. `vserver security file-directory remove-slag` コマンドを使用して、ストレージレベルのアクセス保護を削除します。

#### 例

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. `vserver security file-directory show` コマンドを使用して、ボリュームや `qtree` からストレージレベルのアクセス保護が削除されたことを確認します。

#### 例

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
  AUDIT-EXAMPLE\Domain Users-0xf01ff-0I|CI|FA
DACL - ACEs
  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-0I|CI
  ALLOW-EXAMPLE\Domain Users-0x1301bf-0I|CI
```

## FlexVolでのSMBファイル名の変換のための文字マッピングの設定

NFSクライアントは、SMBクライアントと特定のWindowsアプリケーションでは無効な文字を含むファイル名を作成できます。FlexVolにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効なNFS名を持つファイルにSMBクライアントからアクセスできます。

#### タスク概要

SMBクライアントがNFSクライアントによって作成されたファイルにアクセスすると、Data ONTAPはファイル名を調べます。ファイル名が有効なSMBファイル名でない場合は(たとえば、コロン「:」文字が含まれている場合)、Data ONTAPは各ファイルに対して維持されている8.3形式のファイル名

を返します。ただし、これにより、長いファイル名に重要な情報をエンコードしているアプリケーションでは問題が発生します。

したがって、異なるオペレーティング システムを使用するクライアント間でファイルを共有する場合は、両方のオペレーティング システムで有効な文字をファイル名に使用するよう to してください。

これとは別に、SMBクライアントで有効でない文字を含むNFSクライアントが作成したファイル名がある場合は、無効なNFSの文字を、SMBと特定のWindowsアプリケーションの両方で有効なUnicode文字に変換するマッピングを定義できます。たとえば、この機能はCATIAR MCADおよびMathematicaアプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に留意する必要があります。

- 文字マッピングは、ジャンクション ポイントを越えて適用されることはありません。  
文字マッピングは、各ジャンクション ボリュームに対して明示的に設定する必要があります。
- 無効な文字を表すUnicode文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。  
たとえば、コロン(:)をハイフン(-)にマッピングしようとした場合に、ファイル名に正しく使用されているハイフン(-)が存在すると、Windowsクライアントが「a-b」という名前のファイルにアクセスする要求を行ったときに、「a:b」というNFS名にマッピングされてしまいます(望ましい結果ではありません)。
- 文字マッピングを適用してもまだマッピングに無効なWindows文字が含まれている場合、Data ONTAPはWindows 8.3ファイル名にフォールバックします。
- FPolicy通知、NAS監査ログ、セキュリティトレース メッセージでは、マッピングされたファイル名が表示されます。
- タイプがDPであるSnapMirror関係が作成されても、ソース ボリュームの文字マッピングはデスティネーションDPボリュームにレプリケーションされません。

## 手順

- 文字マッピングを設定するには、次のコマンドを実行します。

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name -mapping mapping_text, ...
```

マッピングは、「:」で区切られたソースとターゲットの文字のペアのリストで構成されます。文字は、16進数値で入力されたUnicode文字です。例:3C:E03C

コロンで区切られた各mapping\_textペアの最初の値は、変換したいNFS文字の16進値です。2番目の値は、SMBが使用するUnicode値です。マッピングのペアは一意である必要があります(1対1のマッピングが存在する必要があります)。

- ソース マッピング

次の表に、ソース マッピングで許可されているUnicode文字セットを示します。

| Unicode文字 | 表示される文字  | 説明         |
|-----------|----------|------------|
| 0x01-0x19 | サポートされない | 表示されない制御文字 |
| 0x5C      | \        | バックスラッシュ   |
| 0x3A      | :        | コロン        |
| 0x2A      | *        | アスタリスク     |
| 0x3F      | ?        | 疑問符        |

| Unicode文字 | 表示される文字 | 説明        |
|-----------|---------|-----------|
| 0x22      | "       | 引用符       |
| 0x3C      | <       | 小なり       |
| 0x3E      | >       | 大なり       |
| 0x7C      |         | 縦線        |
| 0xB1      | ±       | プラスマイナス記号 |

- ターゲット マッピング  
ターゲット文字には、U+E0000...U+F8FFの範囲のUnicodeの「私用領域」を指定できます。

#### 例

次のコマンドは、Storage Virtual Machine (SVM) vs1の「data」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

| Vserver | Volume Name | Character Mapping         |
|---------|-------------|---------------------------|
| vs1     | data        | 3c:e17c, 3e:f17d, 2a:f745 |

#### 関連コンセプト

[FlexVolを備えたSVMでネームスペースとボリューム ジャンクションがSMBアクセスに与える影響](#)(15ページ)

[NASネームスペースでのデータ ボリュームの作成と管理](#)(150ページ)

### SMBファイル名の変換のための文字マッピングの管理コマンド

FlexVol上でのSMBファイル名の変換に使用する情報を作成、変更、表示したり、それに使用するファイル文字マッピングを削除することによって文字マッピングを管理できます。

| 状況                  | 使用するコマンド                                           |
|---------------------|----------------------------------------------------|
| 新しいファイル文字マッピングを作成する | <code>vserver cifs character-mapping</code>        |
| ファイル文字マッピング情報を表示する  | <code>vserver cifs character-mapping show</code>   |
| 既存のファイル文字マッピングを変更する | <code>vserver cifs character-mapping modify</code> |
| ファイル文字マッピングを削除する    | <code>vserver cifs character-mapping delete</code> |

詳細については、各コマンドのマニュアル ページを参照してください。

#### 関連タスク

[FlexVolでのSMBファイル名の変換のための文字マッピングの設定](#)(164ページ)

## ネーム マッピングの作成

Data ONTAPは、Storage Virtual Machine(SVM)に格納されたデータにSMB接続を介してアクセスする際、ネーム マッピングを使用してWindows IDをUNIX IDにマッピングします。この情報は、ユーザー クレデンシャルを取得し、NTFSセキュリティ形式、UNIXセキュリティ形式、unifiedセキュリティ形式のいずれのデータであるかに関係なく適切なファイル アクセスを提供するために必要です。

ネーム マッピングは、通常、要求ファイルに適用されている有効なセキュリティ形式に関係なく、同じファイルへのSMBおよびNFS経由のマルチプロトコル アクセスを可能にするために必要です。

デフォルトのUNIX IDを使用するように設定する場合は、Windows IDからUNIX IDへのネーム マッピングを設定する必要はありません。

### 関連コンセプト

[FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法](#)(23ページ)

[マルチドメイン ネーム マッピング検索の設定](#)(170ページ)

[UNIXユーザーからWindowsユーザーへのネーム マッピングのためのマルチドメイン検索](#)(170ページ)

### 関連タスク

[デフォルトのUNIXユーザーの設定](#)(101ページ)

## ネーム マッピングの変換ルール

Data ONTAPシステムは、Storage Virtual Machine(SVM)ごとに一連の変換ルールを使用します。各ルールは、パターンとリプレースメントという2つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンはUNIX形式の正規表現です。リプレースメントは、UNIXのsedプログラムと同様に、パターンの部分式を表すエスケープシーケンスを含む文字列です。

適切なマッピング ルールがあれば、ストレージ システムとは異なるドメインに属するユーザーに対して、NTFSセキュリティ形式のボリュームへのNFSアクセスを付与することが可能です。

あるユーザーがルールに一致して別のドメインのユーザーにマッピングされる場合、そのドメインは信頼されている必要があります。SMBアクセスとNFSアクセス両方に関して、ほかのドメインのユーザーにマッピングするためには、ドメイン間に双方向の信頼関係が必要です。

ユーザーがルールに一致しても、ドメインが信頼されていないために認証できない場合、マッピングは失敗します。

SVMでは、双方向の信頼関係が確立されたすべてのドメインが自動的に検出され、それらを使用してマルチドメインのユーザー マッピングの検索が行われます。自動的に検出された信頼できるドメインではなく、信頼できるドメインのリストを独自に設定してネーム マッピングの検索に使用することもできます。

WindowsからUNIXへのマッピングでは、正規表現の大文字と小文字は区別されません。ただし、KerberosからUNIXへのマッピングと、UNIXからWindowsへのマッピングでは、大文字と小文字が区別されます。

たとえば、次のルールでは、「ENG」というドメインの「jones」というWindowsユーザーが、「jones」というUNIXユーザーに変換されます。

| パターン      | 変換後   |
|-----------|-------|
| ENG\jones | jones |

バックスラッシュは正規表現の特殊文字であるため、バックスラッシュを1つ追加してエスケープする必要がありますことに注意してください。

変換後のパターンには、キャレット(^)、アンダースコア(\_)、アンパサンド(&)といった記号を、プレフィックスとして文字に付加できます。これらの記号はそれぞれ、すべて大文字にする、すべて小文字にする、先頭の文字だけを大文字にすることを指定します。たとえば次のように指定できます。

- 元のパターンが(.+)で、返還後のパターンが\1の場合、文字列jOelはjOelにマッピングされます(変更されません)。
- 元のパターンが(.+)で、変換後のパターンが\\_1の場合、文字列jOelはjoelにマッピングされます。
- 元のパターンが(.+)で、変換後のパターンが\1の場合、文字列jOelはJOEにマッピングされます。
- 元のパターンが(.+)で、変換後のパターンが&1の場合、文字列jOelはJoelにマッピングされます。

バックスラッシュとアンダースコア(\\_)、バックスラッシュとキャレット(\^)、またはバックスラッシュとアンパサンド(\&)のシーケンスに続く文字が数字でない場合は、バックスラッシュのあとの文字がそのまま使用されます。

次の例では、「ENG」というドメインの任意のWindowsユーザが、NISで同じ名前のUNIXユーザに変換されます。

| パターン      | リプレースメント |
|-----------|----------|
| ENG\\(.+) | \1       |

2つのバックスラッシュ(\\)は、1つのバックスラッシュに一致します。丸かっこは部分式を表しますが、それ自体はどの文字にも一致しません。ピリオドは任意の1文字に一致します。アスタリスクは、直前の式の0回以上の繰り返しに一致します。上記の例では、ENG\のあとに1文字以上の任意の文字が続く文字列が一致します。変換後の\1は、最初に一致した部分式を表します。つまり、Windowsユーザ名がENG\jonesであるとする、変換後はjones、つまりENG\のあとの名前の部分になります。

注: CLIを使用している場合は、すべての正規表現を二重引用符(")で囲む必要があります。たとえば、CLIで正規表現(.+)を入力するには、コマンドプロンプトで"(.+)"と入力します。Web UIでは引用符は必要ありません。

正規表現の詳細については、UNIXシステムの管理マニュアル、UNIXのsedまたはregexのオンラインマニュアル、または『*Mastering Regular Expressions*』(O'Reilly and Associates)を参照してください。

## ネーム マッピングの作成

vserver name-mapping createコマンドを使用して、ネーム マッピングを作成できます。ネーム マッピングを使用すると、WindowsユーザからUNIXセキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

### タスク概要

Data ONTAPでは、Storage Virtual Machine(SVM)ごとに、各方向について最大1,024個のネーム マッピングがサポートされます。

### 手順

1. ネーム マッピングを作成するには、次のコマンドを入力します。



```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```

-vserver *vserver\_name*には、SVM名を指定します。

-direction {krb-unix|win-unix|unix-win}は、マッピング方向を指定します。

-position *integer*には、新しいマッピングの優先順位リスト内での特定の位置を指定します。

-pattern *text*には、照合するパターンを256文字以内で指定します。

-replacement *text*には、リプレースメント パターンを256文字以内で指定します。

WindowsからUNIXへのマッピングを作成した場合、新しいマッピングが作成されたときにData ONTAPシステムに接続していたすべてのCIFSクライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

### 例

次のコマンドでは、vs1という名前のSVM上にネーム マッピングを作成します。このマッピングは、UNIXからWindowsへのマッピングで、優先順位リスト内での位置は1番目です。このマッピングにより、UNIXユーザーjohndがWindowsユーザENG\Johnにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd -replacement "ENG\John"
```

次のコマンドでは、vs1という名前のSVM上に別のネーム マッピングを作成します。このマッピングは、WindowsからUNIXへのマッピングで、優先順位リスト内での位置は1番目です。このマッピングにより、ドメインENG内のすべてのCIFSユーザが、SVMに関連付けられたNISドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

## ネーム マッピングの管理用コマンド

Data ONTAPには、ネーム マッピングを管理するための固有のコマンドが用意されています。

| 状況                   | 使用するコマンド                    |
|----------------------|-----------------------------|
| ネーム マッピングを作成する       | vserver name-mapping create |
| 特定の位置にネーム マッピングを挿入する | vserver name-mapping insert |
| ネーム マッピングを表示する       | vserver name-mapping show   |
| 2つのネーム マッピングの位置を交換する | vserver name-mapping swap   |
| ネーム マッピングを変更する       | vserver name-mapping modify |
| ネーム マッピングを削除する       | vserver name-mapping delete |

詳細については、各コマンドのマニュアル ページを参照してください。

## マルチドメイン ネーム マッピング検索の設定

Storage Virtual Machine (SVM)を設定してマルチドメイン ネーム マッピング検索を実行できます。これにより、Data ONTAPでは、UNIXユーザとWindowsユーザのネーム マッピングを実行するときに、双方向の信頼関係が確立されたドメインをすべて検索することができます。

### 関連コンセプト

[ネーム マッピングの変換ルール](#) (167ページ)

[UNIXユーザからWindowsユーザへのネーム マッピングのためのマルチドメイン検索](#) (170ページ)

### 関連タスク

[ネーム マッピングの作成](#) (168ページ)

[マルチドメイン ネーム マッピングの検索の有効化と無効化](#) (172ページ)

## UNIXユーザからWindowsユーザへのネーム マッピングのためのマルチドメイン検索

Data ONTAPは、UNIXユーザをWindowsユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

### ドメインの信頼性がUNIXユーザからWindowsユーザへのネーム マッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性がData ONTAPに与える影響を理解しておく必要があります。CIFSサーバのホームドメインとのActive Directoryの信頼関係には、双方向の信頼と単一方向の信頼（インバウンドまたはアウトバウンドのどちらか）があります。ホームドメインは、Storage Virtual Machine (SVM)のCIFSサーバが属しているドメインです。

- **双方向の信頼**  
 双方向の信頼では、両方のドメインが相互に信頼し合っています。CIFSサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属しているユーザを認証および許可でき、逆に、信頼できるドメインはホームドメインに属しているユーザを認証および許可することができます。  
 UNIXユーザからWindowsユーザへのネーム マッピング検索は、ホームドメインともう一方のドメインとの間に双方向の信頼関係があるドメインでのみ実行できます。
- **アウトバウンドの信頼**  
 アウトバウンドの信頼では、ホームドメインがもう一方のドメインを信頼しています。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および許可できます。  
 ホームドメインとアウトバウンドの信頼関係にあるドメインは、UNIXユーザからWindowsユーザへのネーム マッピング検索の際に検索されません。
- **インバウンドの信頼**  
 インバウンドの信頼では、もう一方のドメインがCIFSサーバのホームドメインを信頼しています。この場合、ホームドメインはインバウンドの信頼できるドメインに属しているユーザを認証することも許可することもできません。  
 ホームドメインとインバウンドの信頼関係にあるドメインは、UNIXユーザからWindowsユーザへのネーム マッピング検索の際に検索されません。

### ネーム マッピングでのワイルドカード(\*)を使用したマルチドメイン検索の設定方法

マルチドメインのネーム マッピング検索では、Windowsユーザ名のドメイン セクションにワイルドカードを使用できます。次の表に、ネーム マッピング エントリのドメイン部にワイルドカードを使用して、マルチドメイン検索を可能にする方法を示します。

| パターン | 変換後              | 結果                                                                                                                                                    |
|------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| root | *\\administrator | UNIXユーザ「root」が「administrator」というユーザにマッピングされます。「administrator」という名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。                                          |
| *    | *\\*             | 有効なUNIXユーザが対応するWindowsユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。<br><br>注: パターン*\\*は、UNIXからWindowsへのネーム マッピングでのみ有効であり、反対方向では無効です。 |

### マルチドメインの名前検索の実行方法

マルチドメインの名前検索で使用する信頼できるドメインのリストは、次の2つの方法のどちらかで決定できます。

- Data ONTAPが作成した自動検出による双方向の信頼リストを使用する
  - この方法の長所は、管理のオーバーヘッドがまったく生じないことと、Data ONTAPによって有効と判断された信頼できるドメインでリストが構成されることです。
  - 短所は、信頼できるドメインの検索順序を選択できないことです。
- 自分で作成した信頼できる優先ドメイン リストを使用する
  - この方法の長所は、信頼できるドメインのリストを検索を行いたい順序で設定できることです。
  - 短所は、管理のオーバーヘッドが増えることと、リストの情報が古くなり、一部のドメインが双方向の信頼関係にある有効なドメインでなくなる可能性があることです。

ユーザ名のドメイン セクションにワイルドカードを使用してUNIXユーザがWindowsユーザにマッピングされている場合、Windowsユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先のWindowsユーザはこの検索リスト内でのみ順に検索されます。  
該当するWindowsユーザが見つかり次第、検索は終了します。同じWindowsユーザ名が2つの異なる信頼できるドメインに存在する場合は、信頼できるドメインの優先リストの上位にあるドメインのユーザが返されます。 該当するWindowsユーザが優先リスト内のどのドメインにも見つからない場合は、エラーが返されます。  
ホーム ドメインを検索対象にする場合は、信頼できるドメインの優先リストに含める必要があります。
- 信頼できるドメインの優先リストが設定されていない場合は、ホーム ドメインと双方向の信頼関係にあるすべてのドメインでWindowsユーザが検索されます。  
該当するWindowsユーザが見つかり次第、検索は終了します。同じWindowsユーザ名が2つの異なる信頼できるドメインに存在する場合は、自動検出された信頼できるドメイン リストの上位にあるドメインのユーザが返されます。 自動検出されたリストの信頼できるドメインの順序は変更できません。 該当するWindowsユーザが検出された信頼できるドメインのいずれにも見つからない場合は、ホーム ドメインでユーザが検索されます。

- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、ホームドメインでユーザが検索されます。

UNIXユーザがユーザ名にドメイン セクションのないWindowsユーザにマッピングされている場合は、ホームドメインでWindowsユーザが検索されます。

双方向の信頼関係にあるドメインのリストを管理する方法については、『*clustered Data ONTAP ファイル アクセス管理ガイド(CIFS)*』を参照してください。

#### 関連コンセプト

[FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法](#)(23ページ)

[ネーム マッピングの作成](#)(167ページ)

[ネーム マッピングの変換ルール](#)(167ページ)

#### 関連タスク

[信頼できるドメインのリセットおよび再検出](#)(173ページ)

[検出された信頼できるドメインに関する情報の表示](#)(173ページ)

[信頼できるドメインのリスト内の信頼できるドメインの追加、削除、または置換](#)(174ページ)

[信頼できるドメインの優先リストに関する情報の表示](#)(175ページ)

## マルチドメイン ネーム マッピングの検索の有効化と無効化

マルチドメイン ネーム マッピングの検索では、UNIXユーザからWindowsユーザへのネーム マッピングを設定するときに、Windows名のドメイン部分にワイルドカード(\*)を使用できます。名前のドメイン部分にワイルドカード(\*)を使用することで、CIFSサーバのコンピュータ アカウントが含まれるドメインと双方向の信頼関係が確立されているすべてのドメインを検索できるようになります。

#### タスク概要

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。信頼できるドメインのリストを設定すると、Data ONTAPは双方向の信頼関係が確立された検出ドメインの代わりに、信頼できるドメインのリストを使用してマルチドメイン ネーム マッピングの検索を実行します。

- マルチドメイン ネーム マッピングの検索は、デフォルトで有効になっています。
- このオプションは、advanced権限レベルで使用できます。

#### 手順

- 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- 次のいずれかを実行します。

|    | マルチドメイン ネーム マッピングの検索の設定 | 入力するコマンド                                                                                                    |
|----|-------------------------|-------------------------------------------------------------------------------------------------------------|
| 有効 |                         | <code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum-search-enabled true</code>  |
| 無効 |                         | <code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum-search-enabled false</code> |

- admin権限レベルに戻ります。

```
set -privilege admin
```

## 関連参照情報

使用できるCIFSサーバオプション(71ページ)

## 信頼できるドメインのリセットおよび再検出

すべての信頼できるドメインを強制的に再検出することができます。これは、信頼できるドメインサーバが適切に応答しない場合や、信頼関係が変更された場合に役立ちます。CIFSサーバのコンピュータ アカウントを含むドメインであるホーム ドメインと双方向の信頼があるドメインのみが再検出されます。

## 手順

1. `vsserver cifs domain trusts rediscover` コマンドを使用した信頼できるドメインのリセットおよび再検出

### 例

```
vserver cifs domain trusts rediscover -vserver vs1
```

## 関連タスク

検出された信頼できるドメインに関する情報の表示(173ページ)

## 検出された信頼できるドメインに関する情報の表示

CIFSサーバのホームドメインで検出された信頼できるドメインに関する情報を表示できます。ホームドメインとは、CIFSサーバのコンピュータアカウントが含まれるドメインです。この情報は、検出された信頼できるドメインと、検出された信頼できるドメインのリスト内でのそれらの順序を知りたいときに役立ちます。

## タスク概要

ホームドメインと双方向の信頼関係が確立されたドメインのみが検出されます。ホームドメインのドメインコントローラ(DC)は、信頼できるドメインのリストをDCが決めた順序で返すので、リスト内のドメインの順序は予測できません。信頼できるドメインのリストを表示することで、マルチドメインネームマッピングの検索における検索順序を確認できます。

表示される信頼できるドメインの情報は、ノードおよびStorage Virtual Machine(SVM)ごとにグループ化されます。

## 手順

1. `vserver cifs domain trusts show`コマンドを使用して、検出された信頼できるドメインに関する情報を表示します。

### 例

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1  
Vserver: vs1
```

| Home Domain          | Trusted Domain                                         |
|----------------------|--------------------------------------------------------|
| -----<br>EXAMPLE.COM | CIFS1.EXAMPLE.COM,<br>CIFS2.EXAMPLE.COM<br>EXAMPLE.COM |

```
Node: node2  
Vserver: vs1
```

| Home Domain | Trusted Domain                                         |
|-------------|--------------------------------------------------------|
| -----       | -----                                                  |
| EXAMPLE.COM | CIFS1.EXAMPLE.COM,<br>CIFS2.EXAMPLE.COM<br>EXAMPLE.COM |

関連タスク

[信頼できるドメインのリセットおよび再検出](#) (173ページ)

信頼できるドメインのリスト内の信頼できるドメインの追加、削除、または置換

CIFSサーバの信頼できるドメインの優先リストで信頼できるドメインを追加または削除したり、現在のリストを変更したりすることができます。信頼できるドメインの優先リストを設定すると、マルチドメイン ネーム マッピングの検索を実行するときに、検出された双方向に信頼できるドメインの代わりに優先リストが使用されます。

タスク概要

- 信頼できるドメインを既存のリストに追加する場合、新しいリストが既存のリストにマージされ、新しいエントリが末尾に追加されます。信頼できるドメインは、リスト内の順序で検索されます。
- 信頼できるドメインを既存のリストから削除する際にリストを指定しないと、指定したStorage Virtual Machine (SVM) の信頼できるドメインのリスト全体が削除されます。
- 信頼できるドメインの既存のリストを変更すると、新しいリストで上書きされます。

注: 信頼できるドメインのリストには、双方向の信頼関係にあるドメインのみを登録してください。アウトバウンドまたはインバウンドに信頼できるドメインを信頼できるドメインのリストに登録することはできませんが、それらはマルチドメイン ネーム マッピングの検索では使用されません。一方のドメインはスキップされ、リスト内の次の双方向の信頼関係にあるドメインが検索されます。

手順

1. 次のいずれかを実行します。

| 信頼できるドメインのリストに対して行う操作 | 使用するコマンド                                                                                                       |
|-----------------------|----------------------------------------------------------------------------------------------------------------|
| 信頼できるドメインをリストに追加する    | <code>vserver cifs domain name-mapping-search add -vserver vserver_name -trusted-domains FQDN, ...</code>      |
| 信頼できるドメインをリストから削除する   | <code>vserver cifs domain name-mapping-search remove -vserver vserver_name [-trusted-domains FQDN, ...]</code> |
| 既存のリストを変更する           | <code>vserver cifs domain name-mapping-search modify -vserver vserver_name -trusted-domains FQDN, ...</code>   |

-vserver vserver\_nameには、SVM名を指定します。

-trusted-domain FQDNには、ホーム ドメインに対して信頼できるドメインの完全修飾ドメイン名をカンマで区切って指定します。ホーム ドメインは、CIFSサーバのコンピュータ アカウントが含まれるドメインです。

例

次のコマンドを実行すると、SVM vs1で使用される信頼できるドメインの優先リストに2つの信頼できるドメイン(cifs1.example.comおよびcifs2.example.com)が追加されます。

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1 -trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドを実行すると、SVM vs1で使用されるリストから2つの信頼できるドメインが削除されます。

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1 -
trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドを実行すると、SVM vs1で使用される信頼できるドメインのリストが変更されます。元のリストは新しいリストに置き換えられます。

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1 -
trusted-domains cifs3.example.com
```

関連タスク

[信頼できるドメインの優先リストに関する情報の表示](#)(175ページ)

信頼できるドメインの優先リストに関する情報の表示

信頼できるドメインの優先リストに含まれる信頼できるドメインに関する情報、およびマルチドメイン ネーム マッピングの検索が有効な場合の信頼できるドメインの検索順序に関する情報を表示できます。自動検出される信頼できるドメインの優先リストを使用する代わりに、リストを独自に設定することもできます。

手順

- 1. 次のいずれかを実行します。

| 表示する情報                                                        | 使用するコマンド                                                                        |
|---------------------------------------------------------------|---------------------------------------------------------------------------------|
| Storage Virtual Machine (SVM)ごとにグループ化されたクラスタ内のすべての信頼できる優先ドメイン | <code>vserver cifs domain name-mapping-search show</code>                       |
| 指定したSVMのすべての信頼できる優先ドメイン                                       | <code>vserver cifs domain name-mapping-search show -vserver vserver_name</code> |

例

次のコマンドを実行すると、クラスタ上のすべての信頼できる優先ドメインに関する情報が表示されます。

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver      Trusted Domains
-----
vs1          CIFS1.EXAMPLE.COM
```

関連タスク

[信頼できるドメインのリスト内の信頼できるドメインの追加、削除、または置換](#)(174ページ)

SMB共有の作成と設定

ユーザやアプリケーションがSMB経由でCIFSサーバ上のデータにアクセスできるようにするには、SMB共有を作成して設定する必要があります。SMB共有とは、ボリューム内に指定されたアクセ



ポイントです。共有をカスタマイズするには、共有パラメータと共有プロパティを指定します。既存の共有はいつでも変更できます。

SMB共有を作成すると、すべてのメンバーにフルコントロール権限が設定されたACLがデフォルトとして作成されます。

SMB共有は、Storage Virtual Machine (SVM) 上のCIFSサーバに関連付けられます。SVMが削除された場合、またはSMB共有が関連付けられているCIFSサーバがSVMから削除された場合、SMB共有は削除されます。SVMにCIFSサーバを再作成する場合は、SMB共有を再作成する必要があります。

#### 関連コンセプト

[Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み](#) (24ページ)

[SMBを使用したファイル アクセスの管理](#) (216ページ)

[Microsoft Hyper-VおよびSQL Server over SMBソリューション用のData ONTAPの設定](#) (382ページ)

#### 関連タスク

[FlexVolでのSMBファイル名の変換のための文字マッピングの設定](#) (164ページ)

### デフォルトの管理共有とは

Storage Virtual Machine (SVM) 上にCIFSサーバを作成すると、3つのデフォルトの管理共有が自動的に作成されます。これらのデフォルトの共有とその用途について理解しておく必要があります。

CIFSサーバを作成すると、Data ONTAPによって次のデフォルト管理共有が作成されます。

- ipc\$
- admin\$
- c\$

末尾が\$文字である共有は非表示の共有であるため、デフォルトの管理共有はマイ コンピュータには表示されませんが、共有フォルダを使用すると表示することができます。

#### ipc\$およびadmin\$デフォルト管理共有の用途

ipc\$およびadmin\$共有はData ONTAPが使用するものであり、Windows管理者がSVM上にあるデータにアクセスするために使用することはできません。

- ipc\$共有  
ipc\$共有は、プログラム間通信に必要な名前付きパイプを共有するリソースです。ipc\$共有はコンピュータのリモート管理や、コンピュータの共有リソースを表示する際に使用されます。ipc\$共有の共有設定、共有プロパティ、ACLは変更できません。また、ipc\$共有の名前の変更や削除もできません。
- admin\$共有  
admin\$共有は、SVMのリモート管理に使用されます。このリソースのパスは、常にSVMルートへのパスです。admin\$共有の共有設定、共有プロパティ、ACLは変更できません。また、admin\$共有の名前の変更や削除もできません。

#### c\$デフォルト共有の用途

c\$共有は、クラスタまたはSVMの管理者がSVMのルート ボリュームへのアクセスおよび管理に使用できる管理共有です。

c\$共有には、次のような特徴があります。



- この共有へのパスは、常にSVMルート ボリュームへのパスで、変更することはできません。
- c\$共有のデフォルトACLは、Administrator / Full Controlです。  
このユーザは、BUILTIN\administratorです。デフォルトで、BUILTIN\administratorを共有にマッピングでき、マッピングされたルート ディレクトリ内のファイルやフォルダの表示、作成、変更、削除が可能です。このディレクトリ内のファイルやフォルダを管理すると、警告されます。
- c\$共有のACLは変更できます。
- c\$の共有設定や共有プロパティは変更できます。
- c\$共有は削除できません。
- Data ONTAP 8.2.1および8.2リリース ファミリー以降のリリースでは、c\$がSVMの作成時に自動的に作成されるデフォルトの管理共有となっています。
- c\$管理共有の自動作成をサポートしていないバージョンのData ONTAPからアップグレードし、CIFSサーバがSVM上に存在する場合、アップグレード時にc\$共有は自動作成されません。その場合、管理者が手動でc\$共有を作成する必要があります。
- c\$共有をサポートしていないバージョンのData ONTAPにリバートまたはダウングレードし、CIFSサーバがSVM上に存在する場合、c\$管理共有は自動的に削除されません。c\$管理共有は存在し続け、SVMルート ボリュームのファイルやフォルダの管理に使用することができます。
- SVM管理者は、ネームスペース ジャンクションを横断することによって、マッピングされたc\$共有から残りのSVMネームスペースにアクセスできます。
- c\$共有には、Microsoft管理コンソールを使用してアクセスできます。

#### 関連タスク

[Windowsの\[セキュリティ\]タブを使用した標準のNTFSファイル権限の設定](#)(194ページ)

[Windowsの\[セキュリティ\]タブを使用した詳細なNTFSファイル権限の設定](#)(196ページ)

### 共有の命名に関する考慮事項

CIFSサーバでSMB共有を作成するときは、Data ONTAPの共有の命名規則に注意してください。Data ONTAPの共有の命名規則はWindowsの命名規則と同じであり、次の要件が含まれています。

- 共有名はCIFSサーバでそれぞれ一意にする必要があります。
- 共有名の大文字と小文字は区別されません。
- 共有名の長さは最大80文字です。
- 共有名ではUnicodeがサポートされます。
- \$記号で終わる共有名は非表示の共有です。
- 管理用共有のADMIN\$、IPC\$、c\$は、すべてのCIFSサーバで自動的に作成されます。これらの共有名は予約されています。
- 共有の作成時にONTAP\_ADMIN\$という共有名は使用できません。
- 共有名ではスペースの使用がサポートされます。
  - 共有名の先頭または末尾の文字をスペースにすることはできません。
  - スペースを含む共有名は引用符で囲む必要があります。

注: 単一引用符は共有名の一部とみなされ、引用符の代わりに使用することはできません。

- SMB共有の名前では次の特殊文字の使用がサポートされます。  
! @ # \$ % & ' \_ - . ~ ( ) { }
- SMB共有の名前では次の特殊文字の使用はサポートされません。  
+ [ ] " / \ : ; | < > , ? \* =

#### 関連コンセプト

[SMB共有の作成時に必要な情報](#)(179ページ)

#### 関連タスク

[CIFSサーバでのSMB共有の作成](#)(180ページ)

### 非Unicodeクライアントはサポートされない

clustered Data ONTAPはCIFSでのデータ アクセスでは、Unicodeのクライアントのみをサポートしています。

注: Tiger (Mac OS X 10.4.11) や Leopard (Mac OS X 10.5.8) のバージョンで動作する旧タイプの Macintosh クライアントは、SMB リクエストで Unicode を完全にサポートしていません。このような制限事項のため、Data ONTAP 8.2以降では、これらのクライアントをサポートしていません。SMBでマウントを共有する際にMacintoshのクライアントを使用するには、そのクライアントのOSをSnow Leopard (Mac OS X 10.6) 以降にアップグレードする必要があります。

### マルチプロトコル環境で共有を作成する際のディレクトリの大文字と小文字の区別についての考慮事項

名前に大文字小文字だけの違いがあり、ディレクトリ名の区別に8.3の命名方法が使用されている Storage Virtual Machine (SVM) に共有を作成する場合、クライアントが必要なディレクトリ パスに接続できるように共有パスに8.3の名前を使用する必要があります。

次の例では、Linuxクライアントで「testdir」と「TESTDIR」という名前の2つのディレクトリが作成されています。ディレクトリを含むボリュームのジャンクション パスは、/homeです。最初の出力はLinuxクライアントからで、2番目の出力はSMBクライアントからです。

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir
```

```
Directory of Z:\
```

```
04/17/2015 11:23 AM <DIR> testdir
04/17/2015 11:24 AM <DIR> TESTDI~1
```

2番目のディレクトリへの共有を作成する場合、共有パスに8.3の名前を使用する必要があります。この例では、最初のディレクトリの共有パスは/home/testdirで、2番目のディレクトリの共有パスは/home/TESTDI~1です。

### 共有パスの実行権限に関する要件の廃止

8.1.2より前のバージョンのData ONTAPでは、SMB共有を介してフォルダにアクセスするユーザに対して、ネームスペースのルートおよび含まれているパス コンポーネント (ジャンクション ポイント

など)で実行権限を許可していない場合、アクセスが拒否されることがあります。Data ONTAP 8.1.2以降のリリースでは、この制限は廃止されています。

Data ONTAPでは、NAS用の統合されたネームスペースをサポートしています。NASネームスペースは、Storage Virtual Machine (SVM) ネームスペースのルート、およびルート下にサブディレクトリの階層として存在するジャンクションによって結合されたFlexVolで構成されます。このネームスペース階層は、単一のSMB共有としてクライアントに提供されます。つまり、ジャンクションは、複数のボリュームを接合して1つの大きなファイル構造を作ります。

SMBクライアントからネームスペースにアクセスするには、そのネームスペースのルートにマッピングする必要があります。この場合、SVMのデータLIFを介して、ルート下にあるすべてのボリュームにアクセスできるようになります。また、ボリュームのジャンクション ポイントでのマウントやマッピングによって、またはネームスペース内のディレクトリへのパスを使用したマッピングによって、含まれているフレキシブル ボリュームにクライアントからアクセスできるようになります。この場合、結合されたボリューム内に格納されているデータにアクセスするための代替ルートが提供されます。

Data ONTAP 8.1.2より前のバージョンでは、ネームスペースのルートまたはアクセス先フォルダへのパスのコンポーネントでUNIX対応のセキュリティ形式が使用されている場合 (UNIXセキュリティ形式のボリューム、またはUNIX対応のセキュリティを使用するmixedセキュリティ形式のボリュームである場合)、SMBアクセスの問題が発生することがあります。アクセスの問題は、ネームスペースのルートで、およびUNIXセキュリティ形式のパス コンポーネントで、マッピングされたUNIXユーザに実行権限を付与 (所有者、グループ、または他のモードビットによって、あるいはNFSv4 ACLによって) する必要があるという要件が原因で発生することがあります。これは、ネームスペース階層内の共有の場所に関係なく要件となります。この要件は、ネームスペースのルートを含むすべてのボリュームとすべてのLSミラーがNTFSセキュリティ形式である場合には適用されません。

たとえば、/unix1/dir1/dir2/ntfs1/というパスで、unix1がUNIXセキュリティ形式のボリュームであり、ntfs1がNTFSセキュリティ形式のボリュームであり、dir1とdir2が通常のディレクトリであるとしめます。8.1.2よりも前のバージョンのData ONTAPでは、このパスを参照する共有をマッピングするためには、unix1、dir1、およびdir2で実行権限をユーザに付与する必要があります。

Data ONTAP 8.1.2以降では、この制限は廃止されています。実行権限が付与されていなくても、マッピングされたUNIXユーザはSMB共有を介してデータにアクセスできます。これは、ネームスペースのルート、パス内のディレクトリ コンポーネント、または結合されたボリュームのセキュリティ形式に関係なく適用されます。

8.1.2よりも前のバージョンのData ONTAPからData ONTAP 8.1.2以降にアップグレードすると、この要件の廃止によって、有効なアクセス権が変わる場合があることに注意してください。SMBアクセスを制限する方法として実行権限の要件を使用している場合は、適切なアクセス制限を適用するために、共有またはファイルの権限の調整が必要になることがあります。

## SMB共有の作成時に必要な情報

SMB共有を作成する前にあらかじめ、必要となる情報について知っておく必要があります。SMB共有の作成時に指定する必要がある特定のパラメータがあります。また、共有パラメータと共有プロパティについても、いくつか選択すべきことがあります。

共有を作成する場合、次の情報をすべて指定する必要があります。

- 共有を作成するStorage Virtual Machine (SVM) の名前
- ボリューム内での、SMB共有への完全なパス (ボリュームへのジャンクション パスで始まるパス)  
SMB共有パスでは、大文字と小文字が区別されます。
- 共有に接続するときにユーザが入力する共有の名前

共有を作成する場合、共有の説明を任意で指定できます。共有の説明は、ネットワーク上の共有を参照する際に、[Comment]フィールドに表示されます。

オプションで次の共有パラメータを指定できます。

- シンボリックリンクとワイドリンクをサポートするかどうか
- 共有に構成した新規ファイルに対するカスタムのUNIX umaskを構成するかどうか
- 共有に構成した新規ディレクトリに対するカスタムのUNIX umaskを構成するかどうか
- 属性キャッシュに対する、属性キャッシュのカスタムの有効期間を構成するかどうか  
この共有設定は、属性キャッシュの共有プロパティを設定している場合にのみ有効になります。
- オフライン ファイルを構成するかどうか。また、構成する場合、オフライン ファイル設定の指定をするかどうか
- 処理によって共有に対してウィルス スキャンがトリガーされるかどうか。トリガーされる場合、どの処理によってスキャンがトリガーされるか  
ウィルス対策ソリューションの設定の詳細については、『*clustered Data ONTAP ウィルス対策構成ガイド*』を参照してください。
- 最大接続数を指定して、新しい共有への(ノード レベルの)最大接続数を制限するかどうか
- その共有のファイルにアクセスする際にすべてのSMBユーザを割り当てる「強制グループ」を指定するかどうか  
共有が含まれるボリュームやqtreeのセキュリティ形式がmixedまたはUNIXの場合以外は、この共有設定には効果がありません。

オプションで次の共有プロパティを指定できます。

- ホーム ディレクトリ共有とするかどうか
- 便宜的ロックをサポートするかどうか
- 共有が参照可能かどうか
- Snapshotコピーを表示するかどうか
- 変更通知をサポートするかどうか
- メタデータのキャッシングを有効にするかどうか
- 継続的に利用可能な共有とするかどうか
- 共有ファイルに対するBranchCacheハッシュのリクエストをクライアントに許可するかどうか
- 共有がアクセスベースの列挙をサポートするかどうか
- クライアントがディレクトリの列挙結果をキャッシュすることを許可するかどうか(ネームスペースのキャッシュ)
- SVM上の共有にアクセスする際にSMBの暗号化を要求するかどうか

#### 関連コンセプト

[共有の命名に関する考慮事項](#)(177ページ)

#### 関連タスク

[CIFSサーバでのSMB共有の作成](#)(180ページ)

## CIFSサーバでのSMB共有の作成

CIFSサーバ上のデータをSMBクライアントと共有するには、SMB共有を作成する必要があります。共有の作成時に、シンボリックリンクをクライアントに表示する方法を指定するなど、オプション

の設定を指定することで共有をカスタマイズできます。共有の作成時には共有プロパティも設定できます。

## 手順

1. 必要に応じて、共有のディレクトリパス構造を作成します。

共有を作成する前に、`vserver cifs share create`コマンドの`-path`オプションで指定するディレクトリパス構造を作成する必要があります。`vserver cifs share create`コマンドは、共有の作成時に、`-path`オプションに指定されているパスを確認します。指定されているパスが存在しない場合、コマンドは失敗します。

共有のUNCパス(`\\servername\sharename\filepath`)が256文字を超えている場合(UNCパスの先頭の`\\`は除く)、Windowsの[プロパティ]ダイアログ ボックスの[セキュリティ]タブが機能しません。これは、Data ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないようにしてください。

2. 指定したStorage Virtual Machine(SVM)に関連付けられているCIFSサーバでSMB共有を作成します。

```
vserver cifs share create -vserver vserver_name -share-name share_name
-path path [-share-properties share_properties,...] [-symlink-properties
{enable|hide|read_only},...] [-file-umask octal_integer] [-dir-umask
octal_integer] [-comment text] [-attribute-cache-ttl [integerh]]
[integerm][integers]] [-offline-files {none>manual|documents|programs}]
[-vscan-fileop-profile {no-scan|standard|strict|writes-only}] [-max-
connections-per-share integer] [-force-group-for-create UNIX_group_name]
```

`-vserver vserver_name`には、共有を作成するCIFS対応のSVMを指定します。

`-share-name share_name`には、新しいSMB共有の名前を指定します。

- この共有が、`-share-properties`パラメータに`homedirectory`と指定されたホーム ディレクトリ共有である場合は、`%w`(Windowsユーザ名)または`%u`(UNIXユーザ名)動変数を共有名に含める必要があります。  
共有名には、さらに`%d`(ドメイン名)動変数(例:`%d/%w`)や、固定要素(例:`home1_%w`)を含めることもできます。
- 管理者が他のユーザのホーム ディレクトリに接続するために(`vserver cifs home-directory modify`の`-is-home-dirs-access-for-admin-enabled`オプションが`true`に設定されている)、またはユーザが他のユーザのホーム ディレクトリに接続するために(`advanced vserver cifs home-directory modify`の`-is-home-dirs-access-for-public-enabled`オプションが`true`に設定されている)共有を使用する場合は、動的な共有名のパターンの先頭にチルダ(`~`)を付ける必要があります。

`-path path`には、SMB共有のディレクトリパスを指定します。

- このパスが存在している必要があります。
- ディレクトリパス名は、255文字まで入力できます。
- パス名の中でスペースを使用する場合は、文字列全体を引用符で囲む必要があります(例:`"/new volume/mount here"`)。
- 作成する共有がホーム ディレクトリ共有(`-share-properties`パラメータに`homedirectory`を指定)の場合は、このパラメータに`%w`(Windowsユーザ名)変数、`%u`(UNIXユーザ名)変数、`%d`(ドメイン名)変数、またはこれらを組み合わせて指定することで、動的なパス名を指定できます。

`-share-properties share_properties`には、共有のオプションのプロパティを指定します。

- FlexVol上のすべての共有に対するデフォルトの初期プロパティは、**oplocks**、**changenotify**、および**browsable**です。
- 共有の作成時、共有プロパティの指定はオプションです。  
ただし、共有の作成時に共有プロパティを指定する場合、デフォルト値は使用されません。  
共有の作成時に`-share-properties`パラメータを使用する場合は、適用するすべての共有プロパティをカンマで区切って指定する必要があります。
- Infinite Volumeを備えたSVMの場合、デフォルトの初期プロパティは、**oplocks**および**browsable**です。

共有プロパティのリストには、次の1つ以上の値を指定できます。

- **homedirectory**  
ホーム ディレクトリ共有を作成する場合に指定します。CIFSホーム ディレクトリ機能を使用すると、接続するユーザと一連の変数に基づいてさまざまなディレクトリにマッピングされる共有を設定できます。ユーザごとに別個の共有を作成する必要はありません。1つの共有を設定し、いくつかのホーム ディレクトリ パラメータを指定して、エントリ ポイント(共有)とユーザのホーム ディレクトリ(SVM上のディレクトリ)との間のユーザの関係を定義します。  
  
注: 共有の作成後にこのプロパティを追加または削除することはできません。
- **oplocks**  
共有で便宜的ロック(クライアント側キャッシュ)を使用します。共有では、oplockがデフォルトで有効になっています。ただし、oplockが有効になっている場合、アプリケーションによっては適切に機能しないことがあります。特に、Microsoft Accessなどのデータベース アプリケーションは、oplockが有効になっていると破損が発生しやすくなります。  
共有の利点は、単一のパスを複数回共有して、共有ごとに異なるプロパティを設定できることです。たとえば、`/dept/finance`というパスにデータベースとその他の種類のファイルが含まれている場合、このパスに対して2つの共有を作成し、1つは安全なデータベース アクセスのためにoplockを無効にして、もう1つはクライアント側キャッシュのためにoplockを有効にすることができます。
- **browsable**  
共有をWindowsクライアントから参照できるようにします。
- **showsnapshot**  
クライアントがSnapshotコピーを表示およびトラバースできるようにします。
- **changenotify**  
共有で変更通知要求をサポートします。FlexVolを備えたSVMの共有では、これはデフォルトの初期プロパティです。  
Infinite Volumeを備えたSVMの共有では、**changenotify**プロパティはデフォルトでは設定されず、設定するにはadvanced権限レベルが必要です。Infinite Volumeを備えたSVMの共有に**changenotify**プロパティを設定する場合、ファイル属性とタイム スタンプの変更に關する変更通知は送信されません。
- **attributecache**  
属性にすばやくアクセスできるようにSMB共有のファイル属性のキャッシュを有効にします。デフォルトでは、属性のキャッシュは無効になります。このプロパティは、SMB 1.0経由で共有に接続するクライアントがある場合にのみ有効にしてください。クライアントがSMB 2.xまたはSMB 3.0経由で共有に接続している場合、この共有プロパティは適用されません。
- **continuously-available**  
SMB 3.0以降の対応クライアントがファイルを永続的な方法で開くことを許可します。この方法で開いたファイルは、フェイルオーバーやギブバックなど、システムを停止させるイベントから保護されます。このオプションはInfinite Volumeを備えたSVMではサポートされません。

- **branchcache**

この共有内のファイルに対するBranchCacheハッシュの要求をクライアントに許可します。このオプションは、CIFSのBranchCache設定で動作モードとして**per-share**を指定した場合にのみ有効です。このオプションはInfinite Volumeを備えたSVMではサポートされません。

- **access-based-enumeration**

この共有でアクセスベースの列挙(ABE)を有効にします。各ユーザの権限に基づいてABEフィルタを適用した共有フォルダがユーザに表示され、そのユーザが権限を持たないフォルダやその他の共有リソースは表示されないようにします。

- **namespace-caching**

この共有に接続するSMBクライアントが、CIFSサーバから返されたディレクトリの列挙結果をキャッシュできるようにします。これによってパフォーマンスが向上します。デフォルトでは、SMB 1.0クライアントはディレクトリの列挙結果をキャッシュしません。SMB 2.0およびSMB 3.0クライアントではディレクトリの列挙結果がデフォルトでキャッシュされるため、この共有プロパティを指定してパフォーマンスが向上するのはSMB 1.0クライアントの接続のみです。

- **encrypt-data**

この共有へのアクセス時にSMB暗号化の使用を義務付けます。SMBデータへのアクセスで暗号化をサポートしていないSMBクライアントは、この共有にアクセスできません。

-symlink-properties *share\_symlink\_property*は、UNIXシンボリックリンク(symlinks)をSMBクライアントに表示する方法を指定します。次のいずれかの値を指定できます。

- **enabled**

読み取り / 書き込みアクセスに対してシンボリックリンクを有効にします。

- **read\_only**

読み取り専用アクセスに対してシンボリックリンクを有効にします。この設定はワイドリンクには適用されません。ワイドリンク アクセスは常に読み書き可能です。

- **hide**

SMBクライアントにシンボリックリンクが表示されないようにします。

**注:** シンボリックリンクを無効にするには、値を""または"- "に指定します。

-file-umask *octal\_integer*には、共有上に作成された新しいファイルのデフォルトのUNIX umaskを指定します。指定しない場合、umaskはデフォルト値の022になります。

-dir-umask *octal\_integer*には、共有上に作成された新しいディレクトリのデフォルトのUNIX umaskを指定します。指定しない場合、umaskはデフォルト値の000になります。

**注:** -file-umask/パラメータおよび-dir-umask/パラメータの値が異なる複数のSMB共有で既存のディレクトリまたはファイルにアクセスする場合、権限およびアクセス権の一貫性が失われます。たとえば、ファイルのumaskが000である「share1」という名前の共有と、ファイルのumaskが022である「share2」という名前の共有があり、これらの共有が重複する(つまり、同じディレクトリにアクセスできる)とします。\\server\share1\abcという名前のファイルを作成した場合、そのファイルのumaskは000になります。\\server\share2\123という名前のファイルを作成した場合、そのファイルのumaskは022になります。

-comment *text*には、共有の説明を指定します。説明は、255文字まで入力できます。説明の中でスペースを使用する場合は、文字列全体を引用符で囲む必要があります(例: "This is engineering's share.")。

-attribute-cache-ttl *time\_interval*には、属性キャッシュ共有プロパティの有効期間を指定します。このオプションが役立つのは、**attributecache**を-share-properties/パラメータの値に指定している場合だけです。

-offline-filesは、共有からデータにアクセスするときのWindowsクライアントのキャッシュ動作を指定します。次のいずれかの値を指定できます。

- **none**  
Windowsクライアントがこの共有のファイルをキャッシュすることを禁止します。
- **manual**  
Windowsクライアントのユーザが、キャッシュするファイルを手動で選択することを許可します。
- **documents**  
Windowsクライアントがオフライン アクセスのために使用するユーザ文書をキャッシュすることを許可します。
- **programs**  
Windowsクライアントがオフライン アクセスのために使用するプログラムをキャッシュすることを許可します。ユーザは、共有が使用可能な場合でも、キャッシュしたファイルをオフライン モードで使用できます。

-vscan-filop-profileには、ウィルススキャンをトリガーする処理を指定します。次のいずれかの値を指定できます。

- **no-scan**  
この共有に対してウィルススキャンを一切トリガーしません。
- **standard**  
開く、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。これがデフォルト プロファイルです。
- **strict**  
開く、読み取る、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。
- **writes-only**  
変更したファイルを閉じるときにのみウィルススキャンをトリガーします。

ウィルス対策ソリューションの設定の詳細については、『*clustered Data ONTAP ウィルス対策構成ガイド*』を参照してください。

-max-connections-per-shareには、共有での同時接続の最大数を指定します。

- 上限はSVM単位やクラスタ単位ではなく、ノード単位です。
- デフォルト値は4294967295で、これがこのパラメータの最大値です。

注: 単一セッションで使用できるツリー接続の最大数は4096で、この値は設定できません。

-force-group-for-createでは、SMBユーザが特定の共有内に作成するすべてのファイルが同じグループ (フォースグループとも呼ばれる) に属することを指定します。フォースグループは、UNIXグループ データベース (ファイル、NIS、またはLDAP) に存在している必要があります。この設定は、ボリュームのセキュリティ形式がUNIXセキュリティ形式またはmixedセキュリティ形式でなければ無効です。この設定を指定した場合、共有は次のようになります。

- この共有にアクセスするSMBユーザのプライマリGIDは、フォースグループのGIDに一時的に変更されます。
- SMBユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリGIDに関係なく、同じフォースグループに属します。

#### 例

次のコマンドを実行すると、「SHARE1」という名前のSMB共有がStorage Virtual Machine (SVM、旧Vserver) 「vs1」に作成されます。ディレクトリ パスは/u/engです。oplocksと



browsableを共有に指定し、ファイルには**022**、ディレクトリには**000**のUNIX umaskを明示的に設定します。

```
cluster1:> vserver cifs share create -vserver vs1 -share-name
SHARE1 -path /u/eng -share-properties browsable,oplocks -file-umask
022 -dir-umask 000
```

次のコマンドを実行すると、「DOCUMENTS」という名前のSMB共有がSVM「vs1」に作成されます。共有のパスは/documentsです。この共有では、便宜的ロック(クライアント側キャッシュ)を使用し、変更が発生したときには通知を生成し、クライアントがこの共有上でユーザ文書をキャッシュすることを許可します。

```
cluster1:> vserver cifs share create -vserver vs1 -share-name
DOCUMENTS -path /documents -share-properties changenotify,oplocks -
offline-files documents
```

## 関連コンセプト

- [デフォルトの管理共有とは](#)(176ページ)
- [共有の命名に関する考慮事項](#)(177ページ)
- [SMB共有の作成時に必要な情報](#)(179ページ)
- [トラバース チェックのバイパスの設定](#)(242ページ)
- [フォースグループの共有設定を使用してSMBユーザ アクセスを最適化する方法](#)(185ページ)
- [SMB共有のACLを使用したファイル アクセスの保護](#)(190ページ)
- [ファイル権限を使用したファイル アクセスの保護](#)(193ページ)

## 関連タスク

- [FlexVolでのSMBファイル名の変換のための文字マッピングの設定](#)(164ページ)
- [フォースグループ共有設定を使用したSMB共有の作成](#)(186ページ)
- [SMBセッション情報の表示](#)(306ページ)
- [開いているSMBファイルに関する情報の表示](#)(308ページ)
- [既存のSMB共有に対する共有プロパティの追加または削除](#)(187ページ)

## フォースグループの共有設定を使用してSMBユーザ アクセスを最適化する方法

Data ONTAPコマンドラインから、UNIX対応のセキュリティを使用するデータへの共有を作成するときに、SMBユーザがその共有内に作成するすべてのファイルがフォースグループと呼ばれる同じグループに属するように指定できます。このグループは、UNIXグループ データベース内で事前に定義されている必要があります。フォースグループを使用すると、さまざまなグループに属するSMBユーザがファイルに確実にアクセスできるようになります。

フォースグループの指定は、共有がUNIXまたはmixedセキュリティ形式のqtreeにある場合にのみ意味があります。NTFSセキュリティ形式のボリュームまたはqtreeにある共有内のファイルへのアクセスは、UNIXのGIDではなくWindowsの権限によって判断されるため、これらの共有にフォースグループを設定する必要はありません。

共有にフォースグループが指定されている場合、次のようになります。

- この共有にアクセスするフォースグループ内のSMBユーザは、フォースグループのGIDに一時的に変更されます。  
このGIDを使用すると、フォースグループを含んだ共有内のファイルにアクセスできます。通常、このファイルには、プライマリGIDまたはUIDではアクセスできません。
- SMBユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリGIDに関係なく、同じフォースグループに属します。

SMBユーザが、NFSユーザによって作成されたファイルにアクセスしようすると、SMBユーザのプライマリGIDによって、権限があるかどうか判断されます。

フォースグループは、NFSユーザがこの共有内のファイルにアクセスする方法には影響を与えません。NFSユーザが作成したファイルは、ファイル所有者からGIDを取得します。アクセス権の決定はファイルにアクセスしようとしているNFSユーザのUIDおよびプライマリGIDに基づきます。

フォースグループを使用すると、さまざまなグループに属するSMBユーザがファイルに確実にアクセスできるようになります。たとえば、会社のWebページを保存する共有を作成し、EngineeringグループとMarketingグループのユーザに書き込みアクセス権を付与する必要がある場合、共有を作成して、「webgroup1」という名前のフォースグループに書き込み権限を与えます。フォースグループが指定されているため、SMBユーザがこの共有内に作成するすべてのファイルは「webgroup1」グループによって所有されます。さらに、ユーザが共有にアクセスするときは、「webgroup1」グループのGIDが自動的に割り当てられます。このため、EngineeringグループとMarketingグループのユーザの権限を管理しなくても、すべてのユーザがこの共有に書き込むことができます。

### 関連タスク

[フォースグループ共有設定を使用したSMB共有の作成](#) (186ページ)

## フォースグループ共有設定を使用したSMB共有の作成

UNIXファイル セキュリティ形式のボリュームやqtreeにあるデータにアクセスするSMBユーザが、同じUNIXグループに属しているとData ONTAPでみなされるようにするには、フォースグループ共有設定を使用してSMB共有を作成します。

### 手順

1. SMB共有を作成します。

```
vserver cifs share create -vserver vserver_name -share-name share_name -  
path path -force-group-for-create UNIX_group_name
```

-share-name *share\_name*には、新しいSMB共有の名前を256文字以内で指定します。

-path *path*には、共有のパスを指定します。パスの区切り文字には、スラッシュまたはバックスラッシュを使用できますが、Data ONTAPでは、どちらもスラッシュとして表示されます。

共有のUNCパス(\\servername\sharename\filepath)が256文字を超えている場合(UNCパスの先頭の「\\」は除く)、Windowsの[プロパティ]ダイアログ ボックスの[セキュリティ]タブが機能しません。これは、Data ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないようにしてください。

-force-group-for-create *UNIX\_group\_name*には、フォースグループとして使用するUNIXグループの名前を指定します。

共有の作成後にフォースグループを削除する場合は、-force-group-for-createパラメータの値に空の文字列("")を指定して共有を変更します。共有を変更してフォースグループを削除した場合、この共有への既存のすべての接続には、引き続き以前に設定されたフォースグループがプライマリGIDとして使用されます。

### 例

次のコマンドを実行すると、Webでアクセス可能な「webpages」共有が/corp/companyinfoディレクトリに作成されます。SMBユーザがこのディレクトリ内に作成するすべてのファイルは、webgroup1グループに割り当てられます。

```
vserver cifs share create -vserver vs1 -share-name webpages -path /  
corp/companyinfo -force-group-for-create webgroup1
```

関連コンセプト

[フォースグループの共有設定を使用してSMBユーザアクセスを最適化する方法](#)(185ページ)

関連タスク

[CIFSサーバでのSMB共有の作成](#)(180ページ)

既存のSMB共有に対する共有プロパティの追加または削除

共有プロパティを追加または削除することで、既存のSMB共有をカスタマイズできます。この方法は、環境内での要件の変化に合わせて共有の設定を変更する場合に役立ちます。

開始する前に

プロパティを変更する共有が存在している必要があります。

タスク概要

共有プロパティを追加する場合は、次の点に注意してください。

- カンマで区切って指定することで、1つ以上の共有プロパティを追加できます。
- 以前に指定した共有プロパティは有効なままです。  
新たに追加したプロパティは、共有プロパティの既存のリストに追加されます。
- 共有にすでに適用されている共有プロパティに新しい値を指定した場合は、元の値が新たに指定した値に置き換えられます。
- `vserver cifs share properties add`コマンドでは共有プロパティを削除できません。  
共有プロパティを削除するには、`vserver cifs share properties remove`コマンドを使用してください。

共有プロパティを削除する場合は、次の点に注意してください。

- カンマで区切って指定することで、1つ以上の共有プロパティを削除できます。
- 以前に指定した共有プロパティは、削除しないかぎり有効なままです。

使用可能な共有プロパティは次のとおりです。

| 共有プロパティ      | 説明                                                                                                                                                                                                                                                |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oplocks      | 便宜的ロック( クライアント側キャッシュ)を共有で使用することを指定します。                                                                                                                                                                                                            |
| browsable    | Windowsクライアントが共有を参照することを許可します。                                                                                                                                                                                                                    |
| showsnapshot | クライアントがSnapshotコピーを表示およびトラバースできることを指定します。                                                                                                                                                                                                         |
| changenotify | 共有が変更通知 要求をサポートすることを指定します。FlexVolを備えたSVM上の共有では、これはデフォルトの初期プロパティです。Infinite Volumeを備えたSVM上の共有では、changenotifyプロパティはデフォルトでは設定されず、設定するためにはadvanced権限レベルが必要です。Infinite Volumeを備えたSVM上の共有にchangenotifyプロパティを設定する場合、ファイル属性およびタイムスタンプの変更に関する変更通知は送信されません。 |

| 共有プロパティ                  | 説明                                                                                                                                                                                                                                |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| attributecache           | 属性にすばやくアクセスできるようにSMB共有でのファイル属性のキャッシュを有効にします。デフォルトでは、属性のキャッシュは無効です。このプロパティは、SMB 1.0経由で共有に接続するクライアントがある場合にのみ有効にしてください。クライアントがSMB 2.xまたはSMB 3.0経由で共有に接続している場合、この共有プロパティは適用されません。                                                     |
| continuously-available   | SMBクライアントが 永続的な方法でファイルを開くことを許可します。この方法で開いたファイルは、フェイルオーバーやギブバックなど、システムを停止させるイベントから保護されます。                                                                                                                                          |
| branchcache              | その共有内でファイルの BranchCacheハッシュをクライアントが要求できることを指定します。このオプションが役立つのは、CIFSの BranchCache設定の動作モードとして「per-share」を指定する場合だけです。                                                                                                                |
| access-based-enumeration | このプロパティは、この共有で <b>アクセス ベースの列挙(ABE)</b> を有効にするように指定します。各ユーザの権限に基づいてABEフィルタを適用した共有フォルダがユーザに表示され、そのユーザが権限を持たないフォルダやその他の共有リソースは表示されないようにします。                                                                                          |
| namespace-caching        | このプロパティは、この共有に接続するSMBクライアントが、CIFSサーバが返すディレクトリの列挙結果をキャッシュできることを指定します。これによって、パフォーマンスが向上します。デフォルトでは、SMB 1のクライアントはディレクトリの列挙結果をキャッシュしません。SMB 2およびSMB 3クライアントはデフォルトでディレクトリ列挙結果をキャッシュするため、この共有プロパティを指定してパフォーマンスが向上するのはSMB 1クライアント接続のみです。 |
| encrypt-data             | この共有へのアクセス時にSMB暗号化の使用を義務付けます。SMBデータへのアクセスで暗号化をサポートしていないSMBクライアントは、この共有にアクセスできません。                                                                                                                                                 |

## 手順

- 適切なコマンドを入力します。

| 状況           | 入力するコマンド                                                                                                                        |
|--------------|---------------------------------------------------------------------------------------------------------------------------------|
| 共有プロパティを追加する | <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties properties,...</code>    |
| 共有プロパティを削除する | <code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties properties,...</code> |

- `-vserver vserver_name`は、プロパティを変更する共有を含むStorage Virtual Machine (SVM)の名前を指定します。
- `-share-name share_name`は、プロパティを変更する共有の名前です。
- `-share-properties properties`は、追加または削除する共有プロパティのリストです。

- 共有プロパティの設定を確認します。

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

**例**

次のコマンドでは、SVM vs1上の「share1」という名前の共有にshowsnapshot共有プロパティを追加します。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot
```

```
cluster1::> vserver cifs share show -vserver vs1
```

| Vserver | Share  | Path    | Properties                                           | Comment | ACL                     |
|---------|--------|---------|------------------------------------------------------|---------|-------------------------|
| vs1     | share1 | /share1 | oplocks<br>browsable<br>changenotify<br>showsnapshot | -       | Everyone / Full Control |

次のコマンドでは、SVM vs1上の「share2」という名前の共有からbrowsable共有プロパティを削除します。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable
```

```
cluster1::> vserver cifs share show -vserver vs1
```

| Vserver | Share  | Path    | Properties              | Comment | ACL                     |
|---------|--------|---------|-------------------------|---------|-------------------------|
| vs1     | share2 | /share2 | oplocks<br>changenotify | -       | Everyone / Full Control |

**関連タスク**

[CIFSサーバでのSMB共有の作成](#) (180ページ)

**関連参照情報**

[SMB共有の管理用コマンド](#) (190ページ)

**MMCを使用したSVM共有情報の表示**

MMC (Microsoft Management Console) を使用して Storage Virtual Machine (SVM) のSMB共有情報を表示できます。共有を表示する前に、MMCをSVMに接続する必要があります。

**手順**

1. WindowsサーバでMMCを開くには、エクスプローラでローカル コンピュータのアイコンを右クリックし、**[管理]**を選択します。
2. 左側のパネルで、**[コンピュータの管理]**を選択します。
3. **[操作] > [別のコンピュータへ接続]**を選択します。  
[コンピュータの選択]ダイアログ ボックスが表示されます。
4. ストレージ システムの名前を入力するか、**[参照]**をクリックしてストレージ システムを指定します。
5. **[OK]**をクリックします。  
MMCがSVMに接続します。
6. 次の手順を実行します。
  - a. [コンピュータの管理]ページの左側のナビゲーション ペインで、**[システム ツール]**階層を展開します。

「The remote procedure call failed and did not execute(1727)」というエラーメッセージが表示されます。右側の表示ペインは空白のままになります。これは、このバージョンのData ONTAPの既知の問題です。

- b. この問題を回避するには、[OK]をクリックしてエラー ボックスを閉じ、再度[システム ツール]をクリックします。

[システム ツール]階層を展開します。

7. ナビゲーション ペインで、[共有フォルダ] > [共有]をクリックします。

右側の表示ペインにSVMの共有のリストが表示されます。

8. 共有の共有プロパティを表示するには、共有をダブルクリックして[プロパティ]ボックスを開きます。

#### 関連コンセプト

[SMB共有レベルACLの管理](#)(191ページ)

## SMB共有の管理用コマンド

vserver cifs shareおよびvserver cifs share propertiesコマンドを使用して、SMB共有を管理できます。

| 状況                  | 使用するコマンド                             |
|---------------------|--------------------------------------|
| SMB共有を作成する          | vserver cifs share create            |
| SMB共有を表示する          | vserver cifs share show              |
| SMB共有を変更する          | vserver cifs share modify            |
| SMB共有を削除する          | vserver cifs share delete            |
| 既存の共有に共有プロパティを追加する  | vserver cifs share properties add    |
| 既存の共有から共有プロパティを削除する | vserver cifs share properties remove |
| 共有プロパティについての情報を表示する | vserver cifs share properties show   |

詳細については、各コマンドのマニュアル ページを参照してください。

## SMB共有のACLを使用したファイル アクセスの保護

SMB共有で共有のアクセス制御リスト(ACL)を設定することで、ネットワークを介したファイルやフォルダへのアクセスを保護することができます。共有レベルのACLとファイルレベルの権限を組み合わせ、必要に応じてエクスポート ポリシーも使用して、有効なアクセス権を決定できます。

ACLを設定するときは、ドメインまたはローカルのユーザやグループを使用できます。

#### 関連コンセプト

[Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み](#)(24ページ)

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#)(154ページ)

[ファイル権限を使用したファイル アクセスの保護](#)(193ページ)

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)

**関連タスク**

[CIFSサーバでのSMB共有の作成](#)(180ページ)

[SMB共有のACLの作成](#)(191ページ)

[セキュリティレースの実行](#)(292ページ)

**SMB共有レベルACLの管理**

共有レベルのACLを変更すると、共有に設定する権限を強化したり、軽減したりできます。WindowsのユーザとグループまたはUNIXのユーザとグループのどちらかを使用して共有レベルACLを設定できます。

共有を作成すると、共有レベルのACLのデフォルトでは、Everyoneという名前の標準グループに読み取り権限が与えられます。ACLに読み取り権限が設定されているため、ドメイン内およびすべての信頼できるドメイン内のすべてのユーザに共有への読み取り専用権限が与えられます。

共有レベルのACLを変更するには、WindowsクライアントのMicrosoft管理コンソール(MMC)またはData ONTAPコマンドラインを使用します。

MMCを使用する際には、次の点に留意してください。

- 指定したユーザ名およびグループ名はWindows名である必要があります。
- Windows権限だけを指定できます。

Data ONTAPコマンドラインを使用する際には、次の点に留意してください。

- ユーザ名およびグループ名には、Windows名またはUNIX名を使用できます。  
ACLの作成時や変更時に指定されない場合、デフォルトのタイプはWindowsのユーザとグループになります。
- Windows権限だけを指定できます。

**関連タスク**

[MMCを使用したSVM共有情報の表示](#)(189ページ)

**Data ONTAPでの共有レベルのACLの使用方法**

共有レベルのACLは、Access Control Entry (ACE; アクセス制御エントリ) のリストで構成されます。各ACEには、ユーザまたはグループの名前と、共有が含まれるボリュームまたはqtreeのセキュリティ形式に関係なく、そのユーザまたはグループの共有へのアクセスを決定する一連の権限が含まれています。

SMBユーザが共有にアクセスするたびに、Data ONTAPは共有レベルのACLを確認し、アクセスを許可するかどうかを判断します。

共有レベルのACLは共有内のファイルへのアクセスを制限するもので、ファイルレベルのACLを超える権限を付与することはありません。

**SMB共有のACLの作成**

SMB共有のAccess Control List (ACL; アクセス制御リスト) を作成して共有権限を設定すると、ユーザとグループの共有に対するアクセス レベルを制御できます。

**タスク概要**

ローカルまたはドメインのWindowsユーザまたはグループ名、あるいはUNIXユーザまたはグループ名を使用して共有レベルのACLを設定できます。

- ドメインのWindowsユーザ名を指定する場合は、domain\username形式でユーザのドメインを指定する必要があります。



- user-or-groupパラメータの値は、大文字と小文字が区別されないテキストです。
- permissionパラメータには、次のいずれかの値を指定できます。

- **No\_access**
- **Read**
- **Change**
- **Full\_Control**

## 手順

1. ACLを設定します。

| 設定するACLに使用するアカウント | 入力するコマンド                                                                                                                                                                                      |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windowsユーザ        | <code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name \user_name -permission access_right</code> |
| Windowsグループ       | <code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>             |
| UNIXユーザ           | <code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</code>               |
| UNIXグループ          | <code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</code>             |

2. `vserver cifs share access-control show`コマンドを使用して、共有に適用されたACLが正しいことを確認します。

次のコマンドを実行すると、Storage Virtual Machine(SVM)「vs1」上の「sales」共有に対して、「salesteam」Windowsグループに**Change**権限が付与されます。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share sales -user-or-group salesteam -permission Change

cluster1::> vserver cifs share access-control show
```

| Vserver | Share Name | User/Group Name        | User/Group Type | Access Permission |
|---------|------------|------------------------|-----------------|-------------------|
| vs1     | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs1     | sales      | salesteam              | windows         | Change            |

次のコマンドを実行すると、SVM「vs2」上の「eng」共有に対して、「engineering」UNIXグループに**Read**権限が付与されます。

```
cluster1::> vserver cifs share access-control create -vserver vs2 -share eng -user-group-type unix-group -user-or-group eng -permission Read

cluster1::> vserver cifs share access-control show
```

| Share | User/Group  | User/Group | Access |
|-------|-------------|------------|--------|
| eng   | engineering | unix-group | Read   |



| Vserver | Name | Name                   | Type       | Permission   |
|---------|------|------------------------|------------|--------------|
| vs2     | c\$  | BUILTIN\Administrators | windows    | Full_Control |
| vs2     | eng  | engineering            | unix-group | Read         |

次のコマンドを実行すると、SVM「vs1」上の「datavol5」共有に対して、「group1」という名前のローカルWindowsグループには**Change**権限が、「user1」という名前のローカルWindowsユーザには**Full\_Control**権限が付与されます。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share datavol5 -user-group-type windows -user-or-group group1 -permission Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share datavol5 -user-group-type windows -user-or-group user1 -permission Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
```

| Vserver | Share Name | User/Group Name        | User/Group Type | Access Permission |
|---------|------------|------------------------|-----------------|-------------------|
| vs1     | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs1     | datavol5   | group1                 | windows         | Change            |
| vs1     | datavol5   | user1                  | windows         | Full_Control      |

#### 関連タスク

[CIFSサーバでのSMB共有の作成](#) (180ページ)

### SMB共有アクセス制御リストの管理用コマンド

アクセス制御リスト(ACL)の作成、表示、変更、削除などを含む、SMBのACL管理用コマンドについて説明します。

| 状況          | 使用するコマンド                                              |
|-------------|-------------------------------------------------------|
| 新しいACLを作成する | <code>vserver cifs share access-control create</code> |
| ACLを表示する    | <code>vserver cifs share access-control show</code>   |
| ACLを変更する    | <code>vserver cifs share access-control modify</code> |
| ACLを削除する    | <code>vserver cifs share access-control delete</code> |

### ファイル権限を使用したファイル アクセスの保護

データにアクセスするためにSMBクライアントがアクセスする共有に格納されたファイルやフォルダに対してファイル権限を設定することで、アクセスを保護することができます。ファイルレベルの権限と共有レベルのACLを組み合わせ、必要に応じてエクスポート ポリシーも使用して、有効なアクセス権を決定できます。ファイルとフォルダは、NTFS権限やUNIX権限で保護されることもあります。

ファイルやフォルダがUNIXのファイル権限で保護されている場合は、マッピングされているUNIXユーザやそのグループに基づいてファイル権限が評価されます。

#### 関連コンセプト

[セキュリティ形式がデータ アクセスに与える影響](#) (20ページ)

[FlexVolを備えたSVMでのネーム マッピングを使用したSMBファイル アクセスの保護方法](#) (23ページ)

[Data ONTAPでファイルおよびディレクトリへのアクセスが保護される仕組み](#) (24ページ)

[SMB共有のACLを使用したファイル アクセスの保護](#) (190ページ)

[SMB経由でファイルにアクセスする際のUNIXファイル権限によるアクセス制御方法](#) (199ページ)

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#)(154ページ)

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#)(200ページ)

## 関連タスク

[セキュリティレースの実行](#)(292ページ)

## Windowsの[セキュリティ]タブを使用した標準のNTFSファイル権限の設定

Windowsの[プロパティ]ウィンドウにあるWindowsの[セキュリティ]タブを使用して、ファイルやディレクトリに対する標準のNTFSファイル権限を設定できます。これはWindowsクライアント上に存在するデータに対する標準のファイル権限を設定する場合と同じ方法です。

### 開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分なNTFS権限を持っている必要があります。

### タスク概要

NTFSファイル権限の設定は、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List(DACL; 随意アクセス制御リスト)にエントリを追加することによって行います。その後、セキュリティ記述子をNTFSファイルおよびディレクトリに適用します。これらのタスクはWindows GUIによって自動的に処理されます。セキュリティ記述子には、ファイルやフォルダのアクセス権を適用するためのDACL、ファイルやフォルダを監査するためのシステム アクセス制御リスト(SACL)、またはSACLとDACLの両方を含めることができます。

Windowsホストで次の手順を実行することで、ファイルやフォルダに対する標準のNTFSファイル権限を設定できます。

### 手順

1. Windowsエクスプローラの[ツール]メニューで、[ネットワークドライブの割り当て]を選択します。
2. [ネットワークドライブの割り当て]ボックスのすべての項目に入力します。
  - a. [ドライブ]文字を選択します。
  - b. [フォルダ]ボックスに、権限を適用するデータが格納された共有を含むCIFSサーバの名前と、その共有の名前を入力します。

### 例

CIFSサーバ名がCIFS\_SERVERで、共有の名前が「share1」である場合は、「\CIFS\_SERVER\share1」と入力します。

注: CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

- c. [完了]をクリックします。

選択したドライブがマウントされて使用可能な状態となり、共有内に格納されているファイルやフォルダがWindowsエクスプローラ ウィンドウに表示されます。

3. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリで右クリックし、[プロパティ]を選択します。
5. [セキュリティ]タブを選択します。

[セキュリティ]タブには、NTFS権限が設定されているユーザとグループの一覧が表示されます。[<Object> のアクセス許可]ボックスには、選択したユーザまたはグループに対して有効な権限が[許可]および[拒否]の設定とともに一覧表示されます。

6. **[編集]**をクリックします。

[<Object> のアクセス許可]ボックスが開きます。

7. 次のうち必要な操作を実行します。

| 目的                                | 操作                                                                                                                                                                                            |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しいユーザまたはグループに対する標準のNTFS権限を設定する   | <p>a. <b>[追加]</b>をクリックします。<br/>[ユーザー、コンピューター、サービス アカウントまたはグループの選択]ウィンドウが開きます。</p> <p>b. <b>[選択するオブジェクト名を入力してください]</b>ボックスに、NTFS権限を追加するユーザまたはグループの名前を入力します。</p> <p>c. <b>[OK]</b>をクリックします。</p> |
| ユーザまたはグループに対する標準のNTFS権限を変更または削除する | <b>[グループ名またはユーザー名]</b> ボックスで、変更または削除するユーザまたはグループを選択します。                                                                                                                                       |

8. 次のうち必要な操作を実行します。

| 状況                                   | 操作                                                                                                                     |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 新規または既存のユーザまたはグループに対する標準のNTFS権限を設定する | <b>[&lt;Object&gt; のアクセス許可]</b> ボックスで、選択したユーザまたはグループに対して許可または拒否するアクセス タイプの <b>[許可]</b> ボックスまたは <b>[拒否]</b> ボックスを選択します。 |
| ユーザまたはグループを削除する                      | <b>[削除]</b> をクリックします。                                                                                                  |

標準の権限は、より詳細なアクセス権をまとめたものです。次のような標準の権限を設定できます。

- フル コントロール
- 変更
- 読み取りと実行
- フォルダの内容の一覧表示
- 読み取り
- 書き込み

注: 標準の権限ボックスを選択できないことがありますが、親オブジェクトから権限が継承されているためです。**[特殊なアクセス許可]**ボックスは選択できません。選択されている場合は、選択したユーザまたはグループに対して詳細な権限が1つ以上設定されていることを意味します。

9. そのオブジェクトに対するNTFS権限の追加、削除、または編集が完了したら、**[OK]**をクリックします。

標準のNTFS権限を設定する方法の詳細については、Windowsのマニュアルを参照してください。

## 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用](#) (261ページ)

[NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (247ページ)

[mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (250ページ)

[UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (252ページ)

## Windowsの[セキュリティ]タブを使用した詳細なNTFSファイル権限の設定

Windowsの[プロパティ]ウィンドウにあるWindowsの[セキュリティ]タブを使用して、ファイルやフォルダに対する標準のNTFSファイル権限を設定できます。

### 開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分なNTFS権限を持っている必要があります。

### タスク概要

NTFSファイル権限を設定するには、Windowsホストで、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List (DACL; 随意アクセス制御リスト) にエントリを追加します。その後、セキュリティ記述子をNTFSファイルおよびディレクトリに適用します。これらのタスクはWindows GUIによって自動的に処理されます。

### 手順

1. Windowsエクスプローラの[ツール]メニューで、[ネットワークドライブの割り当て]を選択します。
2. [ネットワークドライブの割り当て]ダイアログ ボックスのすべての項目に入力します。
  - a. [ドライブ]文字を選択します。
  - b. [フォルダ]ボックスに、権限を適用するデータが格納された共有を含むCIFSサーバの名前と、その共有の名前を入力します。

### 例

CIFSサーバ名が「CIFS\_SERVER」で共有名が「share1」の場合は、\\CIFS\_SERVER\share1と入力します。

**注:** CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

- c. [完了]をクリックします。

選択したドライブがマウントされて使用可能な状態となり、共有内に格納されているファイルやフォルダがWindowsエクスプローラ ウィンドウに表示されます。

3. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリで右クリックし、[プロパティ]を選択します。
5. [セキュリティ]タブを選択します。
 

[セキュリティ]タブには、NTFS権限が設定されているユーザとグループの一覧が表示されます。[アクセス許可]ボックスに、選択したユーザまたはグループごとに有効になっている権限の許可および拒否のリストが表示されます。
6. [詳細]をクリックします。

Windowsの[プロパティ]ウィンドウに、ユーザおよびグループに割り当てられている既存のファイル権限に関する情報が表示されます。

7. **[アクセス許可の変更]**をクリックします。

[アクセス許可]ウィンドウが開きます。

8. 次のうち必要な操作を実行します。

| 状況                           | 操作                                                                                                                      |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| 新しいユーザまたはグループの詳細なNTFS権限を設定する | a. <b>[追加]</b> をクリックします。<br>b. <b>[選択するオブジェクト名を入力してください]</b> ボックスに、追加するユーザまたはグループの名前を入力します。<br>c. <b>[OK]</b> をクリックします。 |
| ユーザまたはグループの詳細なNTFS権限を変更する    | a. <b>[アクセス許可エントリ:]</b> ボックスで、詳細な権限を変更するユーザまたはグループを選択します。<br>b. <b>[編集]</b> をクリックします。                                   |
| ユーザまたはグループの詳細なNTFS権限を削除する    | a. <b>[アクセス許可エントリ:]</b> ボックスで、削除するユーザまたはグループを選択します。<br>b. <b>[削除]</b> をクリックします。<br>c. 手順13に進みます。                        |

新しいユーザまたはグループに詳細なNTFS権限を追加する場合、または既存のユーザまたはグループの詳細なNTFS権限を変更する場合は、[<Object>のアクセス許可エントリ]ボックスが開きます。

9. **[適用先]**ボックスで、このNTFSファイル権限エントリをどのように適用するかを選択します。

次のいずれかを選択できます。

- このフォルダ、サブフォルダおよびファイル
- このフォルダとサブフォルダ
- このフォルダのみ
- このフォルダとファイル
- サブフォルダとファイルのみ
- サブフォルダのみ
- ファイルのみ

単一ファイルに対してNTFSファイル権限を設定する場合、**[適用先]**ボックスはアクティブになりません。**[適用先]**の設定はデフォルトで**[このオブジェクトのみ]**になります。

10. **[アクセス許可]**ボックスで、このオブジェクトに対して設定する詳細な権限の**[許可]**ボックスまたは**[拒否]**ボックスを選択します。

- 指定のアクセスを許可する場合は、**[許可]**ボックスを選択します。
- 指定のアクセスを許可しない場合は、**[拒否]**ボックスを選択します。

次の詳細な権限に関する許可を設定できます。

- **フル コントロール**  
この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます(それらの権限が許可または拒否されます)。
- **フォルダのスキャン / ファイルの実行**
- **フォルダの一覧 / データの読み取り**
- **属性の読み取り**
- **拡張属性の読み取り**
- **ファイルの作成 / データの書き込み**
- **フォルダの作成 / データの追加**
- **属性の書き込み**
- **拡張属性の書き込み**
- **サブフォルダとファイルの削除**
- **削除**
- **アクセス許可の読み取り**
- **アクセス許可の変更**
- **所有権の取得**

注: いずれかの詳細な権限ボックスが選択可能になっていない場合、その権限は親オブジェクトから継承されます。

11. このオブジェクトのサブフォルダおよびファイルにこれらの権限が継承されるようにする場合は、**[これらのアクセス許可を、このコンテナの中にあるオブジェクトやコンテナにのみ適用する]**ボックスを選択します。
12. **[OK]**をクリックします。
13. NTFS権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。
  - **[このオブジェクトの親からの継承可能なアクセス許可を含める]**ボックスを選択します。  
この値がデフォルトです。
  - **[子オブジェクトのアクセス許可すべてを、このオブジェクトからの継承可能なアクセス許可で置き換える]**ボックスを選択します。  
単一ファイルに対してNTFSファイル権限を設定する場合、この設定は**[アクセス許可]**ボックスに表示されません。  
  
 注: この設定を選択する場合は注意が必要です。この設定を選択すると、すべての子オブジェクトの既存の権限がすべて削除され、このオブジェクトの権限の設定に置き換えられます。削除するつもりがなかった権限が誤って削除される可能性があります。これは、mixedセキュリティ形式のボリュームまたはqtreeで権限を設定する場合に特に重要です。子オブジェクトがUNIX対応のセキュリティ形式を使用している場合に、このような子オブジェクトにNTFS権限を適用すると、Data ONTAPによってこれらのオブジェクトがUNIXセキュリティ形式からNTFSセキュリティ形式に変更され、これらの子オブジェクトのすべてのUNIX権限がNTFS権限に置き換えられます。
  - 両方のボックスを選択します。
  - どちらのボックスも選択しない。

14. [OK]をクリックして、[アクセス許可]ボックスを閉じます。
15. [OK]をクリックして、[<Object>のセキュリティの詳細設定]ボックスを閉じます。

詳細なNTFS権限の設定方法の詳細については、Windowsのマニュアルを参照してください。

#### 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用](#) (261ページ)

[NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (247ページ)

[mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (250ページ)

[UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (252ページ)

### Data ONTAP CLIを使用したNTFSファイル権限の設定方法

Data ONTAP CLIを使用して、ファイルおよびディレクトリに対してNTFSファイル権限を設定できます。これにより、WindowsクライアントでSMB共有を使用してデータに接続することなくNTFSファイル権限を設定できます。

NTFSファイル権限を設定するには、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List (DACL; 随意アクセス制御リスト) にエントリを追加します。その後、セキュリティ記述子をNTFSファイルおよびディレクトリに適用します。

コマンドラインで設定できるのはNTFSファイル権限だけです。CLIでNFSv4 ACLを設定することはできません。

#### 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用](#) (261ページ)

### SMB経由でファイルにアクセスする際のUNIXファイル権限によるアクセス制御方法

FlexVolでは、NTFS、UNIX、mixedの3種類のセキュリティ形式のいずれかを使用できます。セキュリティ形式に関係なくSMB経由でデータにアクセスできますが、UNIX対応のセキュリティを使用するデータにアクセスするには、適切なUNIXファイル権限が必要になります。

SMB経由でのデータへのアクセス時には、いくつかのアクセス制御を使用して、要求したアクションを実行する権限がユーザにあるかどうか判断されます。

- エクスポート権限  
SMBアクセスに関するエクスポート権限の設定は、Data ONTAP 8.2以降のリリースでは省略可能です。
- 共有権限
- ファイル権限  
ユーザがアクションを実行するデータに、次のタイプのファイル権限を適用できます。
  - NTFS
  - UNIX NFSv4 ACL
  - UNIXモード ビット

NFSv4 ACLまたはUNIXモード ビットが設定されたデータの場合は、UNIX形式の権限を使用してデータへのファイル権限が判断されます。SVM管理者は、適切なファイル権限を設定して、ユーザに目的のアクションを実行する権限が付与されるようにする必要があります。

注: mixedセキュリティ形式のボリューム内のデータでは、NTFSまたはUNIX対応のセキュリティ形式を使用できます。UNIX対応のセキュリティ形式を使用するデータの場合は、データに対するファイル権限を判断するときにNFSv4権限またはUNIXモード ビットが使用されます。

## DAC(ダイナミック アクセス制御)を使用したファイル アクセスの保護

ダイナミック アクセス制御を使用してアクセスを保護できます。Active Directoryで集約型アクセス ポリシーを作成し、適用されたGPOを使用してStorage Virtual Machine(SVM)上のファイルとフォルダにそのポリシーを適用します。集約型アクセス ポリシーのステージング イベントを使用するように監査を設定すると、集約型アクセス ポリシーの変更を適用する前にその効果を確認することができます。

### CIFSクレデンシャルの追加

ダイナミック アクセス制御が導入される前は、CIFSクレデンシャルにセキュリティ プリンシパル(ユーザ)のIDとWindowsグループ メンバーシップが含まれていました。ダイナミック アクセス制御では、デバイスID、デバイスの信頼性、ユーザの信頼性という3つのタイプの情報がクレデンシャルに追加されます。

- デバイスID  
ユーザID情報に似ていますが、デバイスIDはユーザがログインに使用しているデバイスのIDとグループ メンバーシップです。
- デバイスの信頼性  
デバイスのセキュリティ プリンシパルに関するアサーション(成立条件)です。たとえば、デバイスの信頼性として特定のOUのメンバーであることなどがあります。
- ユーザの信頼性  
ユーザのセキュリティ プリンシパルに関するアサーションです。たとえば、ユーザの信頼性としてADアカウントが特定のOUのメンバーであることなどがあります。

### セキュリティ記述子への追加

ダイナミック アクセス制御のサポートには、Microsoftがセキュリティ記述子として定義する3つの新しいACEタイプの追加が含まれます。

- 条件付きACE。管理者にリソースへのアクセスに関する高レベルの制御を提供する条件式です。  
条件付きACEは、DACLまたはSACLに含めることができます。
- リソースACE。ファイルまたはディレクトリに任意の属性を関連付けることができます。  
属性はADで定義され、ACEの名前/値ペアで表されます。たとえば、このメカニズムを使用して、マーケティング グループの所有であることを示すタグをファイルに付けることができます。  
このACEは、SACLでのみ使用できます。
- ポリシーACE。集約型アクセス ポリシーをリソースに結びつけます。  
ポリシーACEには、その後の追加アクセス チェックに使用可能なアクセス ポリシーを検索できるSIDが含まれています。このACEは、SACLでのみ使用できます。これによって、管理者は、Active Directoryの簡単な変更だけでリソースへのアクセスを変更できます。

### 集約型アクセス ポリシー

ファイルの集約型アクセス ポリシーを使用すると、ユーザ グループ、ユーザの信頼性、デバイスの信頼性、およびリソース プロパティを使用した条件式を含む許可ポリシーを、一元的に導入して管理することができます。



たとえば、ビジネスへの影響が大きいデータには、正社員のユーザだけが、管理対象のデバイスからのみアクセスできるようにすることができます。集約型アクセス ポリシーはActive Directoryに定義され、GPOメカニズムを介してファイル サーバに配布されます。

### 高度な監査機能を備えた集約型アクセス ポリシーのステージング

集約型アクセス ポリシーは「ステージング」することができます。その場合、ファイル アクセスのチェック時に「what-if」形式の評価が行われます。ポリシーが適用されていた場合の結果と、現在の設定との違いが、監査イベントのログに記録されます。管理者は実際にポリシーを有効にする前に、監査イベント ログを使用してアクセス ポリシーの変更による影響を確認できます。アクセス ポリシーの変更による影響を評価したあと、GPO経由でポリシーを目的のSVMに導入できます。

#### 関連コンセプト

[サポートされるGPO\(116ページ\)](#)  
[CIFSサーバへのグループ ポリシー オブジェクトの適用\(115ページ\)](#)  
[Flex Volを備えたSVMでのNASイベントの監査\(432ページ\)](#)

#### 関連タスク

[CIFSサーバ上でのGPOサポートの有効化と無効化\(120ページ\)](#)  
[GPO設定に関する情報の表示\(122ページ\)](#)  
[集約型アクセス ポリシーに関する情報の表示\(127ページ\)](#)  
[集約型アクセス ポリシー ルールに関する情報の表示\(128ページ\)](#)  
[CIFSサーバ上のデータを保護する集約型アクセス ポリシーの設定\(204ページ\)](#)  
[ダイナミック アクセス制御セキュリティに関する情報の表示\(206ページ\)](#)  
[セキュリティトレースの実行\(292ページ\)](#)  
[SVMでのファイルとディレクトリの監査設定の作成\(448ページ\)](#)

#### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver security file-directory show - Display file/folder security information](#)

## サポートされるダイナミック アクセス制御機能

CIFSサーバ上でDAC(ダイナミック アクセス制御)を使用する場合、Active Directory環境でのclustered Data ONTAPによるダイナミック アクセス制御機能のサポートについて理解しておく必要があります。

### サポートされるダイナミック アクセス制御

ダイナミック アクセス制御がCIFSサーバ上で有効である場合、clustered Data ONTAPは、次の機能をサポートします。

| 機能            | 説明                                                                                                                                                      |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイル システムへの請求 | 請求とは、ユーザについての何らかの真実を表す単純な名前と値のペアです。現在の請求情報にはユーザ クレデンシャルが含まれており、ファイルのセキュリティ記述子は請求チェックを含むアクセス チェックを実行できます。これによって、管理者は誰がファイルにアクセスできるかの細かいレベルの制御を行うことができます。 |

| 機能                                                              | 説明                                                                                                                                                                                                                     |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイル アクセス チェック用の条件式                                             | ファイルのセキュリティ パラメータを変更する場合、ユーザは任意の複雑な条件式をファイルのセキュリティ記述子に追加できます。条件式には、請求チェックを含めることができます。                                                                                                                                  |
| 集約型アクセス ポリシーによるファイル アクセスの集中管理                                   | 集約型アクセス ポリシーは、ファイルへのタグ付けが可能なActive Directory内に格納される一種のACLです。ファイルへのアクセスは、ディスク上のセキュリティ記述子とタグ付けされた集約型アクセス ポリシーの両方のアクセス チェックでアクセスが許可される場合のみ許可されます。<br>これによって、管理者はディスク上のセキュリティ記述子を変更せずに一元的な場所(AD)からファイルへのアクセスを制御できるようになります。 |
| 集約型アクセス ポリシーのステージング                                             | 集約型アクセス ポリシーの変更を「ステージング」して監査レポートで変更の効果を確認することにより、実際のファイル アクセスに影響を与えずにセキュリティの変更を試せるようになります。                                                                                                                             |
| clustered Data ONTAP CLIを使用した集約型アクセス ポリシー セキュリティについての情報の表示のサポート | vserver security file-directory showコマンドを拡張し、適用される集約型アクセス ポリシーについての情報を表示します。                                                                                                                                           |
| 集約型アクセス ポリシーを含むセキュリティトレース                                       | vserver security traceコマンド ファミリーを拡張し、適用される集約型アクセス ポリシーについての情報を含む結果を表示します。                                                                                                                                              |

### サポートされないダイナミック アクセス制御

ダイナミック アクセス制御がCIFSサーバ上で有効である場合、clustered Data ONTAPは、次の機能をサポートしません。

| 機能                          | 説明                                                                               |
|-----------------------------|----------------------------------------------------------------------------------|
| NTFSファイル システム オブジェクトの自動分類   | これは、clustered Data ONTAPでサポートされないWindows File Classification Infrastructure拡張です。 |
| 集約型アクセス ポリシーのステージング以外の高度な監査 | 高度な監査では、集約型アクセス ポリシーのステージングのみがサポートされます。                                          |

## CIFSサーバでダイナミック アクセス制御と集約型アクセス ポリシーを使用する際の考慮事項

CIFSサーバ上のファイルとフォルダを保護するためにDynamic Access Control (DAC;ダイナミック アクセス制御)と集約型アクセス ポリシーを使用する際は、一定の考慮事項に注意する必要があります。

### ポリシー ルールがdomain\administratorユーザに適用されている場合、rootに対してNFSアクセスが拒否されることがある

特定の状況では、rootユーザがアクセスしようとしているデータに集約型アクセス ポリシー セキュリティが適用されていると、rootに対してNFSアクセスが拒否されることがあります。この問題は、集約型アクセス ポリシーにdomain\administratorに適用されるルールが含まれており、rootアカウントがdomain\administratorアカウントにマッピングされている場合に発生します。

domain\administratorユーザにルールを適用する代わりに、domain\administratorsグループなど、管理者権限を持つグループにルールを適用してください。こうすることで、rootをdomain\administratorアカウントにマッピングしても、rootはこの問題の影響を受けなくなります。

**適用された集約型アクセス ポリシーがActive Directoryに見つからないと、CIFSサーバの BUILTIN\Administratorsグループにリソースへのアクセスが許可される**

CIFSサーバ内のリソースに集約型アクセス ポリシーが適用されている場合に、CIFSサーバが集約型アクセス ポリシーのSIDを使用してActive Directoryから情報を取得しようとしてもそのSIDがActive Directoryにある集約型アクセス ポリシーの既存のどのSIDとも一致しないことがあります。この場合、CIFSサーバはそのリソースにローカルのデフォルトのリカバリ ポリシーを適用します。

ローカルのデフォルトのリカバリ ポリシーでは、CIFSサーバのBUILTIN\Administratorsグループにそのリソースへのアクセスが許可されます。

**ダイナミック アクセス制御の有効化と無効化**

Dynamic Access Control (DAC;ダイナミック アクセス制御)を使用してCIFSサーバ上のオブジェクトを保護するオプションは、デフォルトでは無効になっています。CIFSサーバでダイナミック アクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFSサーバに格納されたオブジェクトの保護にダイナミック アクセス制御を使用する必要がなくなった場合は、このオプションを無効にすることができます。

**タスク概要**

ダイナミック アクセス制御を有効にすると、ダイナミック アクセス制御関連のエントリを使用するACLをファイル システムに含めることができます。ダイナミック アクセス制御を無効にすると、現在のダイナミック アクセス制御のエントリは無視され、新しいエントリは許可されません。

このオプションは、advanced権限レベルでのみ使用できます。

**手順**

- 1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- 2. 次のいずれかを実行します。

| ダイナミック アクセス制御の<br>設定 | 入力するコマンド                                                                   |
|----------------------|----------------------------------------------------------------------------|
| 有効                   | vserver cifs options modify -vserver vserver_name<br>-is-dac-enabled true  |
| 無効                   | vserver cifs options modify -vserver vserver_name<br>-is-dac-enabled false |

- 3. 管理者権限レベルに戻ります。

```
set -privilege admin
```

**関連タスク**

[CIFSサーバ上のデータを保護する集約型アクセス ポリシーの設定](#)(204ページ)

## ダイナミック アクセス制御が無効な場合のダイナミック アクセス制御ACEを含むACLの管理

ダイナミック アクセス制御ACEが適用されたACLが割り当てられたリソースがある場合にStorage Virtual Machine (SVM) でダイナミック アクセス制御を無効にすると、ダイナミック アクセス制御ACEを削除するまではそのリソースの非ダイナミック アクセス制御ACEを管理できません。

### タスク概要

ダイナミック アクセス制御を無効にした場合、既存のダイナミック アクセス制御ACEを削除するまでは、既存の非ダイナミック アクセス制御ACEの削除や新しい非ダイナミック アクセス制御ACEの追加はできません。

次の手順は、通常のACL管理に使用している任意のツールで実行することができます。

### 手順

1. リソースに適用されているダイナミック アクセス制御ACEを確認します。
2. リソースからダイナミック アクセス制御ACEを削除します。
3. リソースに対して非ダイナミック アクセス制御ACEの追加または削除を行います。

## CIFSサーバ上のデータを保護する集約型アクセス ポリシーの設定

CIFSサーバでのダイナミック アクセス制御 (DAC) の有効化、Active Directoryでの集約型アクセス ポリシーの設定、GPOが設定された集約型アクセス ポリシーのActive Directoryコンテナへの適用、CIFSサーバでのGPOの有効化などの集約型アクセス ポリシーを使用してCIFSサーバのデータへのアクセスを保護するには、いくつかの手順を実行する必要があります。

### 開始する前に

- 集約型アクセス ポリシーを使用するには、Active Directoryを設定する必要があります。
- 集約型アクセス ポリシーを作成し、CIFSサーバを含むコンテナにGPOの作成と適用を行うには、Active Directoryドメイン コントローラに対して十分なアクセスが必要です。
- 必要なコマンドを実行するためには、Storage Virtual Machine (SVM) で十分な管理アクセスが必要です。

### タスク概要

集約型アクセス ポリシーは、Active Directoryのグループ ポリシー オブジェクト (GPO) に対して定義および適用されます。集約型アクセス ポリシーおよびGPOの設定についてはMicrosoft TechNetライブラリを参照してください。

[Microsoft TechNetライブラリ](#)

### 手順

1. `vserver cifs options modify` コマンドを使用してSVMのダイナミック アクセス制御を有効化していない場合は、有効化します。

### 例

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. `vserver cifs group-policy modify` コマンドを使用してCIFSサーバのグループ ポリシー オブジェクト (GPO) を有効化していない場合は、有効化します。

**例**

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Active Directoryで集約型アクセス規則と集約型アクセス ポリシーを作成します。
4. グループ ポリシー オブジェクト(GPO)を作成してActive Directoryに集約型アクセス ポリシーを導入します。
5. CIFSサーバコンピュータ アカウントが存在するコンテナにGPOを適用します。
6. `vserver cifs group-policy update`コマンドを使用してCIFSサーバに適用されたGPOを手動で更新します。

**例**

```
vserver cifs group-policy update -vserver vs1
```

7. `vserver cifs group-policy show-applied`コマンドを使用して、GPO集約型アクセス ポリシーがCIFSサーバのリソースに適用されていることを確認します。

**例**

次の例は、デフォルトのドメイン ポリシーには、CIFSサーバに適用されている2つの集約型アクセス ポリシーがあることを示しています。

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----
  GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
  Advanced Audit Settings:
    Object Access:
      Central Access Policy Staging: failure
  Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
  Security Settings:
    Event Audit and Event Log:
      Audit Logon Events: none
      Audit Object Access: success
      Log Retention Method: overwrite-as-needed
      Max Log Size: 16384
    File Security:
      /vol1/home
      /vol1/dir1
    Kerberos:
      Max Clock Skew: 5
      Max Ticket Age: 10
      Max Renew Age: 7
    Privilege Rights:
      Take Ownership: usr1, usr2
      Security Privilege: usr1, usr2
      Change Notify: usr1, usr2
    Registry Values:
      Signing Required: false
    Restrict Anonymous:
      No enumeration of SAM accounts: true
      No enumeration of SAM accounts and shares: false
      Restrict anonymous access to shares and named pipes: true
      Combined restriction for anonymous user: no-access
    Restricted Groups:
      gpr1
      gpr2
```

```

Central Access Policy Settings:
  Policies: cap1
           cap2

  GPO Name: Resultant Set of Policy
  Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2
2 entries were displayed.

```

## 関連タスク

- [GPO設定に関する情報の表示](#)(122ページ)
- [集約型アクセス ポリシーに関する情報の表示](#)(127ページ)
- [集約型アクセス ポリシー ルールに関する情報の表示](#)(128ページ)
- [ダイナミック アクセス制御の有効化と無効化](#)(203ページ)

## ダイナミック アクセス制御セキュリティに関する情報の表示

NTFSボリューム、およびmixedセキュリティ形式のボリューム上のNTFS対応セキュリティを使用するデータについて、ダイナミック アクセス制御(DAC)セキュリティに関する情報を表示できます。これには、条件付きACE、リソースACE、および集約型アクセス ポリシーACEに関する情報が含まれます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine(SVM)の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

## 手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

| 表示する情報            | 入力するコマンド                                                                                               |
|-------------------|--------------------------------------------------------------------------------------------------------|
| 要約形式              | <code>vserver security file-directory show -vserver vserver_name -path path</code>                     |
| 詳細を表示             | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>   |
| グループSIDとユーザSIDを表示 | <code>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</code> |

## 例

次の例では、SVM vs1のパス/vol1に関するダイナミック アクセス制御セキュリティの情報を表示します。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
Vserver: vs1
File Path: /vol1
File Inode Number: 112
Security Style: mixed
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attribute: -
  Unix User Id: 0
  Unix Group Id: 1
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
      Control:0xbf14
      Owner:CIFS1\Administrator
      Group:CIFS1\Domain Admins
      SACL - ACES
        ALL-Everyone-0xf01ff-0I|CI|SA|FA
        RESOURCE ATTRIBUTE-Everyone-0x0
        ("Department_MS",TS,0x10020,"Finance")
        POLICY ID-All resources - No Write-0x0-0I|CI
      DACL - ACES
        ALLOW-CIFS1\Administrator-0x1f01ff-0I|CI
        ALLOW-Everyone-0x1f01ff-0I|CI
        ALLOW CALLBACK-DAC\user1-0x1200a9-0I|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@Device.departme
nt==@Resource.Department_MS)
```

## 関連タスク

- [GPO設定に関する情報の表示](#)(122ページ)
- [集約型アクセス ポリシーに関する情報の表示](#)(127ページ)
- [集約型アクセス ポリシー ルールに関する情報の表示](#)(128ページ)

## ダイナミック アクセス制御のリバートに関する考慮事項

DAC(ダイナミック アクセス制御)をサポートしないバージョンのData ONTAPにリバートする場合に発生する状況と、リバートの前後に必要な処理を把握しておく必要があります。

ダイナミック アクセス制御がサポートされていないバージョンのclustered Data ONTAPにクラスタをリバートし、1つまたは複数のStorage Virtual Machine(SVM)でダイナミック アクセス制御が有効になっている場合、リバート前に以下の処理を実行する必要があります。

- クラスタでダイナミック アクセス制御が有効になっているすべてのSVMで、ダイナミック アクセス制御を無効にする必要があります。
- `cap-staging`イベント タイプが含まれているクラスタで、`file-op`イベント タイプのみを使用するように監査設定を変更する必要があります。



ダイナミック アクセス制御ACEが設定されているファイルやフォルダについて、いくつかの重要なリバートに関する考慮事項について理解し、対応する必要があります。

- クラスタをリバートしても既存のダイナミック アクセス制御ACEは削除されませんが、ファイル アクセス チェックでは無視されます。
- リバート後はダイナミック アクセス制御ACEは無視されるため、ダイナミック アクセス制御ACEが設定されたファイルへのアクセスには変更が発生します。  
以前にファイルにアクセスできなかったユーザがアクセスできるようになったり、アクセスできたファイルにアクセスできなくなる可能性があります。
- 以前のセキュリティレベルに戻すには、影響を受けるファイルに非ダイナミック アクセス制御ACEを適用する必要があります。  
この処理は、リバート前またはリバート完了直後に実行します。

注: リバート後はダイナミック アクセス制御ACEは無視されるため、影響を受けるファイルに非ダイナミック アクセス制御ACEを適用する際にダイナミック アクセス制御ACEを削除する必要はありません。ただし、手動で削除することも可能です。

## ダイナミック アクセス制御と集約型アクセス ポリシーの設定方法および使用方法の参照先

ダイナミック アクセス制御と集約型アクセス ポリシーを設定および使用する際には、参考資料を利用することができます。

Active Directoryのダイナミック アクセス制御と集約型アクセス ポリシーの設定方法についての情報は、Microsoft TechNetライブラリにあります。

[Microsoft TechNet:「Dynamic Access Control Scenario Overview」](#)

[Microsoft TechNet:「Central Access Policy Scenario」](#)

CIFSサーバを設定してダイナミック アクセス制御と集約型アクセス ポリシーを使用またはサポートするには、次の参考資料を使用することができます。

### CIFSサーバでのGPOの使用

[CIFSサーバへのグループ ポリシー オブジェクトの適用](#)(115ページ)

### CIFSサーバでのNAS監査の設定

[FlexVolを備えたSVMでのNASイベントの監査](#)(432ページ)

## エクスポート ポリシーを使用したSMBアクセスの保護

必要に応じて、エクスポート ポリシーを使用することにより、Storage Virtual Machine(SVM)ボリューム上のファイルやフォルダへのSMBアクセスを制限することができます。エクスポート ポリシーを共有レベルおよびファイルレベルの権限と組み合わせて、有効な権限を決定できます。

エクスポート ポリシーの設定および管理の詳細については、『*clustered Data ONTAP ファイル アクセス管理ガイド(NFS)*』を参照してください。

### 関連コンセプト

[SMBアクセスでのエクスポート ポリシーの役割](#)(25ページ)

[SMB共有の作成と設定](#)(175ページ)

[SMB共有のACLを使用したファイル アクセスの保護](#)(190ページ)

[ファイル権限を使用したファイル アクセスの保護](#)(193ページ)



## SMBアクセスでのエクスポート ポリシーの使用方法

CIFSサーバでSMBアクセスに関するエクスポート ポリシーが有効になっている場合は、SMBクライアントによるStorage Virtual Machine(SVM)ボリュームまたはqtreeへのアクセスを制御するときにエクスポート ポリシーが使用されます。データにアクセスするには、SMBアクセスを許可するエクスポート ポリシーを作成し、SMB共有を含むボリュームまたはqtreeにそのポリシーを関連付けます。

エクスポート ポリシーには1つ以上のルールが適用されており、このルールで、データへのアクセスを許可されるクライアントや、読み取り専用アクセスと読み取り / 書き込みアクセスでサポートされる認証プロトコルを指定します。エクスポート ポリシーは、SMB経由のアクセスをすべてのクライアントに許可するか、特定のサブネットのクライアントに許可するか、特定のクライアントに許可するように設定できます。また、データへの読み取り専用アクセスと読み取り / 書き込みアクセスを決定するときに、Kerberos認証を許可するか、NTLM認証を許可するか、KerberosとNTLMの両方の認証を許可するように設定できます。

Data ONTAPでエクスポート ポリシーに適用されたすべてのエクスポート ルールを処理したら、クライアント アクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポート ルールは、Windowsのユーザおよびグループではなくクライアント マシンに適用されます。エクスポート ルールは、Windowsのユーザおよびグループベースの認証と許可に代わるものではありません。共有とファイルのアクセス権限に加えて、エクスポート ルールはもう1つのアクセス セキュリティレイヤを提供します。

ボリュームへのクライアント アクセスを設定するには、ボリュームごとに1つのエクスポート ポリシーを関連付けます。各SVMには複数のエクスポート ポリシーを含めることができます。これにより、複数のボリュームを備えたSVMに対して次の操作を実行できます。

- SVMのボリュームごとに異なるエクスポート ポリシーを割り当て、SVMの各ボリュームへのクライアント アクセスを個別に制御する。
- SVMの複数のボリュームに同じエクスポート ポリシーを割り当て、ボリュームごとに新しいエクスポート ポリシーを作成せずに、同一のクライアント アクセス制御を実行する。

ボリュームまたはqtreeへのクライアント アクセスを設定するには、各ボリュームまたはqtreeにエクスポート ポリシーを1つだけ関連付けます。各SVMには複数のエクスポート ポリシーを含めることができます。これにより、複数のボリュームまたはqtreeを備えたSVMに対して次の操作を実行できます。

- SVMのボリュームまたはqtreeごとに異なるエクスポート ポリシーを割り当て、SVMの各ボリュームまたはqtreeへのクライアント アクセスを個別に制御する。
- SVMの複数のボリュームまたはqtreeに同じエクスポート ポリシーを割り当て、ボリュームまたはqtreeごとに新しいエクスポート ポリシーを作成せずに、同一のクライアント アクセス制御を実行する。

各SVMには、「default」と呼ばれる少なくとも1つのエクスポート ポリシーがあります。これにはルールは含まれません。このエクスポート ポリシーは削除できませんが、名前や内容は変更できます。デフォルトでは、SVM上の各ボリュームはデフォルトのエクスポート ポリシーに関連付けられています。SVMでSMBアクセスのエクスポート ポリシーが無効になっている場合、「default」エクスポート ポリシーはSMBアクセスには影響しません。

NFSホストとSMBホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポート ポリシーに関連付けることができます。このポリシーを、NFSホストとSMBホストの両方がアクセスする必要があるデータを含むボリュームまたはqtreeに関連付けることができます。または、SMBクライアントのみがアクセスする必要があるボリュームまたはqtreeがある場合は、SMBプロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証にKerberosまたはNTLMのみ(あるいはその両方)を使用するルールを含むエクスポート ポリシーを設定できます。その後、このエクスポート ポリシーをSMBアクセスのみが必要なボリュームまたはqtreeに関連付けます。

SMBに関するエクスポート ポリシーが有効になっている場合に、クライアントが適用可能なエクスポート ポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントがボリュームのエクスポート ポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポート ポリシーが空の場合は、すべてのアクセスが暗黙的に拒否されます。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、SMB共有を含むボリュームまたはqtreeで少なくとも以下を許可するようにエクスポート ポリシーを設定する必要があります。

- すべてのクライアント、またはクライアントの適切なサブセットにアクセスを許可する
- SMB経由のアクセスを許可する
- Kerberos認証またはNTLM認証(あるいはその両方)を使用した適切な読み取り専用アクセスと書き込みアクセスを許可する

エクスポート ポリシーの設定および管理の詳細については、『*clustered Data ONTAP ファイル アクセス管理ガイド(NFS)*』を参照してください。

#### 関連コンセプト

[アップグレード時に既存のSMBエクスポート ポリシーが受ける影響](#)(210ページ)

[エクスポート ルールの仕組み](#)(212ページ)

#### 関連タスク

[SMBアクセスに関するエクスポート ポリシーの有効化と無効化](#)(210ページ)

#### 関連参照情報

[SMB経由のアクセスを制限または許可するエクスポート ポリシー ルールの例](#)(213ページ)

## アップグレード時に既存のSMBエクスポート ポリシーが受ける影響

Data ONTAP 8.2より前のリリースでは、SMBエクスポート ポリシーは必須です。Data ONTAP 8.2以降、SMBアクセスのエクスポート ポリシーは省略可能になり、デフォルトで無効になっています。エクスポート ポリシーが必須であるリリースからアップグレードするときは、それを実行した場合の動作について理解しておく必要があります。

SMBアクセスのエクスポート ポリシーの設定が必須であるバージョンからData ONTAPをアップグレードする場合、CIFSサーバを含むStorage Virtual Machine(SVM)がクラスタに含まれていれば、アップグレード後もそれらのSVMに対してエクスポート ポリシーのサポートが有効になります。アップグレード時に既存のCIFSサーバのSMBアクセスを再設定する必要はありません。

アップグレードしたクラスタでSVMとCIFSサーバを新規に作成する場合、新しいCIFSサーバのエクスポート ポリシーはデフォルトでは無効になります。新しいCIFSサーバについては、必要に応じてエクスポート ポリシーを有効にして設定することができます。

## SMBアクセスに関するエクスポート ポリシーの有効化と無効化

Storage Virtual Machine(SVM)でのSMBアクセスに関するエクスポート ポリシーを有効または無効にすることができます。エクスポート ポリシーを使用したリソースへのSMBアクセスの制御は、Data ONTAP 8.2以降では省略可能です。

#### 開始する前に

SMBに関するエクスポート ポリシーを有効にするための要件は次のとおりです。

- クライアントのエクスポート ルールを作成する前に、そのクライアントの「PTR」レコードがDNSに登録されている必要があります。

- SVMがNFSクライアントにアクセスを提供し、NFSアクセスに使用するホスト名がCFSサーバ名と異なる場合は、ホスト名に対して「A」レコードと「PTR」レコードのセットが追加が必要です。

タスク概要

Data ONTAP 8.2以降では、新しいオプションによって、SMBアクセスに関するエクスポート ポリシーを有効にするかどうかを制御されます。SVMに新しいCIFSサーバをセットアップするときに、SMBアクセスに関するエクスポート ポリシーの使用はデフォルトで無効になります。認証プロトコル、クライアントIPアドレス、またはホスト名に基づいてアクセスを制御する場合、SMBアクセスのエクスポート ポリシーを有効にできます。SMBアクセスに関するエクスポート ポリシーはいつでも有効または無効にできます。

8.2より前のバージョンのData ONTAPからアップグレードする場合、このオプションは、エクスポート ポリシーを使用してSMBアクセスを制御するクラスタ上のCIFSサーバで、自動的に有効になります。SMBアクセスのエクスポート ポリシーを省略可能なバージョンのData ONTAPにアップグレードする場合、設定済みのアクセス制御への想定外の変更は発生しません。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| エクスポート ポリシーの設定 | 入力するコマンド                                                                                      |
|----------------|-----------------------------------------------------------------------------------------------|
| 有効             | <code>vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true</code>  |
| 無効             | <code>vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false</code> |

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例では、エクスポート ポリシーを使用したSVM vs1上のリソースへのSMBクライアントアクセスの制御を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy-
enabled true

cluster1::*> set -privilege admin
```

関連コンセプト

[SMBアクセスでのエクスポート ポリシーの使用方法](#)(209ページ)

## エクスポート ルールの仕組み

エクスポート ルールは、エクスポート ポリシーの機能要素です。エクスポート ルールでは、ボリュームまたはqtreeへのクライアント アクセス要求が設定済みの特定のパラメータと照合され、クライアント アクセス要求の処理方法が決定されます。

エクスポート ポリシーには、クライアントにアクセスを許可するエクスポート ルールを少なくとも1つ 含める必要があります。エクスポート ポリシーに複数のルールが含まれている場合、ルールはエクスポート ポリシーに表示される順に処理されます。ルールの順序は、ルール インデックス番号によって決まります。ルールがクライアントに一致すると、そのルールのアクセス権が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用して、クライアントのアクセス権を決定するようにエクスポート ルールを設定できます。

- クライアントが要求の送信に使用するファイル アクセス プロトコル(NFSv4やSMBなど)
- クライアント識別子(ホスト名やIPアドレスなど)
- クライアントが認証に使用するセキュリティ タイプ(Kerberos v5、NTLM、AUTH\_SYSなど)

ルールで複数の条件が指定されており、クライアントがその1つ以上に一致しない場合、そのルールは適用されません。

### 例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv3プロトコルを使用して送信され、クライアントのIPアドレスは10.1.17.37です。

クライアント アクセス プロトコルは一致していますが、クライアントのIPアドレスがエクスポート ルールで指定されているアドレスとは異なるサブネット内にあります。したがって、クライアントは一致せず、このルールはこのクライアントに適用されません。

### 例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアント アクセス プロトコルが一致し、クライアントのIPアドレスが指定されたサブネット内にあります。したがって、クライアントは一致し、このルールはこのクライアントに適用されます。セキュリティ タイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

#### 例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- -protocol **nfs3**
- -clientmatch **10.1.16.0/255.255.255.0**
- -rorule **any**
- -rwrule **krb5,ntlm**

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH\_SYSで認証されます。

どちらのクライアントも、クライアント アクセス プロトコルとIPアドレスは一致しています。読み取り専用パラメータは、認証に使用されたセキュリティ タイプに関係なく、すべてのクライアントに読み取り専用アクセスを許可するように設定されています。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り / 書き込みアクセス権を取得するのは、承認されているセキュリティ タイプKerberos v5を認証に使用したクライアント#1だけです。クライアント#2は読み取り / 書き込みアクセス権を取得できません。

#### 関連参照情報

[SMB経由のアクセスを制限または許可するエクスポート ポリシー ルールの例](#)(213ページ)

### SMB経由のアクセスを制限または許可するエクスポート ポリシー ルールの例

以下の例は、SMBアクセスのエクスポート ポリシーが有効になっているStorage Virtual Machine (SVM)でSMB経由のアクセスを制限または許可するエクスポート ポリシー ルールを作成する方法を示しています。

SMBアクセスのエクスポート ポリシーは、デフォルトでは無効になっています。SMB経由のアクセスを制限または許可するエクスポート ポリシー ルールは、SMBアクセスのエクスポート ポリシーを有効にしている場合にのみ設定する必要があります。

#### SMBアクセスのみのエクスポート ルール

次のコマンドを実行すると、「vs1」という名前のSVMで、次のような設定のエクスポート ルールが作成されます。

- ポリシー名 : cifs1
- インデックス番号 : 1
- クライアント一致 : 192.168.1.0/24ネットワーク上のクライアントにのみ一致
- プロトコル : SMBアクセスのみを有効化
- 読み取り専用アクセス : NTLM認証またはKerberos認証を使用するクライアントに許可
- 読み取り / 書き込みアクセス : Kerberos認証を使用するクライアントに許可

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname cifs1
-ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0 -rorule
krb5,ntlm -rwrule krb5
```

### SMBおよびNFSアクセスのエクスポート ルール

次のコマンドを実行すると、「vs1」という名前のSVMで、次のような設定のエクスポート ルールが作成されます。

- ポリシー名: cifs nfs1
- インデックス番号: 2
- クライアント一致: すべてのクライアントに一致
- プロトコル: SMBアクセスとNFSアクセス
- 読み取り専用アクセス: すべてのクライアントに許可
- 読み取り / 書き込みアクセス: Kerberos認証 (NFSおよびSMB) またはNTLM認証 (SMB) を使用するクライアントに許可
- UNIXユーザID 0 (ゼロ) のマッピング: ユーザID 65534 (通常ユーザ名nobodyにマップされる) にマッピング
- suidとsgidのアクセス: 許可

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname cifs nfs1
-ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule
krb5,ntlm -anon 65534 -allow-suid true
```

### NTLMのみを使用するSMBアクセスのエクスポート ルール

次のコマンドを実行すると、「vs1」という名前のSVMで、次のような設定のエクスポート ルールが作成されます。

- ポリシー名: ntlm1
- インデックス番号: 1
- クライアント一致: すべてのクライアントに一致
- プロトコル: SMBアクセスのみを有効化
- 読み取り専用アクセス: NTLMを使用するクライアントにのみ許可
- 読み取り / 書き込みアクセス: NTLMを使用するクライアントにのみ許可

**注:** NTLMのみを使用するアクセスに読み取り専用オプションまたは読み取り / 書き込みオプションを設定する場合は、クライアント一致オプションでIPアドレスベースのエントリを使用する必要があります。そうしないと、access deniedエラーが表示されます。これは、Data ONTAPがホスト名を使用してクライアントの権限を確認するときに、Kerberos Service Principal Name (SPN; サービス プリンシパル名) を使用するためです。NTLM認証では、SPN名はサポートされません。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname ntlm1
-ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm -rwrule ntlm
```

エクスポート ポリシーの設定および管理の詳細については、『*clustered Data ONTAP ファイル アクセス管理ガイド(NFS)*』を参照してください。

## 関連コンセプト

[エクスポート ルールの仕組み](#) (212ページ)

## SMBのエクスポート ポリシーをリバートする際の考慮事項

Data ONTAP 8.2より前のリリースでは、SMBエクスポート ポリシーは必須です。Data ONTAP 8.2以降、SMBアクセスのエクスポート ポリシーは省略可能になり、デフォルトで無効になっています。エクスポート ポリシーが必須であるリリースにリバートする場合には一定の考慮事項があります。

次の2つのシナリオでは、SMBアクセスのエクスポート ポリシーが必須であるData ONTAPのバージョンにリバートする場合にSMBのエクスポート ポリシーについて注意する必要があります。

- SMBのエクスポート ポリシーの使用が任意であるData ONTAPのバージョンがインストールされているクラスタがあり、そのすべてのStorage Virtual Machine (SVM) 上でエクスポート ポリシーが無効になっている。

この場合、SVMと含まれるボリュームには、SMBアクセスを許可するエクスポート ポリシーがありません。エクスポート ポリシーが必須であるData ONTAPのバージョンにリバートすると、エクスポート ポリシーが有効になり、SMBアクセスに必要となります。そのため、SMBクライアントへのアクセスが拒否されます。

推奨される方法は、SMBクライアント アクセスに関する解決しにくい問題がリバート後に発生しないように、リバートする前に、すべてのSVM上でSMBのエクスポート ポリシーを設定することです。
- SMBアクセスのエクスポート ポリシーの使用が任意であるData ONTAPのバージョンがインストールされているクラスタがあり、その一部(すべてではなく)のSVM上でSMBのエクスポート ポリシーが有効になっている。

エクスポート ポリシーが必須であるData ONTAPのバージョンにリバートすると、エクスポート ポリシーが有効になり、すべてのSVMでSMBアクセスに必要となります。そのため、エクスポート ポリシーがリバート前に有効になっていなかったSVMで、SMBクライアントへのアクセスが拒否されます。

推奨される方法は、SMBクライアント アクセスに関する解決しにくい問題がリバート後に発生しないように、リバートする前に、すべてのSVM上でSMBのエクスポート ポリシーを設定することです。

**注:** エクスポート ポリシーが必須であるData ONTAPのバージョンからアップグレードすると、既存SVM上でSMBのエクスポート ポリシーが自動的に有効になります。あとから、その既存のSVM上でSMBのエクスポート ポリシーを無効にした場合でも、エクスポート ポリシーはそのまま残っています。この場合に、エクスポート ポリシーが必須であるData ONTAPのバージョンにリバートすると、その既存のエクスポート ポリシーを使用して、SMBアクセスが決定されます。ただし、リバートする前に、最初のアップグレード後に作成したすべての新しいSVM上でSMBアクセスのエクスポート ポリシーを作成する必要があります。

## SMBを使用したファイル アクセスの管理

Storage Virtual Machine (SVM) に CIFS サーバを作成して構成し、SMB 共有経由のファイル アクセスを設定したら、さまざまなファイル アクセスを管理するタスクを実行できます。

### ローカル ユーザおよびローカル グループを使用した認証と許可

Storage Virtual Machine (SVM) では、ローカル ユーザやローカル グループを作成することができます。CIFS サーバでの CIFS 認証にローカル ユーザを使用すると、共有やファイルおよびディレクトリに対する許可をローカル ユーザとローカル グループに基づいて決定できます。

ローカル グループには、ローカル ユーザ、ドメイン ユーザ、ドメイン グループ、およびドメイン マシン アカウントを含めることができます。

ローカル ユーザとローカル グループには権限を割り当てることもできます。SVM リソースへのアクセスを制御するこれらの権限は、オブジェクトに対して設定されているアクセス許可よりも優先されます。権限が割り当てられたユーザまたはグループのメンバーには、その権限で許可される特定の権利が付与されます。

**注:** clustered Data ONTAP の全般的な管理機能は権限では付与されません。

#### 関連コンセプト

[ローカル権限とは](#) (220 ページ)

[ローカル ユーザとローカル グループ機能の有効化と無効化](#) (224 ページ)

[ローカル ユーザ アカウントの管理](#) (226 ページ)

[ローカル グループの管理](#) (232 ページ)

[ローカル権限の管理](#) (239 ページ)

### Data ONTAP でのローカル ユーザとローカル グループの使用方法

ローカル ユーザとローカル グループを設定して使用する場合は、その概要と使用方法について理解しておく必要があります。たとえば、ローカル ユーザとローカル グループを使用すると、Storage Virtual Machine (SVM) に存在するデータに対して共有とファイル アクセスのセキュリティを確保できます。また、ローカル ユーザとローカル グループを使用して、ユーザにユーザ管理権限を割り当てることもできます。

#### ローカル ユーザとローカル グループの概念

ローカル ユーザとローカル グループを設定して使用するかどうかを決定する前に、ローカル ユーザとローカル グループの定義を理解し、基本的ないくつかの情報を理解しておく必要があります。

##### ローカル ユーザ

一意の Security Identifier (SID; セキュリティ識別子) を持つユーザ アカウント。そのユーザ アカウントを作成した Storage Virtual Machine (SVM) 上でのみ認識されます。ローカル ユーザ アカウントには、ユーザ名や SID などの一連の属性があります。このアカウントは、NTLM 認証を使用して CIFS サーバ上でローカルに認証されます。

ユーザ アカウントには、次に示すいくつかの用途があります。

- ユーザ権限の管理が可能な権限をユーザに付与する。
- SVM が保有するファイル リソースおよびフォルダ リソースに対する共有レベルとファイルレベルのアクセスを制御する。

##### ローカル グループ



一意のSIDを持つグループ。そのグループを作成したSVM上でのみ認識されます。グループは複数のメンバーで構成されます。このメンバーになれるのは、ローカル ユーザ、ドメイン ユーザ、ドメイン グループ、ドメイン マシンの各アカウントです。グループは、作成、変更、削除することができます。

グループには、次に示すいくつかの用途があります。

- ユーザ権限の管理が可能な権限をグループのメンバーに付与する。
- SVMが保有するファイル リソースおよびフォルダ リソースに対する共有レベルとファイルレベルのアクセスを制御する。

## ローカルドメイン

ローカル スコープを持つドメイン。SVMによりバインドされています。ローカルドメインの名前はCIFSサーバの名前になります。ローカル ユーザとローカル グループはローカルドメイン内に配置されます。

## Security Identifier (SID;セキュリティ識別子)

Windows形式のセキュリティプリンシパルを識別する可変長の数値。たとえば、通常のSIDの場合は、次のような形式になります。

S-1-5-21-3139654847-1303905135-2517279418-123456。

## NTLM認証

CIFSサーバ上のユーザの認証で使用する、Microsoft Windowsのセキュリティ方式。

## 複製されたクラスタ データベース(RDB)

クラスタ内の各ノードのインスタンスを持つ複製されたデータベース。ローカル ユーザとローカル グループの各オブジェクトは、このRDBに格納されます。

## ローカル ユーザおよびグループを作成する理由

Storage Virtual Machine (SVM) でローカル ユーザやローカル グループを作成する理由はいくつかあります。たとえば、ドメイン コントローラを使用できないときでも、ローカル ユーザ アカウントを使用すればCIFSサーバにアクセスできます。また、ローカル グループを使用して権限を割り当てることもできます。

ローカル ユーザ アカウントを作成する理由には、次のようなものがあります。

- ドメイン コントローラを使用できないときに、CIFSサーバで認証してログインできるようにする。ドメイン コントローラがダウンしている場合や、ネットワークの問題によってCIFSサーバからドメイン コントローラに接続できない場合でも、ローカル ユーザであれば、NTLM認証を使用してCIFSサーバに認証できます。
- ローカル ユーザにユーザ権限の管理権限を割り当てる。  
ユーザ権限の管理は、ユーザやグループに付与するSVMの権限をCIFSサーバ管理者が制御できる機能です。ユーザに権限を割り当てるには、ユーザのアカウントにそれらの権限を割り当てるか、ユーザをそれらの権限が割り当てられたローカル グループのメンバーにします。

**注:** ローカル ユーザはローカルで認証できますが、CIFSサーバはワークグループモードでは動作しません。ワークグループモードはこのバージョンのData ONTAPではサポートされておらず、CIFSサーバはActive Directoryドメインに属している必要があります。CIFSサーバは、Active Directoryドメインのメンバー サーバとして動作します。

ローカル グループを作成する理由には、次のようなものがあります。

- 共有やファイル アクセスの制御にローカル グループを使用して、ファイルやフォルダのリソースへのアクセスを制御する。
- カスタマイズしたユーザ権限の管理権限を持つローカル グループを作成する。  
権限があらかじめ定義された組み込みのユーザ グループがいくつか用意されています。カスタマイズした一連の権限を割り当てるには、ローカル グループを作成し、そのグループに必要な

権限を割り当てます。そのあとで、作成したローカル グループに、ローカル ユーザ、ドメイン ユーザ、およびドメイン グループを追加します。

#### 関連コンセプト

[ローカル ユーザ認証の仕組み](#) (218ページ)

[ローカル権限とは](#) (220ページ)

#### ローカル ユーザ認証の仕組み

CIFSサーバのデータにアクセスする前に、ローカル ユーザは認証されたセッションを作成する必要があります。

SMBはセッションベースであるため、ユーザのIDは、最初にセッションがセットアップされるときに一度だけ確認できます。CIFSサーバでは、ローカル ユーザの認証時にNTLMベースの認証が使用されます。NTLMv1とNTLMv2の両方がサポートされています。

Data ONTAPでは、3つの事例でローカル認証が使用されます。各事例は、ユーザ名のドメイン部分(DOMAIN\user形式)がCIFSサーバのローカルドメイン名(CIFSサーバ名)と一致するかどうかによります。

- ドメイン部分が一致する  
データへのアクセスを要求するときにローカル ユーザ クレデンシャルを指定したユーザが、CIFSサーバでローカルに認証されます。
- ドメイン部分が一致しない  
Data ONTAPは、CIFSサーバが属しているドメインのドメイン コントローラでNTLM認証を試行します。認証に成功した場合は、ログインが完了します。失敗した場合は、認証の失敗理由によって次の動作が異なります。  
たとえば、ユーザはActive Directory内に存在するが、パスワードが無効であるか期限切れになっている場合は、CIFSサーバ上の対応するローカル ユーザ アカウントの使用は試行されません。代わりに、認証は失敗します。NetBIOSドメイン名が一致しなくてもCIFSサーバ上の対応するローカル アカウント(存在する場合)が認証に使用されるケースはほかにもあります。たとえば、一致するドメイン アカウントが存在するが無効になっている場合は、CIFSサーバ上の対応するローカル アカウントが認証に使用されます。
- ドメイン部分が指定されていない  
まず、ローカル ユーザとしての認証が試行されます。ローカル ユーザとしての認証に失敗した場合は、CIFSサーバが属しているドメインのドメイン コントローラでユーザが認証されます。

ローカル ユーザまたはドメイン ユーザの認証が完了したら、ローカル グループ メンバーシップおよび権限が考慮される完全なユーザ アクセストークンが構築されます。

ローカル ユーザのNTLM認証の詳細については、Microsoft Windowsのマニュアルを参照してください。

#### 関連タスク

[ローカル ユーザ認証の有効化と無効化](#) (225ページ)

#### ユーザ アクセストークンの構成方法

ユーザが共有をマッピングすると、認証されたSMBセッションが確立され、ユーザ アクセストークンが構成されます。このユーザ トークンには、ユーザ、ユーザのグループ メンバーシップ、累積権限、マッピングされたUNIXユーザのそれぞれについて、情報が格納されています。

この機能が無効にされていない限り、ローカル ユーザとローカル グループのそれぞれについても、ユーザ アクセストークンに情報が追加されます。アクセストークンの構成方法は、ローカル ユーザのログインとActive Directoryドメイン ユーザのログインでは、方法が異なります。

- ローカル ユーザ ログイン

ローカル ユーザは複数のローカル グループのメンバーになることができますが、ローカル グループは他のローカル グループのメンバーになることができません。ローカル ユーザ アクセス トークンは、その特定のローカル ユーザが属するグループに割り当てられたすべての権限の組み合わせから構成されます。

- ドメイン ユーザ ログイン

ドメイン ユーザのログインでは、Data ONTAPは、ユーザのSIDと、そのユーザが属するすべてのドメイン グループのSIDが格納されたユーザ アクセス トークンを取得します。また、ユーザ ドメイン グループ のローカル メンバーシップ (存在する場合) が提供するアクセス トークンとドメイン ユーザ アクセス トークンとの組み合わせを、Data ONTAPは使用します。また、ドメイン ユーザに割り当てられた直接権限や、ドメイン グループ メンバーシップの直接権限も使用します。

ローカル ユーザのログインとドメイン ユーザのログインの両方で、ユーザ アクセス トークンには、Primary Group Relative Identifier (RID; 相対識別子) も設定されます。デフォルトのRIDはドメイン ユーザ (RID 513) です。Data ONTAPのこのバージョンでは、デフォルトのRIDを変更することはできません。

WindowsからUNIXへの名前のマッピングと、UNIXからWindowsへの名前のマッピングではローカル アカウントとドメイン アカウントのどちらも同じルールに従います。

注: UNIXユーザがローカル アカウントに自動的にマッピングされることはありません。UNIXユーザをローカル アカウントにマッピングする必要がある場合は、既存のネーム マッピング コマンドを使用して、明示的なマッピング ルールを指定する必要があります。

## ローカル グループを含むSVM上でSnapMirrorを使用する際の考慮事項

ローカル グループを含むStorage Virtual Machine (SVM) によって所有されているボリュームでSnapMirrorを設定する場合は、一定の考慮事項に注意する必要があります。

SnapMirrorによって別のSVMにレプリケートされるファイル、ディレクトリ、または共有に適用するACEではローカル グループを使用できません。SnapMirror機能を使用して別のSVM上のボリュームに対するDRミラーを作成する場合に、そのボリュームにローカル グループのACEがあるときは、ミラーにはACEは適用されません。データが別のSVMにレプリケートされる場合、実質的に、そのデータは別のローカルドメインに格納されることになります。ローカル ユーザとローカル グループに付与される権限は、そのオブジェクトが最初に作成されたSVMの範囲内でのみ有効です。

## CIFSサーバを削除したときにローカル ユーザとローカル グループが受ける影響

CIFSサーバを作成すると、デフォルトの一連のローカル ユーザとローカル グループが作成され、CIFSサーバをホストするStorage Virtual Machine (SVM) に関連付けられます。また、SVM管理者は、ローカル ユーザやローカル グループをいつでも作成することができます。CIFSサーバを削除するときは、それを実行した場合のローカル ユーザやローカル グループに対する影響について理解しておく必要があります。

ローカル ユーザとローカル グループはSVMに関連付けられます。そのため、セキュリティの観点から、CIFSサーバを削除してもそれらが削除されることはありません。ただし、CIFSサーバを削除すると、ローカル ユーザとローカル グループは削除される代わりに非表示になります。SVMでCIFSサーバを再作成するまで、表示したり管理したりすることはできません。

注: CIFSサーバの 管理ステータスは、ローカル ユーザやローカル グループが表示されるかどうかには影響しません。

## Microsoft管理コンソールでのローカル ユーザとローカル グループの情報の表示

Microsoft管理コンソールを使用して、ローカル ユーザとローカル グループのそれぞれの情報を表示できます。Data ONTAPの今回のリリースでは、Microsoft管理コンソールで、ローカル ユーザとローカル グループに対する上記以外の管理タスクを実行することはできません。

## リバート時の考慮事項

ローカル ユーザとグループを使用してファイル アクセスまたはユーザ権限を管理している場合に、ローカル ユーザとグループをサポートしないData ONTAPリリースにクラスタをリバートするときは、一定の考慮事項に注意する必要があります。

- セキュリティ上の理由から、ローカル ユーザとグループの機能をサポートしないバージョンにData ONTAPをリバートしても、設定されているローカル ユーザ、グループ、および権限に関する情報は削除されません。
- Data ONTAPの以前のメジャー バージョンにリバートする際、認証とクレデンシャルの作成時にローカル ユーザとグループは使用されません。
- ローカル ユーザとローカル グループは、ファイルおよびフォルダのACLからは削除されません。
- ファイル アクセス要求が、ローカル ユーザまたはローカル グループに付与された権限に基づいて許可されるアクセスに依存する場合、その要求は拒否されます。  
アクセスを許可するには、ローカル ユーザとローカル グループ オブジェクトではなく、ドメイン オブジェクトに基づいてアクセスを許可するようにファイル権限を再設定する必要があります。

## ローカル権限とは

権限とは、CIFSサーバでユーザ権限の管理作業を実行するためにローカルおよびドメインのユーザやグループに割り当てることができるアクセス権です。権限を独自に作成することはできず、既存の権限の追加または削除だけが可能です。

## サポートされる権限の一覧

Data ONTAPには、一連のサポートされる権限が事前に定義されています。特定の事前定義されたローカル グループには、これらの権限の一部がデフォルトで設定されています。事前定義グループの権限は追加、削除できます。また、新規のローカル ユーザまたはローカル グループを作成して、そのグループや、既存のドメイン ユーザおよびグループに権限を追加することもできます。

次の表に、Storage Virtual Machine (SVM) でサポートされる権限の一覧と、その権限が割り当てられているBUILTINグループを示します。

| 権限の名前                    | デフォルトのセキュリティ設定                                      | 説明                              |
|--------------------------|-----------------------------------------------------|---------------------------------|
| SeTcbPrivilege           | なし                                                  | オペレーティング システムの一部として機能           |
| SeBackupPrivilege        | BUILTIN\Administrators,<br>BUILTIN\Backup Operators | ACLを無視してファイルとディレクトリをバックアップ      |
| SeRestorePrivilege       | BUILTIN\Administrators,<br>BUILTIN\Backup Operators | ACLを無視してファイルおよびディレクトリをリストア      |
| SeTakeOwnershipPrivilege | BUILTIN\Administrators                              | ファイルなどの、オブジェクトの所有権を取得           |
| SeSecurityPrivilege      | BUILTIN\Administrators                              | 監査の管理<br>セキュリティ ログの表示、ダンプ、消去など。 |

| 権限の名前                   | デフォルトのセキュリティ設定                                                                                             | 説明                                                                                                         |
|-------------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| SeChangeNotifyPrivilege | BUILTIN\Administrators,<br>BUILTIN\Backup<br>Operators, BUILTIN\Power<br>Users, BUILTIN\Users,<br>Everyone | トラバース チェックのバ<br>イパス<br>この権限を持つユーザ<br>は、フォルダ、シンボリック<br>クリンク、ジャンクション<br>を経由するためのトラバ<br>ース(x) 権限は必要あり<br>ません。 |

#### 関連コンセプト

[ローカル権限の管理](#)(239ページ)

[トラバース チェックのバイパスの設定](#)(242ページ)

#### 権限の割り当て方法

ローカル ユーザまたはドメイン ユーザに権限を直接割り当てることができます。また、ユーザに付与する権限と一致する権限が割り当てられているローカル グループにユーザを割り当てることができます。

- 作成したグループに権限セットを割り当てることができます。  
その後、ユーザに付与する権限が割り当てられているグループにユーザを追加します。
- ローカル ユーザおよびドメイン ユーザを、デフォルトの権限がユーザに付与する権限と一致している事前定義グループに割り当てることができます。

#### 関連コンセプト

[トラバース チェックのバイパスの設定](#)(242ページ)

#### 関連タスク

[ローカルまたはドメインのユーザまたはグループに対する権限の追加](#)(239ページ)

[ローカルまたはドメインのユーザまたはグループの権限の削除](#)(240ページ)

[ローカルまたはドメインのユーザまたはグループの権限の再設定](#)(241ページ)

#### 要件および考慮事項

CIFSサーバでローカル ユーザやローカル グループを作成して設定する前に、一定の要件と考慮事項について確認しておく必要があります。

#### BUILTINグループとローカル管理者アカウントを使用する際の考慮事項

BUILTINグループとローカル管理者アカウントを使用する場合は、一定の考慮事項に注意する必要があります。たとえば、ローカル管理者アカウントは、名前の変更は可能ですが、削除はできないことを理解しておく必要があります。

- Administratorアカウントは、名前の変更は可能ですが、削除はできません。
- AdministratorアカウントはBUILTIN\Administratorsグループから削除できません。
- BUILTINグループは、名前の変更は可能ですが、削除はできません。  
BUILTINグループの名前を変更したあと、よく知られた名前を使用して別のローカル オブジェクトを作成できますが、そのオブジェクトには新しいRIDが割り当てられます。
- ローカルGuestアカウントは存在しません。

**関連参照情報**

[事前定義のBUILTINグループとそのデフォルトの権限](#) (222ページ)

**ローカル ユーザのパスワードの要件**

デフォルトでは、ローカル ユーザのパスワードは複雑さの要件を満たしている必要があります。パスワードの複雑さの要件は、Microsoft Windowsのローカル セキュリティ ポリシーで定義される要件に似ています。

パスワードは次の基準を満たしている必要があります。

- 6文字以上である必要があります。
- ユーザ アカウント名を含めることはできません。
- 次の4種類のうちの3種類以上の文字を含める必要があります。
  - 大文字のアルファベット(A～Z)
  - 小文字のアルファベット(a～z)
  - 数字(0～9)
  - 特殊文字:

~!@#0^&\* \_ - + = ` \ | ( ) [ ] ; : ' " < > , . ? /

**関連タスク**

[ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化](#) (82ページ)

[CIFSサーバのセキュリティ設定に関する情報の表示](#) (81ページ)

[ローカル ユーザのアカウント パスワードの変更](#) (229ページ)

**事前定義のBUILTINグループとそのデフォルトの権限**

ローカル ユーザまたはドメイン ユーザのメンバーシップを、Data ONTAPの事前定義された一連のBUILTINグループに割り当てることができます。BUILTINグループには、事前定義された権限が割り当てられています。

次の表に、事前定義グループを示します。

| 事前定義のBUILTINグループ                                                                                                                                                                                                                                        | デフォルトの権限                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BUILTIN\Administrators</b><br>RID 544<br>RIDが500のローカルAdministratorアカウントは、最初に作成された時点で自動的にこのグループのメンバーになります。Storage Virtual Machine (SVM) がドメインに参加すると、domain\Domain Adminsグループがこのグループに追加されます。SVMがドメインから削除されると、domain\Domain Adminsグループも、このグループから削除されます。 | <ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeSecurityPrivilege</li> <li>• SeTakeOwnershipPrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul> |

| 事前定義のBUILTINグループ                                                                                                                                                                                                                                         | デフォルトの権限                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BUILTIN\Power Users</b><br>RID 547<br>このグループには、最初に作成された時点ではメンバーがありません。このグループのメンバーには次のような特徴があります。 <ul style="list-style-type: none"> <li>ローカル ユーザとローカル グループを作成、管理できます。</li> <li>自身や他のオブジェクトを<b>BUILTIN\Administrators</b>グループに追加することはできません。</li> </ul> | <b>SeChangeNotifyPrivilege</b>                                                                                                                        |
| <b>BUILTIN\Backup Operators</b><br>RID 551<br>このグループには、最初に作成された時点ではメンバーがありません。このグループのメンバーは、バックアップ目的で開いたファイルやフォルダの読み取りおよび書き込み権限を上書きできます。                                                                                                                  | <ul style="list-style-type: none"> <li><b>SeBackupPrivilege</b></li> <li><b>SeRestorePrivilege</b></li> <li><b>SeChangeNotifyPrivilege</b></li> </ul> |
| <b>BUILTIN\Users</b><br>RID 545<br>このグループには、最初に作成された時点では（暗黙の <b>Authenticated Users</b> 特殊グループ以外には）メンバーがありません。SVMがドメインに参加すると、 <b>domain\Domain Users</b> グループがこのグループに追加されます。SVMがドメインから削除されると、 <b>domain\Domain Users</b> グループも、このグループから削除されます。           | <b>SeChangeNotifyPrivilege</b>                                                                                                                        |
| <b>Everyone</b><br>SID S-1-1-0<br>このグループには、ゲストを含むすべてのユーザが含まれます（ただし匿名ユーザは除く）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。                                                                                                                                              | <b>SeChangeNotifyPrivilege</b>                                                                                                                        |

#### 関連コンセプト

[BUILTINグループとローカル管理者アカウントを使用する際の考慮事項](#)(221ページ)  
[トラバース チェックのバイパスの設定](#)(242ページ)

#### 関連参照情報

[サポートされる権限の一覧](#)(220ページ)

## ローカル ユーザとローカル グループ機能の有効化と無効化

NTFSセキュリティ形式データのアクセス制御にローカル ユーザとローカル グループを使用する前に、ローカル ユーザとローカル グループ機能を有効にする必要があります。また、SMB認証にローカル ユーザを使用する場合は、ローカル ユーザ認証機能を有効にする必要があります。

ローカル ユーザとローカル グループ機能とローカル ユーザ認証はデフォルトで有効になっています。有効になっていない場合は、ローカル ユーザとローカル グループを設定して使用する前に有効にする必要があります。ローカル ユーザとローカル グループ機能はいつでも無効にできます。

ローカル ユーザとローカル グループ機能の明示的な無効化に加えて、Data ONTAPでは、クラスタ内のノードがローカル ユーザとローカル グループ機能をサポートしていないリリースのData ONTAPにリポートされた場合にその機能が無効になります。クラスタ内のすべてのノードでその機能をサポートするバージョンのData ONTAPが実行されるまで、ローカル ユーザとローカル グループ機能は有効になりません。

### 関連コンセプト

[ローカル ユーザ アカウントの管理](#)(226ページ)

[ローカル グループの管理](#)(232ページ)

[ローカル権限の管理](#)(239ページ)

## ローカル ユーザとローカル グループの有効化と無効化

Storage Virtual Machine(SVM)で、SMBアクセスに使用するローカル ユーザとローカル グループを有効または無効にすることができます。ローカル ユーザとローカル グループ機能はデフォルトで有効になっています。

### タスク概要

SMB共有およびNTFSファイル権限の設定時にローカル ユーザとローカル グループを使用でき、必要に応じて、SMB接続の作成時の認証のためにローカル ユーザを使用できます。認証のためにローカル ユーザを使用するには、ローカル ユーザとローカル グループ認証オプションも有効にする必要があります。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| ローカル ユーザとローカル<br>グループの設定 | 入力するコマンド                                                                                                    |
|--------------------------|-------------------------------------------------------------------------------------------------------------|
| 有効                       | <code>vserver cifs options modify -vserver vserver_name<br/>-is-local-users-and-groups-enabled true</code>  |
| 無効                       | <code>vserver cifs options modify -vserver vserver_name<br/>-is-local-users-and-groups-enabled false</code> |

3. admin権限レベルに戻ります。

```
set -privilege admin
```

### 例

次の例では、SVM vs1でローカル ユーザとローカル グループ機能を有効にします。



```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options modify -vsserver vs1 -is-local-users-and-
groups-enabled true

cluster1::*> set -privilege admin
```

関連タスク

- [ローカル ユーザ認証の有効化と無効化](#) (225ページ)
- [ローカル ユーザ アカウントの有効化と無効化](#) (229ページ)

ローカル ユーザ認証の有効化と無効化

Storage Virtual Machine (SVM) での SMB アクセスに関するローカル ユーザ認証を有効または無効にすることができます。デフォルトでは、ローカル ユーザ認証は許可されます。これは、SVM がドメイン コントローラにアクセスできない場合、またはドメインレベルのアクセス制御を使用しない場合に役立ちます。

開始する前に

CIFS サーバでローカル ユーザとローカル グループ機能を有効にしておく必要があります。

タスク概要

ローカル ユーザ認証はいつでも有効または無効にできます。SMB 接続の作成時の認証のためにローカル ユーザを使用する場合は、CIFS サーバのローカル ユーザとローカル グループ オプションも有効にする必要があります。

手順

- 権限レベルをadvancedに設定します。  
`set -privilege advanced`
- 次のいずれかを実行します。

| ローカル認証の設定 | 入力するコマンド                                                                                       |
|-----------|------------------------------------------------------------------------------------------------|
| 有効        | <code>vsserver cifs options modify -vsserver vsserver_name -is-local-auth-enabled true</code>  |
| 無効        | <code>vsserver cifs options modify -vsserver vsserver_name -is-local-auth-enabled false</code> |

- admin権限レベルに戻ります。  
`set -privilege admin`

例

次の例では、SVM vs1でローカル ユーザ認証を有効にします。

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
```

```
cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth-enabled
true

cluster1::*> set -privilege admin
```

#### 関連コンセプト

[ローカル ユーザ認証の仕組み](#) (218ページ)

#### 関連タスク

[ローカル ユーザとローカル グループの有効化と無効化](#) (224ページ)

## ローカル ユーザ アカウントの管理

ローカル ユーザ アカウントの管理では、ローカル ユーザ アカウントを作成、変更、削除したり、ユーザ アカウントやユーザ グループ メンバーシップの情報を表示したりできます。また、このほかにも、アカウントの有効化、無効化、名前の変更や、アカウントのパスワードの設定、パスワードの複雑性の管理などの管理タスクを実行することもできます。

#### 関連コンセプト

[ローカル グループの管理](#) (232ページ)

[ローカル権限の管理](#) (239ページ)

## ローカル ユーザ アカウントの作成

Storage Virtual Machine (SVM) に格納されたデータへのSMB接続を介したアクセスの許可に使用できるローカル ユーザ アカウントを作成できます。ローカル ユーザ アカウントは、SMBセッションを作成する際の認証に使用することもできます。

#### 開始する前に

ローカル ユーザとグループの機能を有効にする必要があります。

#### タスク概要

ローカル ユーザ アカウントを作成するときは、ユーザ名を指定する必要があり、アカウントを関連付けるSVMを指定する必要があります。ユーザ名は次の要件を満たす必要があります。

- 20文字以内にする必要があります。
- 最後の文字をピリオドにすることはできません。
- カンマは使用できません。
- 次の印刷可能文字は使用できません。  
", / \ , [ , ] , : , | , < , > , + , = , ; , ? , \* , @ 。
- 印字されないASCII文字 (1～31の範囲) は使用できません。

必要に応じて、次のパラメータを指定できます。

- `-full-name user_name`には、ユーザのフルネームを指定します。  
フルネームの中でスペースを使用する場合は、引用符で囲む必要があります。
- `-description text`には、ローカル ユーザの説明を指定します。  
説明の中でスペースを使用する場合は、引用符で囲む必要があります。

- `-is account-disabled {true|false}`は、ユーザ アカウントを有効にするか、無効にするかを指定します。  
デフォルトでは、ユーザ アカウントは有効です

### 手順

1. 次のコマンドを入力して、ローカル ユーザを作成します。

```
vserver cifs users-and-groups local-user create -vserver vserver_name  
user-name user_name optional_parameters
```

ローカル ユーザのパスワードを入力するよう求めるプロンプトが表示されます。

2. ローカル ユーザのパスワードを入力し、確認のためにもう一度入力します。

パスワードは次の要件を満たす必要があります。

- 6文字以上である必要があります。
- ユーザ アカウント名を含めることはできません。
- 次の4種類のうちの3種類以上の文字を含める必要があります。
  - 大文字のアルファベット(A～Z)
  - 小文字のアルファベット(a～z)
  - 数字(0～9)
  - 特殊文字:~、!、@、#、0、^、&、\*、\_、-、+、=、`、\、|、(、)、[、]、:、;、"、'、<、>、,、.、?、/

3. ユーザが正常に作成されたことを確認します。

```
vserver cifs users-and-groups local-user show -vserver vserver_name
```

### 例

次の例では、SVM vs1に関連付けられるローカル ユーザ「CIFS\_SERVER\sue」を作成します。

```
cluster1::> vserver cifs users-and-groups local-user create -vserver vs1 -user-name  
CIFS_SERVER\sue  
  
Enter the password:  
Confirm the password:  
  
cluster1::> vserver cifs users-and-groups local-user show  
Vserver  User Name          Full Name  Description  
-----  
vs1      CIFS_SERVER\Administrator  Built-in administrator account  
vs1      CIFS_SERVER\sue
```

### ローカル ユーザ アカウントの変更

既存のユーザのフルネームや説明を変更したり、ユーザ アカウントを有効または無効にしたりする場合は、ローカル ユーザ アカウントを変更します。また、ユーザ名が侵害を受けたり、管理上の

目的で名前の変更が必要になったりした場合も、ローカル ユーザ アカウントの名前を変更します。

| 状況                       | 入力するコマンド                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ローカル ユーザのフルネームの変更        | <pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -full-name text</pre> <p>変更するフルネームにスペースが含まれている場合には、そのフルネームを2重引用符で囲む必要があります。</p>                                                                                                                                                                                                                                                                                                 |
| ローカル ユーザの説明の変更           | <pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -description text</pre> <p>変更する説明にスペースが含まれている場合には、その説明を2重引用符で囲む必要があります。</p>                                                                                                                                                                                                                                                                                                     |
| ローカル ユーザ アカウントの有効化または無効化 | <pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is- account-disabled {true false}</pre>                                                                                                                                                                                                                                                                                                                                        |
| ローカル ユーザ アカウントの名前の変更     | <pre>vserver cifs users-and-groups local-user rename -vserver vserver_name -user-name user_name - new-user-name new_user_name</pre> <p>新規のユーザ名は次の条件に従う必要があります。</p> <ul style="list-style-type: none"> <li>20文字以内にする必要があります。</li> <li>最後の文字をピリオドにすることはできません。</li> <li>カンマは使用できません。</li> <li>次の印刷可能文字は使用できません。<br/>"、/、\、[、]、:、\、&lt;、&gt;、+、=、;、?、*、@。</li> <li>印字されないASCII文字(1～31の範囲)は使用できません。</li> </ul> <p>ローカル ユーザの名前を変更する場合は、古いユーザ名と同様に、新規のユーザ名を同じCIFSサーバに関連付ける必要があります。</p> |

#### 例

次の例では、Storage Virtual Machine(SVM、旧Vserver)vs1上のローカル ユーザの名前を「CIFS\_SERVER\sue」から「CIFS\_SERVER\sue\_new」に変更しています。

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

ローカル ユーザ アカウントの有効化と無効化

Storage Virtual Machine (SVM) に格納されたデータにユーザがSMB接続経由でアクセスできるようにするには、ローカル ユーザ アカウントを有効にします。また、SVMのデータにそのユーザがSMB経由でアクセスできないようにするには、ローカル ユーザ アカウントを無効にします。

タスク概要

ユーザ アカウントを変更してローカル ユーザを有効にします。

手順

- 1. 適切な処理を実行します。

| 状況              | 入力するコマンド                                                                                                                           |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------|
| ユーザ アカウントを有効にする | <code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled false</code> |
| ユーザ アカウントを無効にする | <code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled true</code>  |

ローカル ユーザのアカウント パスワードの変更

ローカル ユーザのアカウント パスワードを変更できます。これは、ユーザのパスワードが侵害された場合、またはユーザがパスワードを忘れた場合に役立ちます。

手順

- 1. 適切な操作を実行してパスワードを変更します。

```
vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name
```

パスワードは次の基準を満たしている必要があります。

- 6文字以上である必要があります。
- ユーザ アカウント名を含めることはできません。
- 次の4種類のうちの3種類以上の文字を含める必要があります。
  - 大文字のアルファベット (A～Z)
  - 小文字のアルファベット (a～z)
  - 数字 (0～9)
  - 特殊文字:

```
~!@#0^&* _ - + = ` \ | ( ) [ ] ; : " ' < > , . ? /
```

例

次の例では、Storage Virtual Machine (SVM、旧Vserver) vs1に関連付けられたローカル ユーザ「CIFS\_SERVER\sue」のパスワードを設定します。

```
cluster1::> vsriver cifs users-and-groups local-user set-password -user-name
CIFS_SERVER\sue -vsriver vs1

Enter the new password:
Confirm the new password:
```

## 関連タスク

[ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化](#) (82ページ)

[CIFSサーバのセキュリティ設定に関する情報の表示](#) (81ページ)

## ローカル ユーザに関する情報の表示

すべてのローカル ユーザの一覧を要約形式で表示できます。特定のユーザに対するアカウント設定を確認する必要がある場合は、そのユーザの詳細なアカウント情報、および複数のユーザのアカウント情報を表示できます。この情報は、ユーザの設定を変更する必要があるかどうかを判断する場合に加えて、認証やファイル アクセスに関する問題のトラブルシューティングを行う場合にも役立ちます。

## タスク概要

ユーザのパスワードに関する情報は表示されません。

## 手順

1. 次のいずれかを実行します。

| 状況                                                | 入力するコマンド                                                                                                  |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Storage Virtual Machine (SVM) のすべてのユーザに関する情報を表示する | <b>vsriver cifs users-and-groups local-user show -vsriver vsriver_name</b>                                |
| 特定のユーザの詳細なアカウント情報を表示する                            | <b>vsriver cifs users-and-groups local-user show -instance -vsriver vsriver_name -user-name user_name</b> |

ほかにも、このコマンドを実行するときに選択できるオプションのパラメータがあります。詳細については、マニュアル ページを参照してください。

## 例

次の例では、SVM vs1のすべてのローカル ユーザに関する情報を表示します。

```
cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver  User Name      Full Name      Description
-----
vs1      CIFS_SERVER\Administrator  James Smith    Built-in administrator account
vs1      CIFS_SERVER\sue           Sue Jones
```

## ローカル ユーザのグループ メンバーシップに関する情報の表示

ローカル ユーザが属しているローカル グループに関する情報を表示できます。この情報を使用して、ユーザに付与する必要があるファイルやフォルダへのアクセスを確認できます。この情報は、ユーザに付与する必要があるファイルやフォルダへのアクセス権や、ファイル アクセスに関する問題のトラブルシューティングを行うタイミングを判断するのに役立ちます。

## タスク概要

コマンドをカスタマイズして、必要な情報のみを表示することができます。

手順

1. 次のいずれかを実行します。

| 状況                                                                         | 入力するコマンド                                                                                              |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 指定したローカル ユーザのローカル ユーザ メンバーシップに関する情報を表示する                                   | <code>vserver cifs users-and-groups local-user show-membership -user-name user_name</code>            |
| このローカル ユーザが属しているローカル グループのローカル ユーザ メンバーシップに関する情報を表示する                      | <code>vserver cifs users-and-groups local-user show-membership -membership group_name</code>          |
| 指定したStorage Virtual Machine (SVM)に関連付けられているローカル ユーザのユーザ メンバーシップに関する情報を表示する | <code>vserver cifs users-and-groups local-user show-membership -vserver vserver_name</code>           |
| 指定したSVM上のすべてのローカル ユーザに関する詳細情報を表示する                                         | <code>vserver cifs users-and-groups local-user show-membership -instance -vserver vserver_name</code> |

例

次の例では、SVM vs1上のすべてのローカル ユーザのメンバーシップ情報を表示します。ユーザ「CIFS\_SERVER\Administrator」は「BUILTIN\Administrators」グループのメンバーで、「CIFS\_SERVER\sue」は「CIFS\_SERVER\g1」グループのメンバーです。

```
cluster1::> vserver cifs users-and-groups local-user show-membership -
vserver vs1
Vserver      User Name                               Membership
-----
vs1          CIFS_SERVER\Administrator               BUILTIN\Administrators
              CIFS_SERVER\sue                  CIFS_SERVER\g1
```

ローカル ユーザ アカウントの削除

CIFSサーバに対するローカルSMB認証や、Storage Virtual Machine (SVM)に格納されたデータへの権限の確認に必要ななくなった場合は、SVMからローカル ユーザ アカウントを削除できます。

タスク概要

ローカル ユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。  
そのユーザを参照するファイルおよびディレクトリのWindowsセキュリティ記述子は調整されません。
- ローカル ユーザへのすべての参照はメンバーシップおよび権限のデータベースから削除されます。
- 一般に使用される標準のユーザ (Administratorなど) は削除できません。

手順

1. 削除するローカル ユーザ アカウントの名前を確認します。

```
vserver cifs users-and-groups local-user show -vserver vserver_name
```

2. ローカル ユーザを削除します。

```
vserver cifs users-and-groups local-user delete -vserver vserver_name
-user-name username_name
```

3. ユーザ アカウントが削除されたことを確認します。

```
vserver cifs users-and-groups local-user show -vserver vserver_name
```

#### 例

次の例では、SVM vs1に関連付けられたローカル ユーザ「CIFS\_SERVER\sue」を削除します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name          Full Name          Description
-----
vs1      CIFS_SERVER\Administrator  James Smith      Built-in administrator account
vs1      CIFS_SERVER\sue          Sue Jones
```

```
cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1 -user-name
CIFS_SERVER\sue
```

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name          Full Name          Description
-----
vs1      CIFS_SERVER\Administrator  James Smith      Built-in administrator account
```

## ローカル グループの管理

ローカル グループの管理では、グループを作成、変更したり、グループやグループ メンバーシップの情報を表示したりできます。また、不要なグループを削除することもできます。また、このほかにも、グループの名前の変更や、ローカル ユーザとドメイン ユーザの両方について、ローカル グループへの追加、ローカル グループからの削除を行うなど、管理タスクを実行することもできます。

### 関連コンセプト

[ローカル ユーザ アカウントの管理](#)(226ページ)

[ローカル権限の管理](#)(239ページ)

## ローカル グループの作成

Storage Virtual Machine (SVM)に関連付けられたデータへのSMB接続を介したアクセスの許可に使用できるローカル グループを作成できます。また、グループのメンバーに付与するアクセス権を定義する権限を割り当てすることもできます。

### 開始する前に

ローカル ユーザとグループの機能を有効にする必要があります。

### タスク概要

ローカル グループを作成する場合は、次の点に注意してください。

- グループ名を指定する際、ローカルドメイン名は指定してもしなくても構いません。ローカルドメインは、SVM上のCIFSサーバ名です。たとえば、CIFSサーバ名が「CIFS\_SERVER」で、「engineering」グループを作成する場合は、グループ名を「engineering」または「CIFS\_SERVER\engineering」と指定できます。ローカルドメインをグループ名の一部として使用するときのルールを次に示します。
  - 指定できるのは、グループを適用するSVMのローカルドメイン名だけです。たとえば、ローカルCIFSサーバ名が「CIFS\_SERVER」の場合、「CORP\_SERVER\group1」などのローカル グループ名は指定できません。



- *BUILTIN*という語をグループ名のローカルドメインとして使用することはできません。  
たとえば、「*BUILTIN\group1*」というグループは作成できません。
- すでに存在するグループ名は指定できません。

ローカル グループを作成するときは、グループの名前を指定する必要があり、グループを関連付けるSVMを指定する必要があります。必要に応じて、ローカル グループの説明を指定することもできます。グループ名は次の要件を満たす必要があります。

- 256文字以内にする必要があります。
- 最後の文字をピリオドにすることはできません。
- カンマは使用できません。
- 次の印刷可能文字は使用できません。  
"、/、\、[、]、:、\、|、<、>、+、=、;、?、\*、@。
- 印字されないASCII文字(1～31の範囲)は使用できません。

手順

1. 次のコマンドを入力して、ローカル グループを作成します。  
**vserver cifs users-and-groups local-group create -vserver *vserver\_name* -group-name *group\_name***
2. グループが正常に作成されたことを確認します。  
**vserver cifs users-and-groups local-group show -vserver *vserver\_name***

**例**  
次の例では、SVM vs1に関連付けられるローカル グループ「*CIFS\_SERVER\engineering*」を作成します。

```
cluster1::> vserver cifs users-and-groups local-group create -vserver vs1 -group-name CIFS_SERVER\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name      Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users    Restricted administrative privileges
vs1          BUILTIN\Users          All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales
```

ローカル グループの変更

既存のローカル グループの変更では、そのグループの説明と名前を変更できます。

| 状況              | 使用するコマンド                                                                                                                                                                                    |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ローカル グループの説明の変更 | <b>vserver cifs users-and-groups local-group modify -vserver <i>vserver_name</i> -group-name <i>group_name</i> -description <i>text</i></b><br>変更する説明にスペースが含まれている場合には、その説明を2重引用符で囲む必要があります。 |

| 状況              | 使用するコマンド                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ローカル グループの名前の変更 | <pre><b>vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name</b></pre> <p>新規のグループ名は次の条件に従う必要があります。</p> <ul style="list-style-type: none"> <li>256文字以内にする必要があります。</li> <li>最後の文字をピリオドにすることはできません。</li> <li>カンマは使用できません。</li> <li>次の印刷可能文字は使用できません。<br/>", / \ , [ , ] , : ,   , &lt; , &gt; , + , = , ; , ? , * , @ .</li> <li>印字されないASCII文字(1～31の範囲)は使用できません。</li> </ul> |

**例**

次の例では、ローカル グループの名前を「CIFS\_SERVER\engineering」から「CIFS\_SERVER\engineering\_new」に変更します。

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1 -
group-name CIFS_SERVER\engineering -new-group-name CIFS_SERVER
\engineering_new
```

次の例では、ローカル グループの説明「CIFS\_SERVER\engineering」を変更します。

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1 -
group-name CIFS_SERVER\engineering -description "New Description"
```

**ローカル グループに関する情報の表示**

クラスタまたは指定したStorage Virtual Machine(SVM)で設定されているすべてのローカル グループの一覧を表示できます。この情報は、SVMに格納されているデータに対するファイル アクセスに関する問題や、SVMのユーザ権限に関する問題のトラブルシューティングに役立ちます。

**手順**

1. 次のいずれかを実行します。

| 必要な情報              | 入力するコマンド                                                                    |
|--------------------|-----------------------------------------------------------------------------|
| クラスタのすべてのローカル グループ | <b>vserver cifs users-and-groups local-group show</b>                       |
| SVMのすべてのローカル グループ  | <b>vserver cifs users-and-groups local-group show -vserver vserver_name</b> |

ほかにも、このコマンドを実行するときに選択できるオプションのパラメータがあります。詳細については、マニュアル ページを参照してください。

**例**

次の例では、SVM vs1のすべてのローカル グループに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                Description
-----
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

## ローカル グループ メンバーシップの管理

ローカル グループ メンバーシップの管理では、ローカル ユーザやドメイン ユーザの追加と削除、ドメイン グループの追加と削除ができます。この機能は、特定のグループに配置されたデータへのアクセスをアクセス制御ベースで制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

特定のグループで、メンバーシップに基づいてドメイン ユーザやドメイン グループに付与された権限や権限を取り消す場合に、メンバーをグループから削除して処理できます。

メンバーをローカル グループに追加する場合は、次の点に留意する必要があります。

- 特殊なグループである *Everyone* にユーザを追加することはできません。
- ローカル グループにユーザを追加する前に、あらかじめそのグループが存在している必要があります。
- ローカル グループにユーザを追加する前に、あらかじめそのユーザが存在している必要があります。
- 別のローカル グループにローカル グループを追加することはできません。
- ローカル グループにドメイン ユーザまたはグループを追加するには、Data ONTAP でSIDを名前解決できる必要があります。

メンバーをローカル グループから削除する場合は、次の点に留意する必要があります。

- 特別な *Everyone* グループからメンバーを削除することはできません。
- メンバーを削除するグループが存在している必要があります。
- グループから削除するメンバーの名前を、対応するSIDに対して、Data ONTAPで解決できる必要があります。

| 状況             | 使用するコマンド                                                                                                                                                                                                               |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| グループへのメンバーの追加  | <pre>vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[, ...]</pre> <p>カンマ区切りのリストに記載されたローカル ユーザ、ドメイン ユーザ、ドメイン グループを指定し、特定のローカル グループに追加します。</p>     |
| グループからのメンバーの削除 | <pre>vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[, ...]</pre> <p>カンマ区切りのリストに記載されたローカル ユーザ、ドメイン ユーザ、ドメイン グループを指定し、特定のローカル グループから削除します。</p> |

**例**

次の例では、ローカル ユーザ「CIFS\_SERVER\sue」およびドメイン グループ「AD\_DOMAIN\dom\_eng」をStorage Virtual Machine(SVM、旧Vserver)vs1のローカル グループ「CIFS\_SERVER\engineering」に追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1 -group-name CIFS_SERVER\engineering -member-names CIFS_SERVER
\sue,AD_DOMAIN\dom_eng
```

次の例では、ローカル ユーザ「CIFS\_SERVER\sue」および「CIFS\_SERVER\james」を、SVM vs1のローカル グループ「CIFS\_SERVER\engineering」から削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members -
vserver vs1 -group-name CIFS_SERVER\engineering -member-names CIFS_SERVER
\sue,CIFS_SERVER\james
```

**関連タスク**

[ローカル グループのメンバーに関する情報の表示](#)(236ページ)

**ローカル グループのメンバーに関する情報の表示**

クラスタまたは指定したStorage Virtual Machine(SVM)で設定されているローカル グループのすべてのメンバーの一覧を表示できます。この情報は、ファイル アクセスに関する問題やユーザ権限に関する問題のトラブルシューティングに役立ちます。

**手順**

1. 次のいずれかを実行します。

| 表示する情報                  | 入力するコマンド                                                                                   |
|-------------------------|--------------------------------------------------------------------------------------------|
| クラスタのすべてのローカル グループのメンバー | <b>vserver cifs users-and-groups local-group show-members</b>                              |
| SVMのすべてのローカル グループのメンバー  | <b>vserver cifs users-and-groups local-group show-members -vserver <i>vserver_name</i></b> |

**例**

次の例では、SVM vs1のすべてのローカル グループのメンバーに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show-members -vserver
vs1
```

| Vserver | Group Name              | Members                                                                    |
|---------|-------------------------|----------------------------------------------------------------------------|
| vs1     | BUILTIN\Administrators  | CIFS_SERVER\Administrator<br>AD_DOMAIN\Domain Admins<br>AD_DOMAIN\dom_grp1 |
|         | BUILTIN\Users           | AD_DOMAIN\Domain Users<br>AD_DOMAIN\dom_usr1                               |
|         | CIFS_SERVER\engineering | CIFS_SERVER\james                                                          |

## ローカル グループの削除

Storage Virtual Machine (SVM) に関連付けられたデータへの権限を決定するのに必要なくなった場合や、SVM ユーザ権限をグループ メンバーに割り当てるのに必要なくなった場合は、SVM からローカル グループを削除できます。

### タスク概要

ローカル グループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。  
このグループを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。
- そのグループが存在しない場合、エラーが返されます。
- 特殊なグループである *Everyone* は削除できません。
- *BUILTIN\Administrators* や *BUILTIN\Users* などの組み込みのグループは削除できません。

### 手順

1. SVM 上のローカル グループの一覧を表示して、削除するローカル グループの名前を確認します。

```
vserver cifs users-and-groups local-group show -vserver vserver_name
```

2. ローカル グループを削除します。

```
vserver cifs users-and-groups local-group delete -vserver vserver_name
-group-name group_name
```

3. グループが削除されたことを確認します。

```
vserver cifs users-and-groups local-user show -vserver vserver_name
```

### 例

次の例では、SVM vs1 に関連付けられたローカル グループ「CIFS\_SERVER\sales」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name      Description
-----
vs1       BUILTIN\Administrators Built-in Administrators group
vs1       BUILTIN\Backup Operators Backup Operators group
vs1       BUILTIN\Power Users   Restricted administrative privileges
vs1       BUILTIN\Users         All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1 -group-name
CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name      Description
-----
vs1       BUILTIN\Administrators Built-in Administrators group
vs1       BUILTIN\Backup Operators Backup Operators group
vs1       BUILTIN\Power Users   Restricted administrative privileges
vs1       BUILTIN\Users         All users
vs1       CIFS_SERVER\engineering
```

## ローカル データベースのドメイン ユーザ名およびグループ名の更新

CIFSサーバのローカル グループにドメイン ユーザやドメイン グループを追加できます。これらのドメイン オブジェクトは、クラスタのローカル データベースに登録されます。ドメイン オブジェクトの名前を変更した場合は、ローカル データベースを手動で更新する必要があります。

### タスク概要

ドメイン名を更新するStorage Virtual Machine(SVM)の名前を指定する必要があります。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 適切な処理を実行します。

| ドメイン ユーザおよびドメイン グループの更新後の処理                       | 使用するコマンド                                                                                                    |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| ドメイン ユーザとドメイン グループについて、正常に更新されたものと更新できなかったものを表示する | <pre>vs1&gt; vserver cifs users-and-groups update-names - vserver vs1_name</pre>                            |
| ドメイン ユーザとドメイン グループについて、正常に更新されたものを表示する            | <pre>vs1&gt; vserver cifs users-and-groups update-names - vserver vs1_name -display-failed-only false</pre> |
| ドメイン ユーザとドメイン グループについて、更新できなかったものを表示する            | <pre>vs1&gt; vserver cifs users-and-groups update-names - vserver vs1_name -display-failed-only true</pre>  |
| 更新に関するすべてのステータス情報を非表示にする                          | <pre>vs1&gt; vserver cifs users-and-groups update-names - vserver vs1_name -suppress-all-output true</pre>  |

3. admin権限レベルに戻ります。

```
set -privilege admin
```

### 例

次の例では、Storage Virtual Machine(SVM、旧Vserver)vs1に関連付けられたドメイン ユーザおよびグループの名前を更新しています。前回の更新に基づいて、一連の名前を更新する必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::> vserver cifs users-and-groups update-names -vserver vs1

Vserver:      vs1
SID:          S-1-5-21-123456789-234565432-987654321-12345
Domain:       EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:  dom_user2
Status:       Successfully updated

Vserver:      vs1
SID:          S-1-5-21-123456789-234565432-987654322-23456
Domain:       EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:  dom_user2
Status:       Successfully updated
```

```

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID
"S-1-5-21-123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

## ローカル権限の管理

ローカル権限の管理では、ローカル ユーザ アカウント、ドメイン ユーザ アカウント、グループについて、権限の追加、削除、再設定ができます。また、ローカル ユーザ アカウント、ドメイン ユーザ アカウント、グループに割り当てられた権限について、情報を表示することもできます。

### 関連コンセプト

[権限の割り当て方法](#)(221ページ)

[ローカル ユーザ アカウントの管理](#)(226ページ)

[ローカル グループの管理](#)(232ページ)

### 関連参照情報

[サポートされる権限の一覧](#)(220ページ)

## ローカルまたはドメインのユーザまたはグループに対する権限の追加

ローカルまたはドメインのユーザまたはグループのユーザ権限を管理できます。追加した権限は、対象のオブジェクトに割り当てられていたデフォルトの権限よりも優先されます。これにより、ユーザまたはグループに付与する権限をカスタマイズして、セキュリティを強化できます。

### 開始する前に

権限を追加する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

### タスク概要

オブジェクトに権限を追加すると、そのユーザまたはグループのデフォルトの権限は無効になります。権限を追加しても、以前に追加した権限は削除されません。

ローカルまたはドメインのユーザまたはグループに権限を追加する場合は、次の点に注意する必要があります。

- 権限は1つでも複数でも追加できます。
- ドメイン ユーザまたはグループへの権限の追加時、Data ONTAPでは、ドメイン コントローラに接続してそのドメイン ユーザまたはグループを検証することがあります。  
Data ONTAPからドメイン コントローラに接続できない場合、コマンドが失敗することがあります。

**手順**

1. ローカルまたはドメインのユーザまたはグループに1つ以上の権限を追加します。

```
vserver cifs users-and-groups privilege add-privilege -vserver  
vserver_name -user-or-group-name name -privileges privilege[,...]
```

-user-or-group-nameパラメータの値には、ローカル ユーザまたはグループか、ドメイン ユーザまたはグループを指定します。

-privileges privilege[,...]には、1つ以上の権限をカンマで区切って指定します。

2. 目的の権限がオブジェクトに適用されていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-  
or-group-name name
```

**例**

次の例では、権限「SeTcbPrivilege」および「SeTakeOwnershipPrivilege」をStorage Virtual Machine (SVM、旧Vserver) vs1のユーザ「CIFS\_SERVER\sue」に追加します。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver  
vs1 -user-or-group-name CIFS_SERVER\sue -privileges  
SeTcbPrivilege,SeTakeOwnershipPrivilege  
  
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1  
Vserver    User or Group Name    Privileges  
-----  
vs1        CIFS_SERVER\sue    SeTcbPrivilege  
                                SeTakeOwnershipPrivilege
```

**ローカルまたはドメインのユーザまたはグループの権限の削除**

ローカルまたはドメインのユーザやグループのユーザ権限の管理作業として、権限を削除することができます。これにより、ユーザやグループに割り当てる権限の上限をカスタマイズして、セキュリティを強化することができます。

**開始する前に**

権限を削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

**タスク概要**

ローカルまたはドメインのユーザやグループの権限を削除するときは、次の点に注意してください。

- 1つまたは複数の権限を削除できます。
- ドメインのユーザまたはグループの権限を削除する場合、Data ONTAPでそれらのユーザやグループを検証するために、ドメイン コントローラに接続することがあります。  
Data ONTAPからドメイン コントローラに接続できない場合、コマンドが失敗することがあります。

**手順**

1. ローカルまたはドメインのユーザまたはグループの権限を削除します。

```
vserver cifs users-and-groups privilege remove-privilege -vserver  
vserver_name -user-or-group-name name -privileges privilege[,...]
```

-user-or-group-nameパラメータには、ローカルまたはドメインのユーザまたはグループの名前を指定します。



-privileges *privilege*[,...]には、1つ以上の権限をカンマで区切って指定します。

2. 指定したユーザまたはグループで指定した権限が削除されていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
```

#### 例

次の例は、「SeTcbPrivilege」権限および「SeTakeOwnershipPrivilege」権限をStorage Virtual Machine (SVM、旧Vserver) vs1上のユーザ「CIFS\_SERVER\sueo」から削除します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      SeTcbPrivilege
                        SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege -
vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      -
```

### ローカルまたはドメインのユーザまたはグループの権限の再設定

ローカルまたはドメインのユーザやグループの権限をリセットできます。これは、ローカルまたはドメインのユーザやグループの権限に対して行った変更が不要になり、元に戻す場合に役立ちます。

#### タスク概要

ローカルまたはドメインのユーザやグループの権限をリセットすると、そのユーザまたはグループの権限のエントリがすべて削除されます。

#### 手順

1. ローカルまたはドメインのユーザまたはグループの権限をリセットします。

```
vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name
```

-user-or-group-name/パラメータには、ローカルまたはドメインのユーザまたはグループの名前を指定します。

2. 指定したユーザまたはグループの権限がリセットされていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
```

#### 例

次の例は、Storage Virtual Machine (SVM、旧Vserver) vs1のユーザ「CIFS\_SERVER\sue」の権限をリセットしています。デフォルトでは、標準のユーザのアカウントにはどの権限も関連付けられません。

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      SeTcbPrivilege
                        SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege -vserver
```

```
vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

次に、グループ「BUILTIN\Administrators」の権限をリセットする例を示します。これにより、実質的に権限のエントリが削除されます。

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name    Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                                     SeSecurityPrivilege
                                     SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege -vserver
vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

### 権限の上書きに関する情報の表示

ドメインまたはローカルのユーザ アカウントまたはグループに割り当てられているカスタムの権限に関する情報を表示できます。この情報は、適切なユーザ権限が適用されているかどうかを確認するのに役立ちます。

#### 手順

1. 次のいずれかを実行します。

| 表示する情報                                                          | コマンド                                                                                                             |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Storage Virtual Machine (SVM) 上のすべてのドメインおよびローカルのユーザとグループのカスタム権限 | <b>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></b>                                 |
| SVM上の特定のドメインまたはローカルのユーザとグループのカスタム権限                             | <b>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></b> |

ほかにも、このコマンドを実行するときに選択できるオプションのパラメータがあります。詳細については、マニュアル ページを参照してください。

#### 例

次のコマンドを実行すると、SVM vs1のローカルまたはドメインのユーザとグループに明示的に関連付けられているすべての権限が表示されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                     SeRestorePrivilege
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                     SeTakeOwnershipPrivilege
```

## トラバース チェックのバイパスの設定

トラバース チェックのバイパスは、トラバースするディレクトリに対する **権限** がユーザにない場合でも、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできるかどうかを判断す

るユーザ権限です。トラバース チェックのバイパスを許可または拒否した場合の動作と、Storage Virtual Machine (SVM) でのユーザに対するトラバース チェックのバイパスの設定方法を理解しておく必要があります。

### トラバース チェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとすると、中間ディレクトリのトラバース権限がチェックされないで、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、Data ONTAPはファイルのパスにあるすべてのディレクトリでトラバース(実行)権限をチェックします。  
いずれかの中間ディレクトリに「X」(トラバース権限)がない場合は、このファイルへのアクセスが拒否されます。

### トラバース チェックのバイパスの設定方法

Data ONTAP CLIを使用するか、Active Directoryグループ ポリシーにこのユーザ権限を設定すると、トラバース チェックのバイパスを設定できます。

**SeChangeNotifyPrivilege**権限は、ユーザがトラバース チェックのバイパスを許可されているかを制御します。

- この権限をSVMのローカルSMBユーザまたはグループ、ドメイン ユーザまたはグループに追加すると、トラバース チェックのバイパスを許可できます。
- この権限をSVMのローカルSMBユーザまたはグループ、ドメイン ユーザまたはグループから削除すると、トラバース チェックのバイパスを拒否できます。

デフォルトで、SVMの次のBUILTINグループがトラバース チェックのバイパス権限を持っています。

- **BUILTIN\Administrators**
- **BUILTIN\Power Users**
- **BUILTIN\Backup Operators**
- **BUILTIN\Users**
- **Everyone**

これらのいずれかのグループのメンバーにトラバース チェックのバイパスを許可したくない場合は、グループからこの権限を削除する必要があります。

CLIを使用してSVMローカルSMBユーザおよびグループのトラバース チェックのバイパスを設定する場合は、次の点に注意する必要があります。

- カスタムのローカルまたはドメイン グループのメンバーにトラバース チェックのバイパスを許可したい場合は、グループに**SeChangeNotifyPrivilege**権限を追加する必要があります。
- ローカルまたはドメイン ユーザに個別にトラバース チェックのバイパスを許可したい場合に、そのユーザが権限を持つグループのメンバーでない場合は、ユーザ アカウントに**SeChangeNotifyPrivilege**権限を追加できます。
- ローカルまたはドメインのユーザやグループから**SeChangeNotifyPrivilege**権限を削除すると、いつでもトラバース チェックのバイパスを無効にできます。

**注:** 特定のローカルまたはドメインのユーザやグループに対してトラバース チェックのバイパスを無効にするには、**Everyone**グループからも**SeChangeNotifyPrivilege**権限を削除する必要があります。

**関連コンセプト**[SMB共有のACLを使用したファイル アクセスの保護](#)(190ページ)[ファイル権限を使用したファイル アクセスの保護](#)(193ページ)[ローカル権限の管理](#)(239ページ)**関連タスク**[ユーザまたはグループに対するディレクトリのトラバース チェックのバイパスの許可](#)(244ページ)[ユーザまたはグループに対するディレクトリのトラバース チェックのバイパスの禁止](#)(245ページ)[FlexVolでのSMBファイル名の変換のための文字マッピングの設定](#)(164ページ)[CIFSサーバでのSMB共有の作成](#)(180ページ)**関連参照情報**[サポートされる権限の一覧](#)(220ページ)**ユーザまたはグループに対するディレクトリのトラバース チェックのバイパスの許可**

トラバースするディレクトリに対する権限がない場合でも、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできるようにするには、Storage Virtual Machine (SVM) のローカル SMBユーザまたはグループに**SeChangeNotifyPrivilege**権限を追加します。デフォルトでは、ユーザはディレクトリのトラバース チェックをバイパスできます。

**開始する前に**

- SVM上にCIFSサーバが存在している必要があります。
- ローカル ユーザとローカル グループのCIFSサーバオプションが有効になっている必要があります。
- **SeChangeNotifyPrivilege**権限を追加する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

**タスク概要**

ドメイン ユーザまたはグループへの権限の追加時、Data ONTAPでは、ドメイン コントローラに接続してそのドメイン ユーザまたはグループを検証することがあります。Data ONTAPからドメイン コントローラに照会できない場合、コマンドが失敗することがあります。

**手順**

1. ローカルまたはドメインのユーザまたはグループに**SeChangeNotifyPrivilege**権限を追加して、トラバース チェックのバイパスを有効にします。

```
vserver cifs users-and-groups privilege add-privilege -vserver
vserver_name -user-or-group-name name -privileges
SeChangeNotifyPrivilege
```

-user-or-group-nameパラメータの値には、ローカル ユーザまたはグループか、ドメイン ユーザまたはグループを指定します。

2. 指定したユーザまたはグループに対してトラバース チェックのバイパスが有効になっていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-
or-group-name name
```

**例**

次のコマンドを実行すると、「EXAMPLE\eng」グループに**SeChangeNotifyPrivilege**権限が追加されて、このグループに属するユーザがディレクトリのトラバース チェックをバイパスできるようになります。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

**関連タスク**

[ユーザまたはグループに対するディレクトリのトラバース チェックのバイパスの禁止](#) (245ページ)

**ユーザまたはグループに対するディレクトリのトラバース チェックのバイパスの禁止**

トラバースするディレクトリに対する権限がない場合に、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできないようにするには、Storage Virtual Machine (SVM) のローカル SMBユーザまたはグループから**SeChangeNotifyPrivilege**権限を削除します。

**開始する前に**

権限を削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

**タスク概要**

ドメイン ユーザまたはグループから権限を削除するときに、Data ONTAPがドメイン コントローラに照会してそのドメイン ユーザまたはグループを検証することがあります。Data ONTAPからドメイン コントローラに照会できない場合、コマンドが失敗することがあります。

**手順**

1. トラバース チェックのバイパスを禁止します。

```
vserver cifs users-and-groups privilege remove-privilege -vserver
vserver_name -user-or-group-name name -privileges
SeChangeNotifyPrivilege
```

このコマンドを実行すると、-user-or-group-nameのname/パラメータの値で指定したローカルまたはドメインのユーザまたはグループから**SeChangeNotifyPrivilege**権限が削除されます。

2. 指定したユーザまたはグループに対してトラバース チェックのバイパスが無効になっていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-
or-group-name name
```

**例**

次のコマンドを実行すると、「EXAMPLE\eng」グループに属するユーザに対して、ディレクトリのトラバース チェックのバイパスが禁止されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name   Privileges
-----
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege -vserver vs1 -user-
or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name   Privileges
-----
vs1       EXAMPLE\eng          -
```

#### 関連タスク

[ユーザまたはグループに対するディレクトリのトラバース チェックのバイパスの許可](#) (244ページ)

## ファイル セキュリティと監査ポリシーに関する情報の表示

Storage Virtual Machine (SVM) のボリューム内に格納されたファイルとディレクトリのファイル セキュリティに関する情報を表示できます。FlexVolの監査ポリシーに関する情報を表示できます。設定されている場合、FlexVolのストレージレベルのアクセス保護およびダイナミック アクセス制御セキュリティの設定に関する情報を表示できます。

#### ファイル セキュリティに関する情報の表示

次のセキュリティ形式のボリュームと (FlexVolの) qtrees に格納されたデータに適用されているファイル セキュリティに関する情報を表示できます。

- NTFS
- UNIX
- Mixed
- Unified (Infinite Volume)

#### 監査ポリシーに関する情報の表示

次のNASプロトコルを介したFlexVolのアクセス イベントを監査する監査ポリシーに関する情報を表示できます。

- SMB (すべてのバージョン)
- NFSv4.x

**注:** Infinite Volumeに格納されたファイルとディレクトリに対してSACLを設定することは可能ですが、clustered Data ONTAPではInfinite Volumeを備えたSVMの監査はサポートされていません。

#### ストレージレベルのアクセス保護 (SLAG) セキュリティに関する情報の表示

ストレージレベルのアクセス保護セキュリティは、次のセキュリティ形式のFlexVolオブジェクトに適用できます。

- NTFS
- Mixed
- UNIX (ボリュームが含まれるSVMでCIFSサーバが設定されている場合)

ダイナミック アクセス制御(DAC)セキュリティに関する情報の表示

ダイナミック アクセス制御セキュリティは、次のセキュリティ形式のFlexVol内のオブジェクトに適用できます。

- NTFS
- Mixed(オブジェクトにNTFS対応のセキュリティが設定されている場合)

関連コンセプト

- [セキュリティ形式がデータ アクセスに与える影響](#)(20ページ)
- [CLIを使用したSVMのNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理](#)(257ページ)
- [ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#)(154ページ)

関連タスク

- [ストレージレベルのアクセス保護に関する情報の表示](#)(162ページ)
- [セキュリティトレースの実行](#)(292ページ)

NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、DOS属性に関する情報など、NTFSセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

タスク概要

- Storage Virtual Machine (SVM) の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。
- NTFSセキュリティ形式のボリュームとqtreeでは、NTFSファイル権限およびWindowsのユーザとグループのみを使用してファイルのアクセス権を判断するため、UNIX関連の出力フィールドのUNIXファイル権限情報は表示のみです。
  - ACL出力は、NTFSセキュリティが適用されたファイルとフォルダについて表示されます。
  - ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたはqtreeで設定できるので、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルACLとストレージレベルのアクセス保護ACLの両方が表示されることがあります。
  - そのファイルまたはディレクトリ パスにダイナミック アクセス制御が設定されていれば、ダイナミック アクセス制御ACEに関する情報も出力に表示されます。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

| 表示する情報 | 入力するコマンド                                                                                             |
|--------|------------------------------------------------------------------------------------------------------|
| 要約形式   | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| 詳細を表示  | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

**例**

次の例では、SVM vs1のパス/vol4に関するセキュリティ情報を表示します。

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

Vserver: vs1
File Path: /vol4
File Inode Number: 64
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-0I|CI|IO
```

次の例では、マスクを展開して、SVM vs1のパス/data/engineeringに関するセキュリティ情報を表示します。

```
cluster::> vserver security file-directory show -vserver vs1 -path -path /data/
engineering -expand-mask true

Vserver: vs1
File Path: /data/engineering
File Inode Number: 5544
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
  ...0 ... = Offline
  ... ..0. ... = Sparse
  ... ..0. ... = Normal
  ... ..0. ... = Archive
  ... ..1 ... = Directory
  ... ..0.. = System
  ... ..0.. = Hidden
  ... ..0 ... = Read Only
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004

  1... .. = Self Relative
  ..0.. .. = RM Control Valid
  ..0. ... = SACL Protected
  ...0 ... = DACL Protected
  ... 0... = SACL Inherited
  ... ..0. = DACL Inherited
  ... ..0. = SACL Inherit Required
  ... ..0 ... = DACL Inherit Required
  ... ..0. ... = SACL Defaulted
  ... ..0 ... = SACL Present
  ... ..0 ... = DACL Defaulted
  ... ..1.. = DACL Present
  ... ..0 ... = Group Defaulted
  ... ..0 ... = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
  0... .. = Generic Read
  ..0. ... = Generic Write
  ...0 ... = Generic Execute
  ...0 ... = Generic All
  ... ..0 ... = System Security
  ... ..1 ... = Synchronize
  ... ..1 ... = Write Owner
  ... ..1 ... = Write DAC
  ... ..1 ... = Read Control
  ... ..1 ... = Delete
  ... ..1 ... = Write Attributes
  ... ..1 ... = Read Attributes
```



```

.....1.. = Delete Child
.....1.. = Execute
.....1.. = Write EA
.....1.. = Read EA
.....1.. = Append
.....1.. = Write
.....1.. = Read

ALLOW-Everyone-0x10000000-0I|CI|IO
0... = Generic Read
.0... = Generic Write
..0... = Generic Execute
...1... = Generic All
.....0... = System Security
.....0... = Synchronize
.....0... = Write Owner
.....0... = Write DAC
.....0... = Read Control
.....0... = Delete
.....0... = Write Attributes
.....0... = Read Attributes
.....0... = Delete Child
.....0... = Execute
.....0... = Write EA
.....0... = Read EA
.....0... = Append
.....0... = Write
.....0... = Read

```

次の例では、SVM vs1のパス/datavol1にあるボリュームの、ストレージレベルのアクセス保護セキュリティ情報を含むセキュリティ情報を表示します。

```

cluster::> vserver security file-directory show -vserver vs1 -path /datavol1

Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-0I|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## 関連タスク

[mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (250ページ)

[UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (252ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver security file-directory show - Display file/folder security information](#)

## mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、mixedセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine (SVM) の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

- mixedセキュリティ形式のボリュームおよびqtreeには、UNIXファイル権限(モードビットまたは NFSv4 ACL)を使用するファイルやフォルダと、NTFSファイル権限を使用するファイルやディレクトリを格納できます。
- mixedセキュリティ形式のボリュームの最上位には、UNIX対応のセキュリティまたはNTFS対応のセキュリティを設定できます。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。  
このフィールドは、モードビットの権限のみ(NFSv4 ACLはなし)が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。
- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、たとえボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXでも、mixedセキュリティ形式のボリュームまたはqtreeで設定できるので、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、UNIXファイル権限とストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミック アクセス制御が設定されていれば、ダイナミック アクセス制御ACEに関する情報も出力に表示されます。

### 手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

| 表示する情報 | 入力するコマンド                                                                                             |
|--------|------------------------------------------------------------------------------------------------------|
| 要約形式   | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| 詳細を表示  | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

### 例

次の例では、マスクを展開した形式で、SVM vs1のパス/projectsに関するセキュリティ情報を表示します。このmixedセキュリティ形式のパスには、UNIX対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /projects -expand-mask true

Vserver: vs1
File Path: /projects
File Inode Number: 78
Security Style: mixed
Effective Style: unix
```

```

DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
...0 .... = Offline
... ..0. .... = Sparse
... .. 0... .... = Normal
... .. ..0. .... = Archive
... .. ...1 .... = Directory
... .. ... .0.. = System
... .. ... ..0. = Hidden
... .. ... ..0 = Read Only
    Unix User Id: 0
    Unix Group Id: 1
    Unix Mode Bits: 700
Unix Mode Bits in Text: rwx-----
ACLs: -

```

次の例では、SVM vs1のパス/dataに関するセキュリティ情報を表示します。このmixedセキュリティ形式のパスには、NTFS対応のセキュリティが設定されています。

```

cluster1::> vserver security file-directory show -vserver vs1 -path /
data

Vserver: vs1
File Path: /data
File Inode Number: 544
Security Style: mixed
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    ALLOW-Everyone-0x10000000-0I|CI|IO

```

次の例では、SVM vs1のパス/datavol5にあるボリュームに関するセキュリティ情報を表示します。このmixedセキュリティ形式のボリュームの最上位には、UNIX対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```

cluster1::> vserver security file-directory show -vserver vs1 -path /
datavol5

Vserver: vs1
File Path: /datavol5
File Inode Number: 3374
Security Style: mixed
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
ACLs: Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    AUDIT-EXAMPLE\market-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-BUILTIN\Administrators-0x1f01ff
    ALLOW-CREATOR OWNER-0x1f01ff
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-EXAMPLE\market-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    AUDIT-EXAMPLE\market-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-BUILTIN\Administrators-0x1f01ff

```

```
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-EXAMPLE\market-0x1f01ff
```

## 関連タスク

[NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (247ページ)

[UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (252ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vservers security file-directory show - Display file/folder security information](#)

## UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、UNIXセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine (SVM) の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

- ファイル権限の決定時、UNIXセキュリティ形式のボリュームおよびqtreeでは、UNIXファイル権限 (モードビットまたはNFSv4 ACL) のみが使用されます。
- ACL出力は、NFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。このフィールドは、モードビットの権限のみ (NFSv4 ACLはなし) が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。
- ACL出力の所有者とグループの出力フィールドは、NFSv4セキュリティ記述子には該当しません。これらのフィールドが意味があるのは、NTFSセキュリティ記述子の場合のみです。
- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合にUNIX形式のボリュームやqtreeでサポートされるので、-pathパラメータで指定されたボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります。

### 手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

| 表示する情報 | 入力するコマンド                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------|
| 要約形式   | <code>vservers security file-directory show -vservers vservers_name -path path</code>                   |
| 詳細を表示  | <code>vservers security file-directory show -vservers vservers_name -path path -expand-mask true</code> |

### 例

次の例では、SVM vs1のパス/homeに関するセキュリティ情報を表示します。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

      Vserver: vs1
      File Path: /home
      File Inode Number: 9590
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
      Unix Mode Bits in Text: rwx-----
      ACLs: -

```

次の例では、マスクを展開した形式で、SVM vs1のパス/homeに関するセキュリティ情報を表示します。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home -expand-mask true
```

```

      Vserver: vs1
      File Path: /home
      File Inode Number: 9590
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: 0x10
        ...0 ... .. = Offline
        ... ..0. ... .. = Sparse
        ... ..0 ... .. = Normal
        ... ..0. ... .. = Archive
        ... ..1 ... .. = Directory
        ... ..0. ... .. = System
        ... ..0. ... .. = Hidden
        ... ..0 ... .. = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
      Unix Mode Bits in Text: rwx-----
      ACLs: -

```

## 関連タスク

[NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (247ページ)

[mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#) (250ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver security file-directory show - Display file/folder security information](#)

## CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システム アクセス制御リストに関する情報など、FlexVolのNTFS監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine (SVM) の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力は、要約形式または詳細なリストで表示できます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、NTFSのSystem Access Control List (SACL; システム アクセス制御リスト) のみが監査ポリシーに使用されます。
- NTFS対応のセキュリティが有効なmixedセキュリティ形式のボリューム内のファイルおよびフォルダには、NTFS監査ポリシーを適用できます。

mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル アクセス権(モードビットまたはNFSv4 ACL)を使用するファイルおよびディレクトリと、NTFSファイル アクセス権を使用するファイルおよびディレクトリを格納できます。

- mixedセキュリティ形式のボリュームの最上位では、UNIXまたはNTFS対応のセキュリティを有効にすることができ、そこにはNTFS SACLが格納されている場合も、格納されていない場合もあります。
- mixedセキュリティ形式のボリュームまたはqtreeでは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、ストレージレベルのアクセス保護セキュリティを設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeの出力には、標準ファイルおよびフォルダのNFSv4 SACLとストレージレベルのアクセス保護のNTFS SACLの両方が表示される場合があります。
- NTFS対応のセキュリティが有効なデータへのパスをコマンドに入力した場合、所定のファイルまたはディレクトリ パスでダイナミック アクセス制御が設定されていれば、出力にダイナミック アクセス制御のACEに関する情報も表示されます。
- NTFS対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報の表示時には、UNIX関連の出力フィールドに表示専用のUNIXファイル アクセス権情報が格納されます。  
ファイル アクセス権の決定時には、NTFSセキュリティ形式のファイルおよびフォルダで、NTFSファイル アクセス権とWindowsユーザおよびグループのみが使用されます。
- ACL出力は、NTFSまたはNFSv4セキュリティ形式によるファイルおよびフォルダでのみ表示されます。  
このフィールドは、モード ビットのアクセス権のみ(NFSv4 ACLはなし)が適用されているUNIXセキュリティ形式のファイルおよびフォルダでは空になります。
- ACL出力の所有者およびグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。

## 手順

1. ファイルおよびディレクトリ監査ポリシー設定を適切な詳細レベルで表示します。

| 情報の表示方法 | 入力するコマンド                                                                                             |
|---------|------------------------------------------------------------------------------------------------------|
| 要約形式    | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| 詳細情報を展開 | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

## 例

次の例は、SVM vs1のパス/corpに関する監査ポリシーの情報を表示します。このパスではNTFS対応のセキュリティが有効になっています。NTFSセキュリティ記述子には、SUCCESSおよびSUCCESS / FAIL SACLエントリの両方が格納されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
Vserver: vs1
File Path: /corp
File Inode Number: 357
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8014
Owner:DOMAIN\Administrator
```

```

Group:BUILTIN\Administrators
SACL - ACES
  ALL-DOMAIN\Administrator-0x100081-0I|CI|SA|FA
  SUCCESSFUL-DOMAIN\user1-0x100116-0I|CI|SA
DACL - ACES
  ALLOW-BUILTIN\Administrators-0x1f01ff-0I|CI
  ALLOW-BUILTIN\Users-0x1f01ff-0I|CI
  ALLOW-CREATOR OWNER-0x1f01ff-0I|CI
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-0I|CI

```

次の例は、SVM vs1のパスSVMに関する監査ポリシーの情報を表示します。このパスには、標準ファイルおよびフォルダのSACLとストレージレベルのアクセス保護のSACLの両方が格納されています。

```

cluster::> vserver security file-directory show -vserver vs1 -path /datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            SACL - ACES
              AUDIT-EXAMPLE\marketing-0xf01ff-0I|CI|FA
            DACL - ACES
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-0I|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-0I|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## CLIを使用したFlexVolのNFSv4監査ポリシーに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、System Access Control List (SACL;システム アクセス制御リスト)に関する情報など、Data ONTAP CLIを使用してFlexVolのNFSv4監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine (SVM) の名前、および監査情報を表示するファイルまたはディレクトリのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

- UNIXセキュリティ形式のボリュームおよびqtreeでは、監査ポリシーにNFSv4 SACLのみが使用されます。
- mixedセキュリティ形式のボリュームにあるUNIXセキュリティ形式のファイルとディレクトリには、NFSv4監査ポリシーを適用できます。  
mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限(モード ビットまたはNFSv4 ACL)を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixedセキュリティ形式のボリュームの最上位には、UNIXまたはNTFS対応のセキュリティを適用でき、NFSv4 SACLが含まれる場合と含まれない場合があります。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。  
このフィールドは、モード ビットの権限のみ(NFSv4 ACLはなし)が適用されているUNIXセキュリティ形式のファイルおよびフォルダでは空になります。
- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- mixedセキュリティ形式のボリュームまたはqtreeには、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXでも、ストレージレベルのアクセス保護セキュリティを設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のNFSv4ファイルおよびディレクトリのSACLとストレージレベルのアクセス保護のNTFS SACLの両方が表示されることがあります。
- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合にUNIX形式のボリュームやqtreeでサポートされるので、-pathパラメータで指定されたボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります。

#### 手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

| 表示する情報 | 入力するコマンド                                                                                             |
|--------|------------------------------------------------------------------------------------------------------|
| 要約形式   | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| 詳細を表示  | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

#### 例

次の例では、SVM vs1のパス/labに関するセキュリティ情報を表示します。このUNIXセキュリティ形式のパスにはNFSv4 SACLが設定されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
      File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
      DOS Attributes in Text: ---D--R
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
      Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACES
              SUCCESSFUL-S-1-520-0-0xf01ff-SA
              FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACES
              ALLOW-S-1-520-1-0xf01ff
```



## CLIを使用したSVMのNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理

CLIを使用して、FlexVolを備えたStorage Virtual Machine (SVM) のNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護を管理できます。

NTFSファイル セキュリティと監査ポリシーは、SMBクライアントから、またはCLIを使用して管理できます。ただし、CLIを使用してファイル セキュリティと監査ポリシーを設定する場合、リモートクライアントを使用せずにファイル セキュリティを管理できます。CLIを使用すると、多数のファイルやフォルダに対してセキュリティを適用する場合でも1つのコマンドで実行できるため、作業時間を大幅に短縮できます。

Data ONTAPがSVMボリュームに提供するもう1つのセキュリティレイヤであるストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護は、すべてのNASプロトコルからストレージレベルのアクセス保護が適用されるストレージオブジェクトへのアクセスに適用されます。

ストレージレベルのアクセス保護はData ONTAP CLIからのみ設定および管理できます。ストレージレベルのアクセス保護設定をSMBクライアントから管理することはできません。さらに、NFSやSMBクライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。システム (WindowsまたはUNIX) 管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が独立して設定および管理できるセキュリティレイヤをデータアクセスに追加で提供します。

**注:** ストレージレベルのアクセス保護ではNTFSのアクセス権のみがサポートされます。ただし、ストレージレベルのアクセス保護が適用されているボリューム上のデータへのNFS経由のアクセスに対しても、そのボリュームを所有するSVM上のWindowsユーザにUNIXユーザがマッピングされている場合は、Data ONTAPでセキュリティチェックを実行できます。

### NTFSセキュリティ形式のボリューム

NTFSのセキュリティ形式のボリュームやqtreeに格納されているファイルやフォルダはすべて、NTFS対応のセキュリティが有効になります。vserver security file-directoryコマンドファミリーを使用すると、NTFSセキュリティ形式のボリュームに次の種類のセキュリティを実装できます。

- ボリュームに含まれるファイルやフォルダに対するファイル権限と監査ポリシー
- ボリュームに対するストレージレベルのアクセス保護セキュリティ

### mixedセキュリティ形式のボリューム

mixedセキュリティ形式のボリュームやqtreeには、次のようなファイルやフォルダを格納できます。UNIX対応のセキュリティが有効で、UNIXファイル権限 (モード ビットまたはNFSv4.x ACL) とNFSv4.x監査ポリシーを使用するファイルやフォルダ。NTFS対応のセキュリティが有効で、NTFSファイル権限と監査ポリシーを使用するファイルやフォルダ。vserver security file-directoryコマンドファミリーを使用すると、mixedセキュリティ形式のデータに次の種類のセキュリティを適用できます。

- mixed形式のボリュームやqtreeでのNTFS対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- NTFS対応またはUNIX対応のセキュリティ形式のボリュームに対するストレージレベルのアクセス保護

## UNIXセキュリティ形式のボリューム

UNIXセキュリティ形式のボリュームとqtreetには、UNIX対応のセキュリティ(モード ビットまたは NFSv4.x ACL)を備えたファイルとフォルダが含まれます。vserver security file-directoryコマンド ファミリーを使用してUNIXセキュリティ形式のボリュームにセキュリティを実装する場合、次の点に留意する必要があります。

- UNIXセキュリティ形式のボリュームやqtreeでは、vserver security file-directoryコマンド ファミリーを使用してUNIXファイル セキュリティや監査ポリシーを管理することはできません。
- そのボリュームを含むSVMにCIFSサーバが含まれる場合は、vserver security file-directoryコマンド ファミリーを使用してUNIXセキュリティ形式のボリュームにストレージレベルのアクセス保護を設定できます。

## 関連コンセプト

[ファイル セキュリティと監査ポリシーに関する情報の表示](#)(246ページ)

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#)(154ページ)

## 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用](#)(261ページ)

[CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用](#)(275ページ)

## CLIを使用してファイルおよびフォルダのセキュリティを設定するユースケース

ファイルおよびフォルダのセキュリティは、リモート クライアントを使用しなくても、ローカルで適用および管理できます。これにより、多数のファイルやフォルダに対して一括でセキュリティを設定するのにかかる時間を大幅に短縮することができます。

CLIを使用してファイルおよびフォルダのセキュリティを設定すると効果的な状況として、次のようなユースケースがあります。

- 大企業の環境でのファイルの保管(ホーム ディレクトリのファイル ストレージなど)
- データの移行
- Windowsドメインの変更
- NTFSファイルシステムのファイル セキュリティと監査ポリシーの標準化

## CLIを使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項

ファイルおよびフォルダのセキュリティ設定でCLIを使用する際には、一定の制限事項を知っておく必要があります。

- vserver security file-directoryコマンド ファミリーはNFSv4 ACLの設定をサポートしていません。  
NTFSのセキュリティ記述子はNTFSファイルとNTFSフォルダにのみ適用できます。
- vserver security file-directoryコマンド ファミリーは、Infinite Volumeを備えたStorage Virtual Machine(SVM)上のファイル セキュリティ設定(NTFSまたはNFSv4)をサポートしていません。

## セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

セキュリティ記述子には、ユーザがファイルやフォルダに対して実行できる操作、およびユーザがファイルやフォルダにアクセスするときに監査される内容を決定するアクセス制御リストが含まれます。

### 権限

権限はオブジェクトの所有者によって許可または拒否され、オブジェクト(ユーザ、グループ、またはコンピュータ オブジェクト)が指定されたファイルまたはフォルダに対して実行できる操作を決定します。

### セキュリティ記述子

セキュリティ記述子は、ファイルまたはフォルダに関連付けられた権限を定義するセキュリティ情報を含むデータ構造です。

#### Access Control List (ACL; アクセス制御リスト)

アクセス制御リストは、セキュリティ記述子内に含まれるリストです。セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータ オブジェクトが実行できる操作に関する情報を示します。セキュリティ記述子には、次の2種類のACLを含めることができます。

- Discretionary Access Control List (DACL; 随意アクセス制御リスト)
- System Access Control List (SACL; システム アクセス制御リスト)

#### Discretionary Access Control List (DACL; 随意アクセス制御リスト)

DACLには、ファイルまたはフォルダに対して操作を実行するためのアクセスが許可または拒否されるユーザ、グループ、およびコンピュータ オブジェクトのSIDリストが含まれます。DACLには、0個以上のAccess Control Entry (ACE; アクセス制御エントリ)が含まれます。

#### System Access Control List (SACL; システム アクセス制御リスト)

SACLには、成功または失敗した監査イベントがログに記録されるユーザ、グループ、およびコンピュータ オブジェクトのSIDリストが含まれます。SACLには、0個以上のAccess Control Entry (ACE; アクセス制御エントリ)が含まれます。

#### Access Control Entry (ACE; アクセス制御エントリ)

ACEは、DACLまたはSACL内の個々のエントリです。

- DACLアクセス制御エントリは、特定のユーザ、グループ、またはコンピュータ オブジェクトに対して許可または拒否されるアクセス権を指定します。
- SACLアクセス制御エントリは、特定のユーザ、グループ、またはコンピュータ オブジェクトによって実行される指定された操作の監査時にログに記録される成功または失敗イベントを指定します。

### 権限の継承

権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトの権限を設定するときに、「**this-folder**、**sub-folders**、および**files**への適用」によって、フォルダ、サブフォルダ、およびファイルがその権限を継承できるかどうかを決定できます。

### 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用](#) (261ページ)

[Windowsの\[セキュリティ\]タブを使用した標準のNTFSファイル権限の設定](#) (194ページ)

[Windowsの\[セキュリティ\]タブを使用した詳細なNTFSファイル権限の設定](#)(196ページ)

[CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用](#)(275ページ)

[Windowsの\[セキュリティ\]タブを使用したNTFS監査ポリシーの設定](#)(451ページ)

## SVMディザスタリカバリ デスティネーションでローカル ユーザまたはグループを使用するファイルとディレクトリのポリシーを適用する際の考慮事項

ファイルとディレクトリのポリシー設定がセキュリティ記述子、DACL、SACLエントリのいずれかでローカル ユーザまたはグループを使用する場合、ID破棄設定のStorage Virtual Machine (SVM) ディザスタリカバリ デスティネーションでファイルとディレクトリのポリシーを適用する前に注意すべきいくつかの考慮事項があります。

ソース クラスタのソースSVMが、ソースSVMからデスティネーション クラスタのデスティネーション SVMにデータと設定をレプリケーションするSVMディザスタリカバリ構成を設定できます。

SVMディザスタリカバリの2つのタイプのうち1つを設定できます。

- ID維持  
この設定では、SVMとCIFSサーバのIDが維持されます。
- ID破棄  
この設定では、SVMとCIFSサーバのIDが維持されません。このシナリオでは、デスティネーションSVMのSVMとCIFSサーバの名前は、ソースSVMのSVMとCIFSサーバの名前と異なります。

### ID破棄設定についての考慮事項

ID破棄設定では、ローカル ユーザ、グループ、権限設定、ローカルドメインの名前(ローカルCIFSサーバ名)を含むSVMソースをSVMデスティネーションのCIFSサーバ名に一致するように変更する必要があります。たとえば、ソースSVM名が「vs1」でCIFSサーバ名が「CIFS1」、デスティネーションSVM名が「vs1\_dst」でCIFSサーバ名が「CIFS1\_DST」の場合、「CIFS1\user1」という名前のローカル ユーザのローカルドメイン名は、デスティネーションSVMで自動的に「CIFS1\_DST\user1」に変更されます。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

| Vserver               | User Name           | Full Name | Description |
|-----------------------|---------------------|-----------|-------------|
| vs1                   | CIFS1\Administrator |           | Built-in    |
| administrator account |                     |           |             |
| vs1                   | CIFS1\user1         | -         | -           |

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

| Vserver               | User Name               | Full Name | Description |
|-----------------------|-------------------------|-----------|-------------|
| vs1_dst               | CIFS1_DST\Administrator |           | Built-in    |
| administrator account |                         |           |             |
| vs1_dst               | CIFS1_DST\user1         | -         | -           |

ローカル ユーザおよびグループ データベースでローカル ユーザおよびグループ名が自動的に変更されても、ファイルとディレクトリのポリシー設定(vserver security file-directoryコマンドファミリーを使用してCLIで設定するポリシー)のローカル ユーザまたはグループ名は自動的に変更されません。

たとえば、「vs1」で-accountパラメータが「CIFS1\user1」に設定されたDACLエントリを設定している場合、デスティネーションSVMでこの設定がデスティネーションCIFSサーバ名を反映して自動的に変更されることはありません。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name | Access Type | Access Rights | Apply To    |
|--------------|-------------|---------------|-------------|
| -----        | -----       | -----         | -----       |
| CIFS1\user1  | allow       | full-control  | this-folder |

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
Vserver: vs1_dst
NTFS Security Descriptor Name: sd1
```

| Account Name        | Access Type | Access Rights | Apply To    |
|---------------------|-------------|---------------|-------------|
| -----               | -----       | -----         | -----       |
| <b>CIFS1</b> \user1 | allow       | full-control  | this-folder |

手動で `vserver security file-directory modify` コマンドを使用して、CIFSサーバ名をデスティネーションCIFSサーバ名に変更する必要があります。

### アカウント パラメータを含むファイルとディレクトリのポリシー設定コンポーネント

ローカル ユーザまたはグループを含むパラメータ設定を使用できるファイルとディレクトリのポリシー設定コンポーネントは3つあります。

- セキュリティ記述子  
オプションで、セキュリティ記述子の所有者とセキュリティ記述子の所有者のプライマリ グループを指定できます。セキュリティ記述子で所有者とプライマリ グループのエントリにローカル ユーザまたはグループを使用する場合、デスティネーションSVMにアカウント名を使用するようにセキュリティ記述子を変更する必要があります。アカウント名に必要な変更を行うには、`vserver security file-directory ntfs modify` コマンドを使用します。
- DACLエントリ  
各DACLエントリは、アカウントと関連付ける必要があります。ローカル ユーザまたはグループアカウントを使用するDACLは、すべてデスティネーションSVM名を使用するように変更する必要があります。既存のDACLエントリのアカウント名は変更できないため、ローカル ユーザまたはグループが設定されたすべてのDACLエントリをセキュリティ記述子から削除し、訂正したデスティネーション アカウント名を設定した新しいDACLエントリを作成し、その新しいDACLエントリを適切なセキュリティ記述子と関連付ける必要があります。
- SACLエントリ  
各SACLエントリは、アカウントと関連付ける必要があります。ローカル ユーザまたはグループアカウントを使用するSACLは、すべてデスティネーションSVM名を使用するように変更する必要があります。既存のSACLエントリのアカウント名は変更できないため、ローカル ユーザまたはグループが設定されたすべてのSACLエントリをセキュリティ記述子から削除し、訂正したデスティネーション アカウント名を設定した新しいSACLエントリを作成し、その新しいSACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

ポリシーを適用する前に、ファイルとディレクトリのポリシー設定で使用されているローカル ユーザまたはグループに必要な変更を行う必要があります。そうでない場合、適用ジョブは失敗します。

## CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用

Data ONTAP CLIを使用してNTFSファイル セキュリティを適用するには、いくつかの手順を実行する必要があります。まず、NTFSセキュリティ記述子を作成し、DACLをセキュリティ記述子に追加

します。次に、セキュリティ ポリシーを作成してポリシー タスクを追加します。その後、FlexVolを備えたStorage Virtual Machine(SVM)にセキュリティ ポリシーを適用します。

### タスク概要

セキュリティ ポリシーを適用したら、セキュリティ ポリシー ジョブを監視して、適用したファイル セキュリティの設定を確認することができます。

### 手順

1. [NTFSセキュリティ記述子の作成](#) (263ページ)  
NTFSセキュリティ記述子の作成は、FlexVolを備えたStorage Virtual Machine(SVM)内に存在するファイルやフォルダのNTFS Access Control List(ACL;アクセス制御リスト)を設定および適用するための最初のステップです。このセキュリティ記述子をポリシー タスクでファイル パスまたはフォルダ パスに関連付けます。
2. [NTFSセキュリティ記述子へのNTFS DACLアクセス制御エントリの追加](#) (265ページ)  
NTFSセキュリティ記述子へのDACL(随意アクセス制御リスト)アクセス制御エントリ(ACE)の追加は、ファイルまたはフォルダに対するNTFS ACLの設定および適用における2番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、ACEで定義されているファイルまたはフォルダに対してオブジェクトが実行できる操作または実行できない操作が定義されます。
3. [セキュリティ ポリシーの作成](#) (268ページ)  
FlexVolを備えたStorage Virtual Machine(SVM)のセキュリティ ポリシーの作成は、ファイルまたはフォルダに対してACLを設定および適用する3番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティ ポリシーにタスクを追加します。
4. [セキュリティ ポリシーへのタスクの追加](#) (269ページ)  
ACLを設定し、FlexVolを備えたStorage Virtual Machine(SVM)内のファイルやフォルダへ適用する4番目のステップでは、ポリシー タスクを作成してセキュリティ ポリシーに追加します。ポリシー タスクを作成する場合、セキュリティ ポリシーとタスクを関連付けます。セキュリティ ポリシーには、1つまたは複数のタスク エントリを追加できます。
5. [セキュリティ ポリシーの適用](#) (272ページ)  
FlexVolを備えたStorage Virtual Machine(SVM)へのセキュリティ ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。
6. [セキュリティ ポリシー ジョブの監視](#) (273ページ)  
FlexVolを備えたStorage Virtual Machine(SVM)にセキュリティ ポリシーを適用する場合、セキュリティ ポリシー ジョブをモニタして、ポリシー適用のタスクの進行状況を監視できます。セキュリティ ポリシーの適用が正常に完了したかどうかを確認する上で、この機能が役に立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この機能は有用です。
7. [適用したファイル セキュリティの監視](#) (273ページ)  
FlexVolを備えたStorage Virtual Machine(SVM)のファイルやフォルダにセキュリティ ポリシーを適用した場合に、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

### 関連コンセプト

- [ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#) (154ページ)
- [CLIを使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項](#) (258ページ)
- [セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法](#) (259ページ)

### 関連タスク

- [Windowsの\[セキュリティ\]タブを使用した標準のNTFSファイル権限の設定](#) (194ページ)

[Windowsの\[セキュリティ\]タブを使用した詳細なNTFSファイル権限の設定](#)(196ページ)  
[NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#)(247ページ)  
[mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#)(250ページ)  
[UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示](#)(252ページ)  
[CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用](#)(275ページ)

## NTFSセキュリティ記述子の作成

NTFSセキュリティ記述子の作成は、FlexVolを備えたStorage Virtual Machine (SVM) 内に存在するファイルやフォルダのNTFS Access Control List (ACL; アクセス制御リスト)を設定および適用するための最初のステップです。このセキュリティ記述子をポリシー タスクでファイル パスまたはフォルダ パスに関連付けます。

### タスク概要

NTFSセキュリティ形式のボリューム内に存在するファイルやフォルダ、またはmixedセキュリティ形式のボリューム上に存在するファイルやフォルダに対して、NTFSセキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、Discretionary Access Control List (DACL; 随意アクセス制御リスト)の4つのAccess Control Entry (ACE; アクセス制御エントリ)がそのセキュリティ記述子に追加されます。4つのデフォルトのACEは次のとおりです。

| 項目                      | アクセス<br>タイプ | 権限        | 権限の適用先             |
|-------------------------|-------------|-----------|--------------------|
| BUILTIN\Administrators  | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |
| BUILTIN\Users           | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |
| CREATOR OWNER           | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |
| NT AUTHORITY<br>\SYSTEM | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |

セキュリティ記述子を作成するときは、次の2つのパラメータを指定する必要があります。

| 必須パラメータ                  | 説明                                                     |
|--------------------------|--------------------------------------------------------|
| -vserver<br>vserver_name | <i>SVM</i> 名<br>セキュリティ記述子を適用するファイルやフォルダが格納されているSVMの名前。 |
| -ntfs-sd SD_name         | <i>セキュリティ記述子</i><br>セキュリティ記述子に割り当てる名前。                 |

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。



| オプションのパラメータ                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -owner name_or_SID             | <p><b>セキュリティ記述子の所有者</b></p> <p>セキュリティ記述子の所有者は、そのセキュリティ記述子が適用されるファイル(またはフォルダ)の権限を変更できます。また、そのセキュリティ記述子が適用されるオブジェクトの所有権を取得する権利を他のユーザに付与することもできます。このパラメータの値を指定するときは、次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>• SID</li> <li>• DOMAIN\ユーザ名</li> <li>• ユーザ名@DOMAIN</li> <li>• ユーザ名@FQDN</li> </ul> <p>3つの名前形式のいずれかを-ownerの値に指定する場合は、大文字と小文字が区別されないことに注意してください。</p> <p>-ownerパラメータの値はストレージレベルのアクセス保護では無視されます。</p>                      |
| -group name_or_SID             | <p><b>所有者のプライマリグループ</b></p> <p>セキュリティ記述子の所有者グループを指定します。所有者グループは、グループ名またはSIDを使用して指定できます。このパラメータの値を指定するときは、次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>• SID</li> <li>• DOMAIN\group-name</li> <li>• group-name@DOMAIN</li> <li>• group-name@FQDN</li> </ul> <p>3つの名前形式のいずれかを-groupの値に指定する場合は、大文字と小文字が区別されないことに注意してください。</p> <p>-groupパラメータの値はストレージレベルのアクセス保護では無視されます。</p> <p><b>注:</b> このパラメータを使用する前に、advanced権限レベルに変更する必要があります。</p> |
| -control-flags-raw Hex_integer | <p><b>raw制御フラグ</b></p> <p>セキュリティ記述子の制御フラグを指定します。</p> <p>-control-flags-rawパラメータの値はストレージレベルのアクセス保護では無視されます。</p> <p><b>注:</b> このパラメータを使用する前に、advanced権限レベルに変更する必要があります。</p>                                                                                                                                                                                                                                                                            |

#### 手順

1. 高度なパラメータを使用する場合は、権限レベルをadvancedに設定します。  

```
set -privilege advanced
```
2. セキュリティ記述子を作成します。



```
vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters
```

例

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner domain\joe
```

3. セキュリティ記述子の設定が正しいことを確認します。

```
vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name
```

例

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. advanced権限レベルになっている場合は、admin権限レベルに戻します。

```
set -privilege admin
```

### NTFSセキュリティ記述子へのNTFS DACLアクセス制御エントリの追加

NTFSセキュリティ記述子へのDACL(随意アクセス制御リスト)アクセス制御エントリ(ACE)の追加は、ファイルまたはフォルダに対するNTFS ACLの設定および適用における2番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、ACEで定義されているファイルまたはフォルダに対してオブジェクトが実行できる操作または実行できない操作が定義されます。

#### タスク概要

セキュリティ記述子のDACLには、1つまたは複数のACEを追加できます。

セキュリティ記述子に既存のACEを含むDACLが格納されている場合は、コマンドを実行すると、DACLに新しいACEが追加されます。セキュリティ記述子にDACLがない場合は、コマンドを実行するとDACLが作成され、そのDACLに新しいACEが追加されます。

DACLにACEを追加するときは、次の4つの必須パラメータの情報を指定する必要があります。

| 必須パラメータ                      | 説明                                                                                 |
|------------------------------|------------------------------------------------------------------------------------|
| -vserver<br>vserver_name     | <i>SVM名</i><br>セキュリティ記述子を適用するファイルやフォルダを含むStorage Virtual Machine(SVM、旧Vserver)の名前。 |
| -ntfs-sd SD_name             | <i>セキュリティ記述子</i><br>DACLエントリを追加するセキュリティ記述子の名前。                                     |
| -access-type<br>{deny allow} | <i>アクセス タイプ</i><br>随意ACEのアクセス制御タイプが許可か拒否かを指定します。                                   |

| 必須パラメータ                 | 説明                                                                                                                                                                                                                                                                                               |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -account<br>name_or_SID | <p>アカウント</p> <p>随意ACEを適用するアカウント。ユーザ名またはSIDを使用してアカウントを指定できます。このパラメータの値を指定するときは、次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>• SID</li> <li>• DOMAIN\ユーザ名</li> <li>• ユーザ名@DOMAIN</li> <li>• ユーザ名@FQDN</li> </ul> <p>3つの名前形式のいずれかを-accountの値に指定する場合は、大文字と小文字が区別されないことに注意してください。</p> |

必要に応じて、-accountパラメータで指定したアカウントに対して許可または拒否する権限を指定することで、DACLエントリをカスタマイズできます。権限を指定する場合、次の相互に排他的な3つの方法があります。

- 権限
- 詳細な権限
- raw権限 (advanced権限)

| オプションのrightsパラメータ                                                   | 説明                                   |
|---------------------------------------------------------------------|--------------------------------------|
| -rights {no-access full-control modify read-and-execute read write} | <p>権限</p> <p>選択できるパラメータ値は1つだけです。</p> |

| オプションのrightsパラメータ                                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-advanced-rights</code><br><code>advanced_access_right</code> | <p><i>詳細な権限</i></p> <p>次の詳細な権限の値のうち1つ以上をカンマで区切って指定できます。</p> <ul style="list-style-type: none"><li>• read-data</li><li>• write-data</li><li>• append-data</li><li>• read-ea</li><li>• write-ea</li><li>• execute-file</li><li>• delete-child</li><li>• read-attr</li><li>• write-attr</li><li>• delete</li><li>• read-perm</li><li>• write-perm</li><li>• write-owner</li><li>• full control</li></ul> |
| <code>-raw-rights</code><br><code>Hex_integer</code>                | <p><i>raw権限</i></p> <p>raw権限は16進整数で指定できます。advancedモードでのみ使用できます。</p> <p>注: これはadvanced権限レベルのパラメータです。このパラメータを使用するには、まず、<code>set -privilege advanced</code>コマンドによってadvanced権限レベルに変更する必要があります。</p>                                                                                                                                                                                                       |

注: DACLエントリの権限を指定しない場合、権限はデフォルトでフル コントロールに設定されます。

必要に応じて、継承の適用方法を指定することで、DACLエントリをカスタマイズできます。

| オプションのapply toパラメータ                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -apply-to {this-folder sub-folder files} | <p><i>DACLエントリの適用先</i></p> <p>1つ以上のパラメータ値をカンマで区切って指定できます。このパラメータを指定しない場合、このDACLエントリはデフォルトでこのフォルダ、サブフォルダ、およびファイルに適用されます。</p> <p>ストレージレベルのアクセス保護には、次の組み合わせの値の <i>-apply-to</i> パラメータが有効です。</p> <ul style="list-style-type: none"> <li>• this-folder, sub-folder, files</li> <li>• this-folder, sub-folder</li> <li>• ファイル</li> </ul> <p>注: ストレージレベルのアクセス保護タスクに関連付けるセキュリティ記述子のDACLを設定する際に、ストレージレベルのアクセス保護の <i>-apply-to</i> パラメータに無効な値を指定すると、関連付けられているすべてのストレージレベルのアクセス保護からDACLを関連付けるセキュリティ記述子が削除されます。</p> |

#### 手順

1. セキュリティ記述子にDACLエントリを追加します。

```
vserver security file-directory ntfs dacl add -vserver vserver_name -
ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID
optional_parameters
```

#### 例

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type
deny -account domain\joe -rights full-control -apply-to this-folder -
vserver vs1
```

2. DACLエントリが正しいことを確認します。

```
vserver security file-directory ntfs dacl show -vserver vserver_name -
ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID
```

#### 例

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
  Allow or Deny: deny
  Account Name or SID: DOMAIN\joe
  Access Rights: full-control
Advanced Access Rights: -
  Apply To: this-folder
  Access Rights: full-control
```

### セキュリティ ポリシーの作成

FlexVolを備えたStorage Virtual Machine(SVM)のセキュリティポリシーの作成は、ファイルまたはフォルダに対してACLを設定および適用する3番目のステップです。ポリシーは、さまざまなタスク

のコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加します。

タスク概要

セキュリティポリシーに追加するタスクには、NTFSセキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、NTFSセキュリティ形式またはmixedセキュリティ形式のボリュームを含むFlexVolを備えた各SVMに、ポリシーを関連付ける必要があります。このコマンドにはパラメータが2つしかなく、両方とも必須です。

| 必須パラメータ                     | 説明                                         |
|-----------------------------|--------------------------------------------|
| -vserver<br>vserver_name    | SVM名<br>ポリシーを関連付けるファイルやフォルダが格納されているSVMの名前。 |
| -policy-name<br>policy_name | policy_name<br>セキュリティポリシーの名前。              |

手順

1. セキュリティポリシーを作成します。
- vserver security file-directory policy create -vserver vserver\_name - policy-name policy\_name

例

```
vserver security file-directory policy create -policy-name policy1 -
vserver vs1
```

2. セキュリティポリシーを確認します。
- vserver security file-directory policy show

例

```
vserver security file-directory policy show
```

|         |             |
|---------|-------------|
| Vserver | Policy Name |
| -----   | -----       |
| vs1     | policy1     |

セキュリティポリシーへのタスクの追加

ACLを設定し、FlexVolを備えたStorage Virtual Machine(SVM)内のファイルやフォルダへ適用する4番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成する場合、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1つまたは複数のタスクエントリを追加できます。

タスク概要

セキュリティポリシーはタスクのコンテナです。タスクとは、NTFSまたはmixedセキュリティ形式(ストレージレベルのアクセス保護を設定している場合はボリュームオブジェクト)のファイルまたはフォルダへのセキュリティポリシーによって実行できる単一の操作を指します。タスクには次の2種類があります。

- ファイルとディレクトリのタスク  
指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用されるACLは、SMBクライアントまたはData ONTAP CLIで管理できます。

- ストレージレベルのアクセス保護タスク

指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用されるACLはData ONTAP CLIからのみ管理できます。

タスクには、ファイル(またはフォルダ)やファイル セット(またはフォルダ セット)のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1つのポリシー内の1つのパスに含められるのは1つのタスクだけです。ポリシーは、重複するタスク エントリを持つことはできません。

タスクをポリシーに追加する場合は、次の考慮事項について理解しておく必要があります。

- ポリシーあたりのタスク エントリは最大10,000個です。
- ポリシーには、1つまたは複数のタスクを含めることができます。  
ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。
- ストレージレベルのアクセス保護は、権限の制限に使用します。  
これによってアクセス権が追加されることはありません。

セキュリティ ポリシーにタスクを追加する際には、次の4つの必須パラメータを指定する必要があります。

| 必須パラメータ                     | 説明                                                                                                                                                                                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -vserver<br>vserver_name    | <i>SVM名</i><br>セキュリティ記述子を適用するパスが含まれているSVMの名前。                                                                                                                                                                                                                           |
| -policy-name<br>policy_name | <i>ポリシー名</i><br>タスクを追加するセキュリティ ポリシーの名前。                                                                                                                                                                                                                                 |
| -path path                  | <i>パス</i><br>このタスクに関連付けられたセキュリティ記述子を適用するパス。                                                                                                                                                                                                                             |
| -ntfs-sd<br>SD_name         | <i>セキュリティ記述子</i><br>タスク内のパスに関連付けるセキュリティ記述子の名前。<br>これは必須パラメータであるため、タスクを作成する前に、セキュリティ記述子を作成してDACLのACE(アクセス制御エントリ)とSACLのACE(必要な場合)に追加してから、タスク内のファイルまたはフォルダのパスにセキュリティ記述子に関連付け、さらに最終的にセキュリティ ポリシーにタスクを追加することをお勧めします。<br>セキュリティ記述子には、複数のACE(DACLのACEとSACLのACEの両方)を含めることができます。 |

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

| オプションのパラメータ                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -security-type<br>{ntfs nfsv4}           | <p><b>セキュリティ タイプ</b></p> <p>このタスクに関連付けられたセキュリティ記述子が、NTFSまたはNFSv4のいずれのタイプのセキュリティ記述子であるかを示します。このオプションパラメータを指定しない場合、デフォルトはntfsです。</p> <p><b>注:</b> nfsv4のタイプは、このリリースではサポートされていません。このオプションのパラメータを指定する場合は、ntfsを-security-typeパラメータに指定する必要があります。</p>                                                                                                                                                                                                                                                                                                                                                                                                            |
| -ntfs-mode<br>{propagate ignore replace} | <p><b>プロパゲーション モード</b></p> <p>子のサブフォルダとファイルにセキュリティ設定を伝播する方法を指定します。この設定では、親フォルダに含まれている子のファイルとフォルダがアクセス制御と監査情報を親フォルダから継承する方法を選択します。3つのパラメータが、それぞれ次の3つのプロパゲーション モードのタイプに対応します。</p> <p><b>Propagate</b></p> <p>継承可能な権限をすべてのサブフォルダおよびファイルに伝播します。既存の権限は置換されません。</p> <p><b>Replace</b></p> <p>すべてのサブフォルダおよびファイルに対する既存の権限を、継承可能な権限に置換します。</p> <p><b>Ignore</b></p> <p>このファイルまたはフォルダの権限の置換を許可しません。</p> <p>このパラメータの値を指定しない場合、デフォルト値はpropagateです。ストレージレベルのアクセス保護セキュリティ設定はボリューム内のすべてのファイルとフォルダに自動的に伝播するため、タスクがストレージレベルのアクセス保護タスクである場合、この設定は無視されます。</p> <p><b>注:</b> ボリュームがボリューム ジャンクション パス以下にマウントされており、そのパスにストレージレベルのアクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。</p> |
| -index-number<br>integer                 | <p><b>インデックス位置</b></p> <p>タスクのインデックス番号を指定します。タスクは、順番に適用されます。大きいインデックス番号を持つタスクは、インデックス番号の小さいタスクの後に適用されます。このオプション パラメータを指定しない場合、新しいタスクはインデックス リストの最後に適用されます。</p> <p>サポートされる値の範囲は1～ 9999です。既存の一番大きいインデックス番号とこのパラメータに指定した値の間がとんでいる場合、この番号のタスクがポリシーの最後のタスクであると見なされ、以前の一番大きいインデックス番号に1を加えたインデックス番号が付けられます。</p> <p><b>注:</b> 既存のタスクにすでに割り当てられているインデックス番号を指定した場合、タスクにはそのインデックス番号が追加され、既存のタスクのインデックス番号は、自動的にテーブル内の次の番号に変更されます。</p>                                                                                                                                                                                                                                 |

| オプションのパラメータ                                        | 説明                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-access-control {file-directory slag}</code> | <p><b>アクセス制御の種類</b></p> <p>タスクのアクセス制御の種類を指定します。</p> <p>デフォルト値はfile-directoryです。</p> <p>ストレージレベルのアクセス保護タスクを追加する場合は、アクセス制御の種類としてslagを指定する必要があります。</p> <p>この値がslagに設定されると、タスクに指定されたセキュリティ記述子が、-pathパラメータで指定されたボリュームに適用されます。それ以外の場合は、セキュリティ記述子は指定されたパスのファイルとディレクトリに適用されます。</p> |

### 手順

1. セキュリティ ポリシーに関連付けられたセキュリティ記述子を含むタスクを追加します。

```
vserver security file-directory policy-task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_name optional_parameters
```

file-directoryは、-access-controlパラメータのデフォルト値です。ファイルとディレクトリのアクセス タスクを設定する場合、アクセス制御の種類の指定はオプションです。

### 例

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. ポリシー タスクの設定を確認します。

```
vserver security file-directory policy-task show -vserver vserver_name -policy-name policy_name -path path
```

### 例

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

| Index | File/Folder Path | Access Control | Security Type | NTFS Mode | NTFS Security Descriptor Name |
|-------|------------------|----------------|---------------|-----------|-------------------------------|
| 1     | /home/dir1       | file-directory | ntfs          | propagate | sd2                           |

## セキュリティ ポリシーの適用

FlexVolを備えたStorage Virtual Machine (SVM) へのセキュリティ ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

### タスク概要

セキュリティ ポリシーに定義されているセキュリティ設定を、FlexVol (NTFSまたはmixedセキュリティ形式) 内のNTFSファイルおよびフォルダに適用できます。



| 必須パラメータ                     | 説明                                                    |
|-----------------------------|-------------------------------------------------------|
| -vserver<br>vserver_name    | <i>SVM</i><br>関連タスクでポリシーを適用するファイルやフォルダが格納されているSVMの名前。 |
| -policy-name<br>policy_name | <i>Policy_name</i><br>適用するセキュリティ ポリシーの名前。             |

#### 手順

1. セキュリティ ポリシーを適用します。

```
vserver security file-directory policy apply -vserver vserver_name
-policy-name policy_name
```

#### 例

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシーの適用ジョブがスケジュールされます。

### セキュリティ ポリシー ジョブの監視

FlexVolを備えたStorage Virtual Machine(SVM)にセキュリティ ポリシーを適用する場合、セキュリティ ポリシー ジョブをモニタして、ポリシー適用のタスクの進行状況を監視できます。セキュリティ ポリシーの適用が正常に完了したかどうかを確認する上で、この機能が役に立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この機能は有用です。

#### タスク概要

セキュリティ ポリシー ジョブの詳細情報を表示するには、-instanceパラメータを使用します。

#### 手順

1. 次のコマンドを実行し、セキュリティ ポリシー ジョブを監視します。

```
vserver security file-directory job show -vserver vserver_name
```

#### 例

```
vserver security file-directory job show -vserver vs1
```

| Job ID                                         | Name            | Vserver | Node  | State   |
|------------------------------------------------|-----------------|---------|-------|---------|
| 53322                                          | Fsecurity Apply | vs1     | node1 | Success |
| Description: File Directory Security Apply Job |                 |         |       |         |

### 適用したファイル セキュリティの監視

FlexVolを備えたStorage Virtual Machine(SVM)のファイルやフォルダにセキュリティ ポリシーを適用した場合に、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

#### タスク概要

データが格納されているSVMの名前、およびセキュリティ設定を確認するファイルとフォルダのパスを指定する必要があります。オプションの-expand-maskパラメータを使用すると、セキュリティ設定に関する詳細な情報を表示できます。

## 手順

1. ファイルとフォルダのセキュリティ設定を表示します。

```
vserver security file-directory show -vserver vserver_name -path path [-  
expand-mask true]
```

## 例

```
vserver security file-directory show -vserver vs1 -path /data/  
engineering -expand-mask true
```

```
Vserver: vs1
  File Path: /data/engineering
  File Inode Number: 5544
  Security Style: ntfs
  Effective Style: ntfs
  DOS Attributes: 10
  DOS Attributes in Text: ---D---
  Expanded Dos Attributes: 0x10
    ...0 ... .. = Offline
    ... ..0 ... .. = Sparse
    ... ..0 ... .. = Normal
    ... ..0 ... .. = Archive
    ... ..1 ... .. = Directory
    ... ..0 ... .. = System
    ... ..0 ... .. = Hidden
    ... ..0 ... .. = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
  ACLs: NTFS Security Descriptor
        Control:0x8004

        1... .. = Self Relative
        ..0... .. = RM Control Valid
        ..0... .. = SACL Protected
        ...0... .. = DACL Protected
        ... 0... .. = SACL Inherited
        ... ..0... .. = DACL Inherited
        ... ..0... .. = SACL Inherit Required
        ... ..0... .. = DACL Inherit Required
        ... ..0... .. = SACL Defaulted
        ... ..0... .. = SACL Present
        ... ..0... .. = DACL Defaulted
        ... ..1... .. = DACL Present
        ... ..0... .. = Group Defaulted
        ... ..0... .. = Owner Defaulted

Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
DACL - ACES
  ALLOW-Everyone-0x1f01ff
    0... .. = Generic Read
    ..0... .. = Generic Write
    ...0... .. = Generic Execute
    ...0... .. = Generic All
    ... ..0... .. = System Security
    ... ..1... .. = Synchronize
    ... ..1... .. = Write Owner
    ... ..1... .. = Write DAC
    ... ..1... .. = Read Control
    ... ..1... .. = Delete
    ... ..1... .. = Write Attributes
    ... ..1... .. = Read Attributes
    ... ..1... .. = Delete Child
    ... ..1... .. = Execute
    ... ..1... .. = Write EA
    ... ..1... .. = Read EA
    ... ..1... .. = Append
    ... ..1... .. = Write
    ... ..1... .. = Read

  ALLOW-Everyone-0x10000000-0I|CI|IO
    0... .. = Generic Read
    ..0... .. = Generic Write
    ...0... .. = Generic Execute
    ...1... .. = Generic All
    ... ..0... .. = System Security
    ... ..0... .. = Synchronize
    ... ..0... .. = Write Owner
    ... ..0... .. = Write DAC
    ... ..0... .. = Read Control
    ... ..0... .. = Delete
    ... ..0... .. = Write Attributes
    ... ..0... .. = Read Attributes
```

```

.....0... = Delete Child
.....0... = Execute
.....0... = Write EA
.....0... = Read EA
.....0... = Append
.....0... = Write
.....0... = Read

```

## CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用

Data ONTAP CLIを使用してNTFSファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、NTFSセキュリティ記述子を作成し、SACLをセキュリティ記述子に追加します。次に、セキュリティ ポリシーを作成してポリシー タスクを追加します。その後、FlexVolを備えたStorage Virtual Machine(SVM)にセキュリティ ポリシーを適用します。

### タスク概要

セキュリティ ポリシーを適用したら、セキュリティ ポリシー ジョブを監視して、適用した監査ポリシーの設定を確認することができます。

### 手順

#### 1. NTFSセキュリティ記述子の作成 (276ページ)

NTFSセキュリティ記述子の作成は、FlexVolを備えたStorage Virtual Machine(SVM)内に存在するファイルやフォルダのNTFS Access Control List(ACL;アクセス制御リスト)を設定および適用するための最初のステップです。このセキュリティ記述子をポリシー タスクでファイル パスまたはフォルダ パスに関連付けます。

#### 2. NTFSセキュリティ記述子へのNTFS SACLアクセス制御エントリの追加 (278ページ)

NTFSセキュリティ記述子へのSACL(システム アクセス制御リスト)アクセス制御エントリ(ACE)の追加は、FlexVolを備えたStorage Virtual Machine(SVM)のファイルやフォルダに対するNTFS監査ポリシーを作成する2番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。また、成功したアクセス試行と失敗したアクセス試行のどちらを監査対象にするかを定義します。

#### 3. セキュリティ ポリシーの作成 (281ページ)

FlexVolを備えたStorage Virtual Machine(SVM)のセキュリティ ポリシーの作成は、ファイルまたはフォルダに対してACLを設定および適用する3番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティ ポリシーにタスクを追加します。

#### 4. セキュリティ ポリシーへのタスクの追加 (282ページ)

ACLを設定し、FlexVolを備えたStorage Virtual Machine(SVM)内のファイルやフォルダへ適用する4番目のステップでは、ポリシー タスクを作成してセキュリティ ポリシーに追加します。ポリシー タスクを作成する場合、セキュリティ ポリシーとタスクを関連付けます。セキュリティ ポリシーには、1つまたは複数のタスク エントリを追加できます。

#### 5. セキュリティ ポリシーの適用 (285ページ)

FlexVolを備えたStorage Virtual Machine(SVM)へのセキュリティ ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

#### 6. セキュリティ ポリシー ジョブの監視 (286ページ)

FlexVolを備えたStorage Virtual Machine(SVM)にセキュリティ ポリシーを適用する場合、セキュリティ ポリシー ジョブをモニタして、ポリシー適用のタスクの進行状況を監視できます。セキュリティ ポリシーの適用が正常に完了したかどうかを確認する上で、この機能が役に立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この機能は有用です。

#### 7. 適用した監査ポリシーの監視 (286ページ)

FlexVolを備えたStorage Virtual Machine(SVM)のファイルやフォルダにセキュリティ ポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりにになっているかを確認するには、監査ポリシーを確認します。

**関連コンセプト**

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#)(154ページ)  
[CLIを使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項](#)(258ページ)  
[セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法](#)(259ページ)

**関連タスク**

[Windowsの\[セキュリティ\]タブを使用したNTFS監査ポリシーの設定](#)(451ページ)  
[Windowsの\[セキュリティ\]タブを使用した監査ポリシーに関する情報の表示](#)(455ページ)  
[CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示](#)(457ページ)  
[CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用](#)(261ページ)

**NTFSセキュリティ記述子の作成**

NTFSセキュリティ記述子の作成は、FlexVolを備えたStorage Virtual Machine(SVM)内に存在するファイルやフォルダのNTFS Access Control List(ACL;アクセス制御リスト)を設定および適用するための最初のステップです。このセキュリティ記述子をポリシー タスクでファイル パスまたはフォルダ パスに関連付けます。

**タスク概要**

NTFSセキュリティ形式のボリューム内に存在するファイルやフォルダ、またはmixedセキュリティ形式のボリューム上に存在するファイルやフォルダに対して、NTFSセキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、Discretionary Access Control List(DACL;随意アクセス制御リスト)の4つのAccess Control Entry(ACE;アクセス制御エントリ)がそのセキュリティ記述子に追加されます。4つのデフォルトのACEは次のとおりです。

| 項目                      | アクセス<br>タイプ | 権限        | 権限の適用先             |
|-------------------------|-------------|-----------|--------------------|
| BUILTIN\Administrators  | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |
| BUILTIN\Users           | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |
| CREATOR OWNER           | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |
| NT AUTHORITY<br>\SYSTEM | 許可          | フル コントロール | このフォルダ、サブフォルダ、ファイル |

セキュリティ記述子を作成するときは、次の2つのパラメータを指定する必要があります。

| 必須パラメータ                  | 説明                                                    |
|--------------------------|-------------------------------------------------------|
| -vserver<br>vserver_name | <i>SVM名</i><br>セキュリティ記述子を適用するファイルやフォルダが格納されているSVMの名前。 |
| -ntfs-sd SD_name         | <i>セキュリティ記述子</i><br>セキュリティ記述子に割り当てる名前。                |

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

| オプションのパラメータ                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -owner name_or_SID             | <p><b>セキュリティ記述子の所有者</b></p> <p>セキュリティ記述子の所有者は、そのセキュリティ記述子が適用されるファイル(またはフォルダ)の権限を変更できます。また、そのセキュリティ記述子が適用されるオブジェクトの所有権を取得する権利を他のユーザに付与することもできます。このパラメータの値を指定するときは、次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>• SID</li> <li>• DOMAIN\ユーザ名</li> <li>• ユーザ名@DOMAIN</li> <li>• ユーザ名@FQDN</li> </ul> <p>3つの名前形式のいずれかを-ownerの値に指定する場合は、大文字と小文字が区別されないことに注意してください。</p> <p>-ownerパラメータの値はストレージレベルのアクセス保護では無視されます。</p>                      |
| -group name_or_SID             | <p><b>所有者のプライマリグループ</b></p> <p>セキュリティ記述子の所有者グループを指定します。所有者グループは、グループ名またはSIDを使用して指定できます。このパラメータの値を指定するときは、次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>• SID</li> <li>• DOMAIN\group-name</li> <li>• group-name@DOMAIN</li> <li>• group-name@FQDN</li> </ul> <p>3つの名前形式のいずれかを-groupの値に指定する場合は、大文字と小文字が区別されないことに注意してください。</p> <p>-groupパラメータの値はストレージレベルのアクセス保護では無視されます。</p> <p><b>注:</b> このパラメータを使用する前に、advanced権限レベルに変更する必要があります。</p> |
| -control-flags-raw Hex_integer | <p><b>raw制御フラグ</b></p> <p>セキュリティ記述子の制御フラグを指定します。</p> <p>-control-flags-rawパラメータの値はストレージレベルのアクセス保護では無視されます。</p> <p><b>注:</b> このパラメータを使用する前に、advanced権限レベルに変更する必要があります。</p>                                                                                                                                                                                                                                                                            |

## 手順

1. 高度なパラメータを使用する場合は、権限レベルをadvancedに設定します。  

```
set -privilege advanced
```
2. セキュリティ記述子を作成します。

```
vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters
```

**例**

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner domain\joe
```

3. セキュリティ記述子の設定が正しいことを確認します。

```
vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name
```

**例**

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. advanced権限レベルになっている場合は、admin権限レベルに戻します。

```
set -privilege admin
```

**NTFSセキュリティ記述子へのNTFS SACLアクセス制御エントリの追加**

NTFSセキュリティ記述子へのSACL(システム アクセス制御リスト)アクセス制御エントリ(ACE)の追加は、FlexVolを備えたStorage Virtual Machine(SVM)のファイルやフォルダに対するNTFS監査ポリシーを作成する2番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。また、成功したアクセス試行と失敗したアクセス試行のどちらを監査対象にするかを定義します。

**タスク概要**

セキュリティ記述子のSACLには、1つまたは複数のACEを追加できます。

セキュリティ記述子に含まれているSACLに既存のACEがある場合は、新しいACEがSACLに追加されます。セキュリティ記述子にSACLが含まれていない場合は、SACLが作成され、そのSACLに新しいACEが追加されます。

ACEをSACLに追加するときは、次の4つの必須パラメータに対する情報を指定する必要があります。

| 必須パラメータ                           | 説明                                                                     |
|-----------------------------------|------------------------------------------------------------------------|
| -vserver<br>vserver_name          | <i>SVM名</i><br>セキュリティ記述子を適用するファイルやフォルダが格納されているSVMの名前。                  |
| -ntfs-sd SD_name                  | <i>セキュリティ記述子</i><br>SACLエントリを追加するセキュリティ記述子の名前。                         |
| -access-type<br>{failure success} | <i>アクセス タイプ</i><br>システムACEの監査タイプを <i>成功</i> にするか <i>失敗</i> にするかを指定します。 |

| 必須パラメータ                 | 説明                                                                                                                                                                                                                                                                                                 |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -account<br>name_or_SID | <p>アカウント</p> <p>システムACEを適用するアカウント。アカウントはユーザ名またはSIDを使用して指定できます。このパラメータの値を指定するときは、次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>• SID</li> <li>• DOMAIN\ユーザ名</li> <li>• ユーザ名@DOMAIN</li> <li>• ユーザ名@FQDN</li> </ul> <p>3つの名前形式のいずれかを-accountの値に指定する場合は、大文字と小文字が区別されないことに注意してください。</p> |

-accountパラメータで指定したアカウントの成功イベントまたは失敗イベントについて監査する権限を指定することで、SACLエントリを設定できます。権限を指定する場合、次の相互に排他的な3つの方法があります。

- 権限
- 詳細な権限
- raw権限 (advanced権限)

イベントを監査するには、3つの権限パラメータのいずれかを設定します。

| オプションのrights<br>パラメータ                                               | 説明                                   |
|---------------------------------------------------------------------|--------------------------------------|
| -rights {no-access full-control modify read-and-execute read write} | <p>権限</p> <p>選択できるパラメータ値は1つだけです。</p> |

| オプションのrights<br>パラメータ                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -advanced-rights<br><i>advanced_access_right</i> | <p><b>詳細な権限</b><br/>次の詳細な権限の値のうち1つ以上をカンマで区切って指定できます。</p> <ul style="list-style-type: none"> <li>• read-data</li> <li>• write-data</li> <li>• append-data</li> <li>• read-ea</li> <li>• write-ea</li> <li>• execute-file</li> <li>• delete-child</li> <li>• read-attr</li> <li>• write-attr</li> <li>• delete</li> <li>• read-perm</li> <li>• write-perm</li> <li>• write-owner</li> <li>• full control</li> </ul> |
| -raw-rights<br><i>Hex_integer</i>                | <p><b>raw権限</b><br/>raw権限は16進整数で指定できます。advancedモードでのみ使用できます。</p> <p>注: これはadvanced権限レベルのパラメータです。このパラメータを使用するには、まず、次のコマンドによってadvanced権限レベルに変更する必要があります。</p> <p><b>set -privilege advanced</b></p>                                                                                                                                                                                                                  |

注: SACLエントリの権限を指定しない場合、デフォルト設定のFull Controlになります。

必要に応じて、apply toパラメータで継承を適用する方法を指定することで、SACLエントリをカスタマイズすることもできます。このパラメータを指定しない場合は、デフォルトで、このSACLエントリがこのフォルダ、サブフォルダ、およびファイルに適用されます。



| オプションのapply toパラメータ                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -apply-to {this-folder sub-folder files} | <p><i>SACLエントリの適用先</i></p> <p>1つ以上のパラメータ値をカンマで区切って指定できます。</p> <p>ストレージレベルのアクセス保護には、次の組み合わせの値の -apply-toパラメータが有効です。</p> <ul style="list-style-type: none"> <li>• this-folder, sub-folder, files</li> <li>• this-folder, sub-folder</li> <li>• ファイル</li> </ul> <p>注: ストレージレベルのアクセス保護タスクに関連付けるセキュリティ記述子のSACLを設定する際に、ストレージレベルのアクセス保護の -apply-toパラメータに無効な値を指定すると、関連付けられているすべてのストレージレベルのアクセス保護からSACLを関連付けるセキュリティ記述子が削除されます。</p> |

#### 手順

1. SAclエントリをセキュリティ記述子に追加します。

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID optional_parameters
```

#### 例

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. SAclエントリが正しいことを確認します。

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID
```

#### 例

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

### セキュリティ ポリシーの作成

FlexVolを備えたStorage Virtual Machine(SVM)のセキュリティポリシーの作成は、ファイルまたはフォルダに対してACLを設定および適用する3番目のステップです。ポリシーは、さまざまなタスク

のコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加します。

#### タスク概要

セキュリティポリシーに追加するタスクには、NTFSセキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、NTFSセキュリティ形式またはmixedセキュリティ形式のボリュームを含むFlexVolを備えた各SVMに、ポリシーを関連付ける必要があります。

このコマンドにはパラメータが2つしかなく、両方とも必須です。

| 必須パラメータ                            | 説明                                                |
|------------------------------------|---------------------------------------------------|
| -vserver<br><i>vserver_name</i>    | <i>SVM名</i><br>ポリシーを関連付けるファイルやフォルダが格納されているSVMの名前。 |
| -policy-name<br><i>policy_name</i> | <i>policy_name</i><br>セキュリティポリシーの名前。              |

#### 手順

1. セキュリティポリシーを作成します。

```
vserver security file-directory policy create -vserver vserver_name -
policy-name policy_name
```

##### 例

```
vserver security file-directory policy create -policy-name policy1 -
vserver vs1
```

2. セキュリティポリシーを確認します。

```
vserver security file-directory policy show
```

##### 例

```
vserver security file-directory policy show
```

| Vserver | Policy Name |
|---------|-------------|
| -----   | -----       |
| vs1     | policy1     |

### セキュリティポリシーへのタスクの追加

ACLを設定し、FlexVolを備えたStorage Virtual Machine(SVM)内のファイルやフォルダへ適用する4番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成する場合、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1つまたは複数のタスクエントリを追加できます。

#### タスク概要

セキュリティポリシーはタスクのコンテナです。タスクとは、NTFSまたはmixedセキュリティ形式(ストレージレベルのアクセス保護を設定している場合はボリュームオブジェクト)のファイルまたはフォルダへのセキュリティポリシーによって実行できる単一の操作を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用されるACLは、SMBクライアントまたはData ONTAP CLIで管理できます。

- ストレージレベルのアクセス保護タスク

指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用されるACLはData ONTAP CLIからのみ管理できます。

タスクには、ファイル(またはフォルダ)やファイル セット(またはフォルダ セット)のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1つのポリシー内の1つのパスに含められるのは1つのタスクだけです。ポリシーは、重複するタスク エントリを持つことはできません。

タスクをポリシーに追加する場合は、次の考慮事項について理解しておく必要があります。

- ポリシーあたりのタスク エントリは最大10,000個です。
- ポリシーには、1つまたは複数のタスクを含めることができます。  
ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。
- ストレージレベルのアクセス保護は、権限の制限に使用します。  
これによってアクセス権が追加されることはありません。

セキュリティ ポリシーにタスクを追加する際には、次の4つの必須パラメータを指定する必要があります。

| 必須パラメータ                     | 説明                                                                                                                                                                                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -vserver<br>vserver_name    | <i>SVM名</i><br>セキュリティ記述子を適用するパスが含まれているSVMの名前。                                                                                                                                                                                                                           |
| -policy-name<br>policy_name | <i>ポリシー名</i><br>タスクを追加するセキュリティ ポリシーの名前。                                                                                                                                                                                                                                 |
| -path path                  | <i>パス</i><br>このタスクに関連付けられたセキュリティ記述子を適用するパス。                                                                                                                                                                                                                             |
| -ntfs-sd<br>SD_name         | <i>セキュリティ記述子</i><br>タスク内のパスに関連付けるセキュリティ記述子の名前。<br>これは必須パラメータであるため、タスクを作成する前に、セキュリティ記述子を作成してDACLのACE(アクセス制御エントリ)とSACLのACE(必要な場合)に追加してから、タスク内のファイルまたはフォルダのパスにセキュリティ記述子に関連付け、さらに最終的にセキュリティ ポリシーにタスクを追加することをお勧めします。<br>セキュリティ記述子には、複数のACE(DACLのACEとSACLのACEの両方)を含めることができます。 |

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

| オプションのパラメータ                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -security-type<br>{ntfs nfsv4}           | <p><b>セキュリティ タイプ</b></p> <p>このタスクに関連付けられたセキュリティ記述子が、NTFSまたはNFSv4のいずれのタイプのセキュリティ記述子であるかを示します。このオプションパラメータを指定しない場合、デフォルトはntfsです。</p> <p><b>注:</b> nfsv4のタイプは、このリリースではサポートされていません。このオプションのパラメータを指定する場合は、ntfsを-security-typeパラメータに指定する必要があります。</p>                                                                                                                                                                                                                                                                                                                                                                                                            |
| -ntfs-mode<br>{propagate ignore replace} | <p><b>プロパゲーション モード</b></p> <p>子のサブフォルダとファイルにセキュリティ設定を伝播する方法を指定します。この設定では、親フォルダに含まれている子のファイルとフォルダがアクセス制御と監査情報を親フォルダから継承する方法を選択します。3つのパラメータが、それぞれ次の3つのプロパゲーション モードのタイプに対応します。</p> <p><b>Propagate</b></p> <p>継承可能な権限をすべてのサブフォルダおよびファイルに伝播します。既存の権限は置換されません。</p> <p><b>Replace</b></p> <p>すべてのサブフォルダおよびファイルに対する既存の権限を、継承可能な権限に置換します。</p> <p><b>Ignore</b></p> <p>このファイルまたはフォルダの権限の置換を許可しません。</p> <p>このパラメータの値を指定しない場合、デフォルト値はpropagateです。ストレージレベルのアクセス保護セキュリティ設定はボリューム内のすべてのファイルとフォルダに自動的に伝播するため、タスクがストレージレベルのアクセス保護タスクである場合、この設定は無視されます。</p> <p><b>注:</b> ボリュームがボリューム ジャンクション パス以下にマウントされており、そのパスにストレージレベルのアクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。</p> |
| -index-number<br>integer                 | <p><b>インデックス位置</b></p> <p>タスクのインデックス番号を指定します。タスクは、順番に適用されます。大きいインデックス番号を持つタスクは、インデックス番号の小さいタスクの後に適用されます。このオプション パラメータを指定しない場合、新しいタスクはインデックス リストの最後に適用されます。</p> <p>サポートされる値の範囲は1～ 9999です。既存の一番大きいインデックス番号とこのパラメータに指定した値の間がとんでいる場合、この番号のタスクがポリシーの最後のタスクであると見なされ、以前の一番大きいインデックス番号に1を加えたインデックス番号が付けられます。</p> <p><b>注:</b> 既存のタスクにすでに割り当てられているインデックス番号を指定した場合、タスクにはそのインデックス番号が追加され、既存のタスクのインデックス番号は、自動的にテーブル内の次の番号に変更されます。</p>                                                                                                                                                                                                                                 |

| オプションのパラメータ                           | 説明                                                                                                                                                                                                                                                                         |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -access-control {file-directory slag} | <p><b>アクセス制御の種類</b></p> <p>タスクのアクセス制御の種類を指定します。</p> <p>デフォルト値はfile-directoryです。</p> <p>ストレージレベルのアクセス保護タスクを追加する場合は、アクセス制御の種類としてslagを指定する必要があります。</p> <p>この値がslagに設定されると、タスクに指定されたセキュリティ記述子が、-pathパラメータで指定されたボリュームに適用されます。それ以外の場合は、セキュリティ記述子は指定されたパスのファイルとディレクトリに適用されます。</p> |

### 手順

1. セキュリティ ポリシーに関連付けられたセキュリティ記述子を含むタスクを追加します。

```
vserver security file-directory policy-task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_name optional_parameters
```

file-directoryは、-access-controlパラメータのデフォルト値です。ファイルとディレクトリのアクセス タスクを設定する場合、アクセス制御の種類の指定はオプションです。

#### 例

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. ポリシー タスクの設定を確認します。

```
vserver security file-directory policy-task show -vserver vserver_name -policy-name policy_name -path path
```

#### 例

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

| Index | File/Folder Path | Access Control | Security Type | NTFS Mode | NTFS Security Descriptor Name |
|-------|------------------|----------------|---------------|-----------|-------------------------------|
| 1     | /home/dir1       | file-directory | ntfs          | propagate | sd2                           |

## セキュリティ ポリシーの適用

FlexVolを備えたStorage Virtual Machine (SVM) へのセキュリティ ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

### タスク概要

セキュリティ ポリシーに定義されているセキュリティ設定を、FlexVol (NTFSまたはmixedセキュリティ形式) 内のNTFSファイルおよびフォルダに適用できます。

| 必須パラメータ                     | 説明                                                    |
|-----------------------------|-------------------------------------------------------|
| -vserver<br>vserver_name    | <i>SVM</i><br>関連タスクでポリシーを適用するファイルやフォルダが格納されているSVMの名前。 |
| -policy-name<br>policy_name | <i>Policy_name</i><br>適用するセキュリティ ポリシーの名前。             |

#### 手順

1. セキュリティ ポリシーを適用します。

```
vserver security file-directory policy apply -vserver vserver_name
-policy-name policy_name
```

#### 例

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシーの適用ジョブがスケジュールされます。

### セキュリティ ポリシー ジョブの監視

FlexVolを備えたStorage Virtual Machine(SVM)にセキュリティ ポリシーを適用する場合、セキュリティ ポリシー ジョブをモニタして、ポリシー適用のタスクの進行状況を監視できます。セキュリティ ポリシーの適用が正常に完了したかどうかを確認する上で、この機能が役に立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この機能は有用です。

#### タスク概要

セキュリティ ポリシー ジョブの詳細情報を表示するには、-instanceパラメータを使用します。

#### 手順

1. 次のコマンドを実行し、セキュリティ ポリシー ジョブを監視します。

```
vserver security file-directory job show -vserver vserver_name
```

#### 例

```
vserver security file-directory job show -vserver vs1
```

| Job ID                                         | Name            | Vserver | Node  | State   |
|------------------------------------------------|-----------------|---------|-------|---------|
| 53322                                          | Fsecurity Apply | vs1     | node1 | Success |
| Description: File Directory Security Apply Job |                 |         |       |         |

### 適用した監査ポリシーの監視

FlexVolを備えたStorage Virtual Machine(SVM)のファイルやフォルダにセキュリティ ポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりになっているかを確認するには、監査ポリシーを確認します。

#### タスク概要

監査ポリシーの情報を表示するには、vserver security file-directory showコマンドを使用します。データが格納されているSVMの名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

**手順**

1. 監査ポリシーの設定を表示します。

```
vserver security file-directory show -vserver vserver_name -path path
```

**例**

次に、SVM vs1のパス「/corp」に適用される監査ポリシーの情報を表示するコマンドの例を示します。このパスには、SUCCESSとSUCCESS/FAIL SACLの両方のエントリが適用されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /
corp

          Vserver: vs1
          File Path: /corp
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
                Control:0x8014
                Owner:DOMAIN\Administrator
                Group:BUILTIN\Administrators
                SACL - ACES
                ALL-DOMAIN\Administrator-0x100081-0I|CI|
SA|FA                SUCCESSFUL-DOMAIN\user1-0x100116-0I|CI|SA
                DACL - ACES
                ALLOW-BUILTIN\Administrators-0x1f01ff-0I|
CI                ALLOW-BUILTIN\Users-0x1f01ff-0I|CI
                ALLOW-CREATOR OWNER-0x1f01ff-0I|CI
                ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-0I|CI
```

**セキュリティ ポリシー ジョブの管理の考慮事項**

セキュリティ ポリシー ジョブが存在する場合、特定の状況下でセキュリティ ポリシーやポリシーに割り当てられたタスクを変更できなくなります。セキュリティ ポリシーの変更が確実に成功するように、ポリシーを変更できる条件やできない条件を理解しておく必要があります。ポリシーの変更には、ポリシーに割り当てられたタスクの追加、削除、変更と、ポリシーの削除または変更が含まれます。

セキュリティ ポリシーにジョブが存在し、そのジョブが次の状態である場合、そのポリシーやポリシーに割り当てられたタスクは変更できません。

- ジョブが実行中または進行中の場合
- ジョブが一時停止中の場合
- ジョブが再開され、実行中の場合
- ジョブが別のノードへのフェイルオーバーを待機中の場合

セキュリティ ポリシーにジョブが存在する場合、次の状況下では、ポリシーやポリシーに関連付けられたタスクの変更は成功します。

- ポリシー ジョブが停止中の場合

- ポリシー ジョブの実行が成功した場合

## NTFSセキュリティ記述子の管理用コマンド

セキュリティ記述子を管理するための特別なData ONTAPコマンドがあります。セキュリティ記述子に関する情報を作成、削除、および表示できます。

| 状況                          | 使用するコマンド                                                 |
|-----------------------------|----------------------------------------------------------|
| NTFSセキュリティ記述子を作成する          | <code>vserver security file-directory ntfs create</code> |
| 既存のNTFSセキュリティ記述子を変更する       | <code>vserver security file-directory ntfs modify</code> |
| 既存のNTFSセキュリティ記述子に関する情報を表示する | <code>vserver security file-directory ntfs show</code>   |
| NTFSセキュリティ記述子を削除する          | <code>vserver security file-directory ntfs delete</code> |

詳細については、`vserver security file-directory ntfs`コマンドのマニュアル ページを参照してください。

## NTFS DACLアクセス制御エントリの管理用コマンド

DACLのアクセス制御エントリ(ACE)を管理するための、特定のData ONTAPコマンドが存在します。ACEはいつでもNTFS DACLに追加できます。また、NTFS DACLのACEに関する情報を変更、削除、表示するなどで、既存のDACLを管理できます。

| 状況                        | 使用するコマンド                                                      |
|---------------------------|---------------------------------------------------------------|
| ACEの作成およびNTFS DACLへの追加    | <code>vserver security file-directory ntfs dacl add</code>    |
| NTFS DACLの既存のACEの変更       | <code>vserver security file-directory ntfs dacl modify</code> |
| NTFS DACLの既存のACEに関する情報の表示 | <code>vserver security file-directory ntfs dacl show</code>   |
| NTFS DACLからの既存のACEの削除     | <code>vserver security file-directory ntfs dacl remove</code> |

詳細については、`vserver security file-directory ntfs dacl`コマンドのマニュアル ページを参照してください。

## NTFS SACLアクセス制御エントリの管理用コマンド

SACLのアクセス制御エントリ(ACE)を管理するための、特定のData ONTAPコマンドが存在します。ACEはいつでもNTFS SACLに追加できます。また、NTFS SACLのACEに関する情報を変更、削除、表示するなどで、既存のSACLを管理することができます。

| 状況                     | 使用するコマンド                                                      |
|------------------------|---------------------------------------------------------------|
| ACEの作成およびNTFS SACLへの追加 | <code>vserver security file-directory ntfs sacl add</code>    |
| NTFS SACLの既存のACEの変更    | <code>vserver security file-directory ntfs sacl modify</code> |



| 状況                        | 使用するコマンド                                                      |
|---------------------------|---------------------------------------------------------------|
| NTFS SACLの既存のACEに関する情報の表示 | <code>vserver security file-directory ntfs sacl show</code>   |
| NTFS SACLからの既存のACEの削除     | <code>vserver security file-directory ntfs sacl remove</code> |

詳細については、`vserver security file-directory ntfs sacl`コマンドのマニュアル ページを参照してください。

## セキュリティ ポリシーの管理用コマンド

セキュリティ ポリシーを管理するための、特定のData ONTAPコマンドが存在します。ポリシーに関する情報を表示したり、ポリシーを削除したりすることができます。セキュリティ ポリシーの変更はできません。

| 状況                     | 使用するコマンド                                                   |
|------------------------|------------------------------------------------------------|
| セキュリティ ポリシーを作成する       | <code>vserver security file-directory policy create</code> |
| セキュリティ ポリシーに関する情報を表示する | <code>vserver security file-directory policy show</code>   |
| セキュリティ ポリシーを削除する       | <code>vserver security file-directory policy delete</code> |

詳細については、`vserver security file-directory policy`コマンドのマニュアル ページを参照してください。

## セキュリティ ポリシー タスクの管理用コマンド

セキュリティ ポリシー タスクに関する情報を追加、変更、削除、表示するための、Data ONTAPコマンドが存在します。

| 状況                         | 使用するコマンド                                                        |
|----------------------------|-----------------------------------------------------------------|
| セキュリティ ポリシー タスクを追加する       | <code>vserver security file-directory policy task add</code>    |
| セキュリティ ポリシー タスクを変更する       | <code>vserver security file-directory policy task modify</code> |
| セキュリティ ポリシー タスクに関する情報を表示する | <code>vserver security file-directory policy task show</code>   |
| セキュリティ ポリシー タスクを削除する       | <code>vserver security file-directory policy task remove</code> |

詳細については、`vserver security file-directory policy task`コマンドのマニュアル ページを参照してください。

## セキュリティ ポリシー ジョブの管理用コマンド

セキュリティ ポリシー ジョブに関する情報を一時停止、再開、停止、表示するための、Data ONTAPコマンドが存在します。

| 状況                         | 使用するコマンド                                                                                                     |
|----------------------------|--------------------------------------------------------------------------------------------------------------|
| セキュリティ ポリシー ジョブを一時停止する     | <code>vserver security file-directory job pause -vserver vserver_name -id integer</code>                     |
| セキュリティ ポリシー ジョブを再開する       | <code>vserver security file-directory job resume -vserver vserver_name -id integer</code>                    |
| セキュリティ ポリシー ジョブに関する情報を表示する | <code>vserver security file-directory job show -vserver vserver_name</code><br>このコマンドを使用して、ジョブのジョブIDを特定できます。 |
| セキュリティ ポリシー ジョブを停止する       | <code>vserver security file-directory job stop -vserver vserver_name -id integer</code>                      |

詳細については、`vserver security file-directory job`コマンドのマニュアル ページを参照してください。

## セキュリティトレースを使用したファイルおよびディレクトリへのアクセスの検証およびトラブルシューティング

パーミッショントレーシング フィルタを追加すると、FlexVolを備えたStorage Virtual Machine(SVM)のCIFSサーバに対するクライアントまたはユーザによる処理要求が許可または拒否された理由がData ONTAPで記録されるようになります。この情報は、ファイル アクセスのセキュリティが適切であることを確認する場合や、ファイル アクセスに関する問題のトラブルシューティングを行う場合に役立ちます。

### セキュリティトレースの仕組み

セキュリティトレースを使用すると、FlexVolを備えたStorage Virtual Machine(SVM)上でのSMB経由のクライアント処理を検出するフィルタを設定して、フィルタに一致するすべてのアクセス チェックをトレースできます。トレース結果には、アクセスが許可または拒否された理由がわかりやすくまとめられています。

SVMのファイルやフォルダに対するSMBアクセスのセキュリティ設定を確認する場合や、アクセスに関する問題がある場合は、パーミッショントレーシングを有効にするフィルタを短時間で追加できます。

次のリストに、セキュリティトレースの仕組みに関する重要な特性を示します。

- セキュリティトレースはSVMレベルで適用されます。
- 各受信要求がスクリーニングされ、有効になっているセキュリティトレースのフィルタ条件に一致するかどうかを確認されます。
- トレースは、ファイルとフォルダの両方のアクセス要求に対して実行されます。
- トレースでは、次の条件に基づくフィルタリングを実行できます。
  - クライアントIP
  - SMBパス

- Windows名
- UNIX名
- 要求がスクリーニングされ、アクセスが許可されるか拒否されるかの応答結果が得られます。
- 有効になっているトレースのフィルタ条件に一致する各要求が、トレース結果ログに記録されます。
- ストレージ管理者は、フィルタが自動的に無効になるようにタイムアウトを設定できます。
- 要求が複数のフィルタに一致する場合は、インデックス番号が最も大きいフィルタの結果が記録されます。
- ストレージ管理者は、トレース結果ログを出力し、アクセス要求が許可または拒否された理由を確認することができます。

#### 関連コンセプト

[セキュリティトレースの結果の解釈方法](#) (299ページ)

[セキュリティ形式がデータ アクセスに与える影響](#) (20ページ)

#### 関連タスク

[セキュリティトレースの実行](#) (292ページ)

### アクセスのタイプによるセキュリティトレース モニタのチェック

ファイルやフォルダに対するアクセス チェックは、複数の基準に基づいて実行されます。それらのすべての基準について、セキュリティトレースで操作を監視できます。

セキュリティトレースで監視されるアクセス チェックの種類は次のとおりです。

- ボリュームとqtreeのセキュリティ形式
- 処理が要求されるファイルやフォルダを含むファイルシステムの効果的なセキュリティ
- ユーザ マッピング
- 共有レベルの権限
- ファイルレベルの権限
- ストレージレベルのアクセス保護セキュリティ

### セキュリティトレースを作成する際の考慮事項

FlexVolを備えたStorage Virtual Machine (SVM) でセキュリティトレースを作成する場合は、以下の考慮事項に注意する必要があります。たとえば、トレースを作成できるプロトコル、サポートされるセキュリティ形式、アクティブなトレースの最大数を把握しておく必要があります。

- セキュリティトレースは、FlexVolを備えたSVM上でしか作成できません。
- セキュリティトレース フィルタの各エントリはSVM固有です。  
トレースを実行するSVMを指定する必要があります。
- SMB要求に関するパーミッショントレーシング フィルタだけを追加できます。
- トレース ファイルを作成するSVM上にCIFSサーバをセットアップする必要があります。
- NTFS、UNIX、mixedセキュリティ形式のボリュームおよびqtree上に存在するファイルやフォルダに対してセキュリティトレースを作成できます。
- パーミッショントレーシング フィルタはSVMごとに10個まで追加できます。

- フィルタを作成または変更するときは、フィルタ インデックス番号を指定する必要があります。フィルタはインデックス番号順に処理されます。インデックス番号の大きいフィルタの条件は、インデックス番号の小さいフィルタの条件よりも先に処理されます。トレースされている要求が、複数の有効なフィルタの条件に一致する場合は、インデックス番号の最も大きいフィルタだけが適用されます。
- セキュリティトレース フィルタを作成し、有効にしたあと、トレース フィルタでキャプチャしてトレース結果ログに記録できるアクティビティを生成するために、クライアント システム上でファイル要求またはフォルダ要求をいくつか実行する必要があります。
- ファイル アクセスの検証またはトラブルシューティング以外の目的でパーミッショントレーシング フィルタを追加しないでください。  
パーミッショントレーシング フィルタを追加すると、コントローラのパフォーマンスが若干低下します。  
検証またはトラブルシューティングが完了したら、すべてのパーミッショントレーシング フィルタを無効化または削除する必要があります。さらに、ログに大量のトレース結果が送信されないように、できるだけ具体的なフィルタ条件を指定する必要があります。

## セキュリティトレースの実行

セキュリティトレースの実行では、セキュリティトレース フィルタの作成、フィルタ条件の確認、フィルタ条件に一致するSMBクライアントへのアクセス リクエストの生成、トレース結果の表示などを行います。

### タスク概要

トレース情報の取得が完了した後に、使用したセキュリティ フィルタに変更を加え、再度利用することができます。続けて使用しない場合は、無効にします。また、フィルタのトレース結果の表示、分析が完了し、その結果が不要になった場合には削除できます。

### 手順

1. **セキュリティトレース フィルタの作成** (293ページ)  
FlexVolを備えたStorage Virtual Machine (SVM) でSMBクライアント処理を検出し、フィルタに一致するすべてのアクセス チェックをトレースするセキュリティトレース フィルタを作成できます。セキュリティトレースの結果を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。
2. **セキュリティトレース フィルタに関する情報の表示** (295ページ)  
Storage Virtual Machine (SVM) で設定されているセキュリティトレース フィルタに関する情報を表示できます。この情報から、各フィルタがトレースするアクセス イベントの種類を確認できます。
3. **セキュリティトレースの結果の表示** (295ページ)  
セキュリティトレース フィルタに一致するファイル操作に対して生成されたセキュリティトレースの結果を表示できます。この結果を使用して、ファイル アクセス セキュリティ設定の検証や、SMBファイル アクセスに関する問題のトラブルシューティングを行うことができます。
4. **セキュリティトレース フィルタの変更** (297ページ)  
トレースされたアクセス イベントを特定する際に使用するオプションのフィルタ パラメータを変更するには、既存のセキュリティトレース フィルタを変更します。
5. **セキュリティトレース フィルタの削除** (298ページ)  
セキュリティトレース フィルタ エントリが必要なくなった場合は、削除できます。セキュリティトレース フィルタはStorage Virtual Machine (SVM) ごとに10個までしか使用できないので、上限に達した場合は、不要なフィルタを削除すると、新しいフィルタを作成できます。
6. **セキュリティトレース レコードの削除** (298ページ)  
セキュリティトレース レコードを使用したファイル アクセス セキュリティの検証や、SMBクライアント アクセスに関する問題のトラブルシューティングが完了したら、セキュリティトレースのログからセキュリティトレース レコードを削除できます。

## 7. すべてのセキュリティトレース レコードの削除 (299ページ)

既存のセキュリティトレース レコードが不要である場合は、1つのコマンドで特定のノード上のレコードをすべて削除できます。

### 関連コンセプト

[セキュリティトレースの仕組み](#) (290ページ)

[アクセスのタイプによるセキュリティトレース モニタのチェック](#) (291ページ)

[セキュリティトレースを作成する際の考慮事項](#) (291ページ)

[セキュリティトレースの結果の解釈方法](#) (299ページ)

[ファイル セキュリティと監査ポリシーに関する情報の表示](#) (246ページ)

### セキュリティトレース フィルタの作成

FlexVolを備えたStorage Virtual Machine (SVM) でSMBクライアント処理を検出し、フィルタに一致するすべてのアクセス チェックをトレースするセキュリティトレース フィルタを作成できます。セキュリティトレースの結果を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。

#### タスク概要

このコマンドには2つの必須パラメータがあります。

| 必須パラメータ                  | 説明                                                                                           |
|--------------------------|----------------------------------------------------------------------------------------------|
| -vserver<br>vserver_name | <i>SVM名</i><br>セキュリティトレース フィルタを適用するファイルやフォルダが格納されているSVMの名前。                                  |
| -index<br>index_number   | <i>フィルタ インデックス番号</i><br>フィルタに適用するインデックス番号。トレース フィルタはSVMごとに10個まで使用できます。このパラメータに指定できる値は1～10です。 |

さまざまなオプションのフィルタ パラメータでセキュリティトレース フィルタをカスタマイズして、セキュリティトレースによって生成された結果を絞り込むことができます。

| フィルタ パラメータ               | 説明                                                                                                                                                                                 |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -client-ip<br>IP_Address | IPアドレスを指定します。このIPアドレスからSVMにアクセスしているユーザが対象となります。                                                                                                                                    |
| -path path               | パーミッショントレース フィルタを適用するパスを指定します。-pathの値には次の形式を使用できます。 <ul style="list-style-type: none"> <li>共有のルートから始まる絶対パス</li> <li>共有のルートに対する相対パス</li> </ul> パス値では、NFS形式のディレクトリ区切り文字を使用する必要があります。 |

| フィルタ パラメータ                                                                       | 説明                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -windows-name<br><i>win_user_name</i> または<br>-unix-name<br><i>unix_user_name</i> | アクセス要求をトレースする対象のWindowsユーザ名またはUNIXユーザ名を指定できます。このユーザ名変数では大文字と小文字が区別されません。同じフィルタでWindowsユーザ名とUNIXユーザ名の両方を指定することはできません。<br><br>注: トレースできるのはSMBアクセス イベントですが、mixedセキュリティ形式またはUNIXセキュリティ形式のデータに対してアクセスチェックを実行するときに、マッピングされたUNIXユーザおよびUNIXグループが使用されることがあります。 |
| -trace-allow<br>{yes no}                                                         | セキュリティトレース フィルタでは、拒否イベントのトレースは常に有効です。必要に応じて、許可イベントをトレースすることもできます。許可イベントをトレースするには、このパラメータをyesに設定します。                                                                                                                                                   |
| -enabled<br>{enabled disabled}                                                   | セキュリティトレース フィルタを有効または無効にすることができます。デフォルトでは、セキュリティトレース フィルタは有効になっています。                                                                                                                                                                                  |
| -time-enabled<br><i>integer</i>                                                  | フィルタのタイムアウトを指定できます。指定した時間が経過すると、フィルタは無効になります。                                                                                                                                                                                                         |

## 手順

1. セキュリティトレース フィルタを作成します。

```
vserver security trace filter create -vserver vserver_name -index  
index_number filter_parameters
```

### 例

*filter\_parameters*は、オプションのフィルタ パラメータのリストです。

詳細については、このコマンドのマニュアル ページを参照してください。

2. セキュリティトレース フィルタのエントリを確認します。

```
vserver security trace filter show -vserver vserver_name -index  
index_number
```

### 例

次のコマンドでは、IPアドレス10.10.10.7から共有パス\\server\share1\dir1\dir2\file.txtのファイルにアクセスしているすべてのユーザを対象とするセキュリティトレース フィルタを作成します。また、このフィルタでは、-path オプションに絶対パスを使用します。データへのアクセスに使用されるクライアントのIPアドレスは10.10.10.7です。30分経過すると、フィルタはタイムアウトします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1 -path /dir1/dir2/  
file.txt -time-enabled 30 -client-ip 10.10.10.7  
cluster1::> vserver security trace filter show -index 1
```

| Vserver | Index | Client-IP  | Path                | Trace-Allow | Windows-Name |
|---------|-------|------------|---------------------|-------------|--------------|
| vs1     | 1     | 10.10.10.7 | /dir1/dir2/file.txt | no          | -            |

次のコマンドでは、-pathオプションに相対パスを使用してセキュリティトレース フィルタを作成します。このフィルタでは、「joe」という名前のWindowsユーザのアクセスをトレースします。joeは共有パス\\server\share1\dir1\dir2\file.txtのファイルにアクセスしています。許可イベントと拒否イベントをトレースします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2 -path /dir1/dir2/
file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
Vserver: vs1
Filter Index: 2
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: mydomain\joe
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

## セキュリティトレース フィルタに関する情報の表示

Storage Virtual Machine(SVM)で設定されているセキュリティトレース フィルタに関する情報を表示できます。この情報から、各フィルタがトレースするアクセス イベントの種類を確認できます。

### 手順

1. `vserver security trace filter show`コマンドを使用して、セキュリティトレース フィルタ エントリに関する情報を表示します。

このコマンドを使用する方法については、マニュアル ページを参照してください。

### 例

次のコマンドを実行すると、SVM vs1のすべてのセキュリティトレース フィルタに関する情報が表示されます。

```
cluster1::> vserver security trace filter show -vserver vs1
```

| Vserver | Index | Client-IP | Path                | Trace-Allow | Windows-Name |
|---------|-------|-----------|---------------------|-------------|--------------|
| vs1     | 1     | -         | /dir1/dir2/file.txt | yes         | -            |
| vs1     | 2     | -         | /dir3/dir4/         | no          | mydomain\joe |

## セキュリティトレースの結果の表示

セキュリティトレース フィルタに一致するファイル操作に対して生成されたセキュリティトレースの結果を表示できます。この結果を使用して、ファイル アクセス セキュリティ設定の検証や、SMBファイル アクセスに関する問題のトラブルシューティングを行うことができます。

### 開始する前に

有効なセキュリティトレース フィルタが存在している必要があり、セキュリティトレースの結果が生成されるように、セキュリティトレース フィルタに一致するSMBクライアントから操作が実行されている必要があります。

### タスク概要

すべてのセキュリティトレースの結果の要約を表示することも、オプションのパラメータを指定して、表示される情報をカスタマイズすることもできます。これは、多数のレコードがセキュリティトレースの結果に含まれる場合に便利です。

オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- Storage Virtual Machine(SVM) 名
- ノード名
- セキュリティトレースのインデックス番号
- セキュリティ形式

- パス

- 理由

- ユーザ名

表示されるユーザ名は、トレース フィルタの設定方法によって異なります。

| フィルタの設定方法      | 表示されるユーザ名           |
|----------------|---------------------|
| UNIXユーザ名を使用    | UNIXユーザ名が表示されます。    |
| Windowsユーザ名を使用 | Windowsユーザ名が表示されます。 |
| ユーザ名を使用しない     | Windowsユーザ名が表示されます。 |

オプションのパラメータを使用して、出力をカスタマイズできます。コマンド出力で返される結果を絞り込むために使用できるオプションのパラメータには、次のようなものがあります。

| オプションのパラメータ                              | 説明                                                                                   |
|------------------------------------------|--------------------------------------------------------------------------------------|
| -fields<br><i>field_name, ...</i>        | 選択したフィールドを表示します。このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。                          |
| -instance                                | セキュリティトレース イベントに関する詳細情報を表示します。このパラメータを他のオプションのパラメータとともに使用して、特定のフィルタ結果に関する詳細情報を表示します。 |
| -node <i>node_name</i>                   | 指定したノード上のイベントに関する情報のみを表示します。                                                         |
| -vserver<br><i>vserver_name</i>          | 指定したSVM上のイベントに関する情報のみを表示します。                                                         |
| -index <i>integer</i>                    | 指定したインデックス番号に対応するフィルタの結果として発生したイベントに関する情報を表示します。                                     |
| -client-ip<br><i>IP_address</i>          | 指定したクライアントIPアドレスからのファイル アクセスの結果として発生したイベントに関する情報を表示します。                              |
| -path <i>path</i>                        | 指定したパスへのファイル アクセスの結果として発生したイベントに関する情報を表示します。                                         |
| -user-name<br><i>user_name</i>           | 指定したWindowsユーザまたはUNIXユーザによるファイル アクセスの結果として発生したイベントに関する情報を表示します。                      |
| -security-style<br><i>security_style</i> | 指定したセキュリティ形式のファイルシステムで発生したイベントに関する情報を表示します。                                          |

コマンドで使用できる他のオプションのパラメータについては、マニュアル ページを参照してください。

## 手順

1. `vserver security trace trace-result show`コマンドを使用して、セキュリティトレース フィルタの結果を表示します。

## 例

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1
```

| Node  | Index | Filter Details   | Reason                        |
|-------|-------|------------------|-------------------------------|
| node1 | 3     | User:domain\user | Access denied by explicit ACE |



|       |   |                                                        |                               |
|-------|---|--------------------------------------------------------|-------------------------------|
|       |   | Security Style:mixed<br>Path:/dir1/dir2/               |                               |
| node1 | 5 | User:domain\user<br>Security Style:unix<br>Path:/dir1/ | Access denied by explicit ACE |

## 関連コンセプト

[セキュリティトレースの結果の解釈方法](#) (299ページ)

## セキュリティトレース フィルタの変更

トレースされたアクセス イベントを特定する際に使用するオプションのフィルタ パラメータを変更するには、既存のセキュリティトレース フィルタを変更します。

### タスク概要

変更するセキュリティトレース フィルタを特定するには、フィルタを適用したStorage Virtual Machine (SVM) の名前とフィルタのインデックス番号を指定します。オプションのフィルタ パラメータはすべて変更できます。

### 手順

1. 次のコマンドを実行し、セキュリティトレース フィルタを変更します。

```
vserver security trace filter modify -vserver vserver_name -index  
index_number filter_parameters
```

- `vserver_name`は、セキュリティトレース フィルタを適用するSVMの名前です。
- `index_number`は、フィルタに適用するインデックス番号です。このパラメータに指定できる値は1～10です。
- `filter_parameters`は、オプションのフィルタ パラメータのリストです。

2. 次のコマンドを実行し、セキュリティトレース フィルタのエントリを確認します。

```
vserver security trace filter show -vserver vserver_name -index  
index_number
```

### 例

以下に示すコマンドでは、インデックス番号1のセキュリティトレース フィルタを変更します。このフィルタでは、各IPアドレスから共有パス\\server\share1\dir1\dir2\file.txt のファイルにアクセスする各ユーザのイベントをトレースします。また、このフィルタでは、`-path` オプションに絶対パスを使用します。許可イベントと拒否イベントをトレースします。

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1 -path /dir1/dir2/  
file.txt -trace-allow yes  
  
cluster1::> vserver security trace filter show -vserver vs1 -index 1  
Vserver: vs1  
Filter Index: 1  
Client IP Address to Match: -  
Path: /dir1/dir2/file.txt  
Windows User Name: -  
UNIX User Name: -  
Trace Allow Events: yes  
Filter Enabled: enabled  
Minutes Filter is Enabled: 60
```

## セキュリティトレース フィルタの削除

セキュリティトレース フィルタ エントリが必要なくなった場合は、削除できます。セキュリティトレース フィルタはStorage Virtual Machine (SVM) ごとに10個までしか使用できないので、上限に達した場合は、不要なフィルタを削除すると、新しいフィルタを作成できます。

### タスク概要

削除するセキュリティトレース フィルタを一意に識別するには、次を指定する必要があります。

- そのトレース フィルタが適用されているSVMの名前
- そのトレース フィルタのフィルタ インデックス番号

### 手順

1. 削除するセキュリティトレース フィルタ エントリのフィルタ インデックス番号を確認します。

```
vserver security trace filter show -vserver vs1
```

#### 例

```
vserver security trace filter show -vserver vs1
```

| Vserver | Index | Client-IP | Path                | Trace-Allow | Windows-Name |
|---------|-------|-----------|---------------------|-------------|--------------|
| vs1     | 1     | -         | /dir1/dir2/file.txt | yes         | -            |
| vs1     | 2     | -         | /dir3/dir4/         | no          | mydomain\joe |

2. 前の手順で確認したフィルタ インデックス番号を使用して、フィルタ エントリを削除します。

```
vserver security trace filter delete -vserver vs1 -index 1
```

#### 例

```
vserver security trace filter delete -vserver vs1 -index 1
```

3. セキュリティトレース フィルタ エントリが削除されたことを確認します。

```
vserver security trace filter show -vserver vs1
```

#### 例

```
vserver security trace filter show -vserver vs1
```

| Vserver | Index | Client-IP | Path        | Trace-Allow | Windows-Name |
|---------|-------|-----------|-------------|-------------|--------------|
| vs1     | 2     | -         | /dir3/dir4/ | no          | mydomain\joe |

## セキュリティトレース レコードの削除

セキュリティトレース レコードを使用したファイル アクセス セキュリティの検証や、SMBクライアント アクセスに関する問題のトラブルシューティングが完了したら、セキュリティトレースのログからセキュリティトレース レコードを削除できます。

### タスク概要

セキュリティトレース レコードを削除する前に、レコードのシーケンス番号を確認する必要があります。

**注:** 各Storage Virtual Machine(SVM)には、最大128件のトレース レコードを保存できます。SVMでこの上限に達した場合、最も古いトレース レコードが自動的に削除されて、新しいレコードが追加されます。したがって、SVMのトレース レコードを手動で削除しなくても、上限に達したときに、Data ONTAPによって自動的に最も古いトレース結果を削除して新しい結果用のスペースを確保することができます。

#### 手順

1. 削除するレコードのシーケンス番号を確認します。

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. セキュリティトレース レコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name -seqnum integer
```

#### 例

```
vserver security trace trace-result delete -vserver vs1 -node node1 -  
seqnum 999
```

- `-node node_name`は、削除するパーミッショントレーシング イベントが発生したクラスタノードの名前です。  
これは必須パラメータです。
- `-vserver vserver_name`は、削除するパーミッショントレーシング イベントが発生したSVMの名前です。  
これは必須パラメータです。
- `-seqnum integer`は、削除するログ イベントのシーケンス番号です。  
これは必須パラメータです。

### すべてのセキュリティトレース レコードの削除

既存のセキュリティトレース レコードが不要である場合は、1つのコマンドで特定のノード上のレコードをすべて削除できます。

#### 手順

1. すべてのセキュリティトレース レコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name *
```

- `-node node_name`は、削除するパーミッショントレーシング イベントが発生したクラスタノードの名前です。
- `-vserver vserver_name`は、削除するパーミッショントレーシング イベントが発生したStorage Virtual Machine(SVM)の名前です。

### セキュリティトレースの結果の解釈方法

セキュリティトレースの結果には、要求が許可または拒否された理由がまとめられています。出力には、アクセスが許可または拒否された理由と、アクセスが許可または拒否されたアクセス チェック経路内の場所を組み合わせた内容が、結果として表示されます。その結果を使用して、アクションが許可された理由または許可されなかった理由を特定できます。

#### 結果タイプとフィルタの詳細のリストを確認する

セキュリティトレースの結果に表示できる結果タイプとフィルタの詳細のリストは、`vserver security trace trace-result show`コマンドのマニュアル ページで確認できます。

**Allow結果タイプのReasonフィールドの出力例**

次に、Allow結果タイプのトレース結果ログに表示されるReasonフィールドの出力例を示します。

```
Access is allowed because CIFS implicit permission grants requested
access while opening existing file or directory.
```

**Deny結果タイプのReasonフィールドの出力例**

次に、Deny結果タイプのトレース結果ログに表示されるReasonフィールドの出力例を示します。

```
Access is denied. The requested permissions are not granted by the ACE
while checking for child-delete access on the parent.
```

**Filter detailsフィールドの出力例**

次に、トレース結果ログのFilter detailsフィールドの出力例を示します。この出力には、フィルタ条件に一致するファイルとフォルダが含まれるファイル システムの有効なセキュリティ形式が表示されます。

```
Security Style: MIXED and ACL
```

**関連タスク**

[セキュリティトレースの実行](#)(292ページ)

**関連情報**

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver security trace trace-result show - Display security trace results](#)

## SMB共有のメタデータ キャッシュの設定

メタデータのキャッシングにより、SMB 1.0クライアントでファイル属性をキャッシュして、ファイル属性およびフォルダ属性にすばやくアクセスできるようになります。属性キャッシュは、共有ごとに有効または無効にすることができます。メタデータのキャッシングが有効な場合は、キャッシュされたエントリに対するTime-To-Live(TTL)を設定することもできます。クライアントがSMB 2.xまたはSMB 3.0で共有に接続している場合は、メタデータ キャッシュの設定は必要ではありません。

### SMBメタデータのキャッシングの仕組み

SMBメタデータのキャッシングを有効にすると、パスとファイルの属性データが一定期間保存されます。これにより、一般的なワークロードでのSMB 1.0クライアントのSMBパフォーマンスを向上させることができます。

特定のタスクでは、SMBによって大量のトラフィックが作成され、そのトラフィックにはパスとファイルのメタデータに対する複数の同一クエリが含まれることがあります。代わりに、SMBメタデータのキャッシングを使用してキャッシュから情報を読み込むことで、重複するクエリを減らし、SMB 1.0クライアントのパフォーマンスを向上させることができます。

**注意:** メタデータのキャッシングを使用すると、ごくまれに、古い情報がSMB 1.0クライアントに提供されることがあります。ご使用の環境でこのリスクを回避する必要がある場合は、この機能を有効にしないでください。

### SMBメタデータのキャッシングの有効化

SMBメタデータのキャッシングを有効にすることで、SMB 1.0クライアントのSMBパフォーマンスが向上します。デフォルトでは、SMBメタデータのキャッシングは無効になっています。

手順

1. 次のうち必要な操作を実行します。

| 状況                           | 入力するコマンド                                                                                                                        |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 共有の作成時にSMBメタデータのキャッシングを有効にする | <code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code> |
| 既存の共有でSMBメタデータのキャッシングを有効にする  | <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</code>    |

関連タスク

- [SMBメタデータ キャッシュ エントリの有効期間の設定](#)(301ページ)
- [CIFSサーバでのSMB共有の作成](#)(180ページ)
- [既存のSMB共有に対する共有プロパティの追加または削除](#)(187ページ)

### SMBメタデータ キャッシュ エントリの有効期間の設定

SMBメタデータ キャッシュ エントリの有効期間を設定できます。これにより、環境内でのSMBメタデータ キャッシュのパフォーマンスを最適化できます。デフォルト値は10秒です。

開始する前に

SMBメタデータ キャッシュ機能を有効にしている必要があります。SMBメタデータのキャッシングが有効でない場合、SMBキャッシュのTTL設定は使用されません。

手順

1. 次のうち必要な操作を実行します。

| SMBメタデータ キャッシュ エントリの有効期間を設定する方法 | 入力するコマンド                                                                                                                                            |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 共有を作成する                         | <code>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</code> |
| 既存の共有を変更する                      | <code>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</code>            |

共有を作成または変更するときに、追加の共有設定オプションおよび共有プロパティを指定できます。詳細については、マニュアル ページを参照してください。

## ファイル ロックの管理

ボリュームやファイルにクライアントがアクセスできない場合、その理由を特定するには、まず最初にStorage Virtual Machine (SVM) の現在のロック状態について情報を表示できます。ファイルのロックを解除する必要がある場合、この情報が役に立ちます。

ファイル ロックがInfinite Volumeに与える影響については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

### プロトコル間のファイル ロックについて

ファイル ロックとは、あるユーザがすでに開いているファイルに別のユーザがアクセスすることを防ぐ機能で、クライアント アプリケーションで使用されます。Data ONTAPでファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントがNFSクライアントである場合、ロックは任意に設定します。クライアントがSMBクライアントである場合、ロックは必須となります。

NFSファイルとSMBファイルのロックの違いのため、SMBアプリケーションですでに開いているファイルにNFSクライアントからアクセスすると、エラーになる場合があります。

NFSクライアントがSMBアプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、rm、rmdir、mvなどのファイル処理を行うと、NFSアプリケーションがエラーになる場合があります。
- NFSの読み取りと書き込みの処理は、SMBの読み取り拒否および書き込み拒否のオープン モードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的なSMBバイトロックでロックされている場合も、NFSの書き込みの処理はエラーになります。

UNIXセキュリティ形式のボリュームでは、NFSのリンク解除および名前変更の処理でSMBのロック状態が無視され、ファイルへのアクセスが許可されます。UNIXセキュリティ形式のボリュームでのその他すべてのNFS処理では、SMBのロック状態が考慮されます。

### Data ONTAPによる読み取り専用ビットの処理方法

読み取り専用ビットは、ファイルが書き込み可能(無効)なのか読み取り専用(有効)なのかを示すために、ファイルごとに設定される2進数の数値です(0または1)。

MS-DOSおよびWindowsを使用するSMBクライアントは、ファイルごとの読み取り専用ビットを設定できます。NFSクライアントは、ファイルごとの読み取り専用ビットを設定しません。NFSクライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

Data ONTAPは、MS-DOSまたはWindowsを使用するSMBクライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルがNFSクライアントとSMBクライアント間で共有されている場合も、読み取り専用ビットを設定できます。一部のソフトウェアは、NFSクライアントおよびSMBクライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFSクライアントとSMBクライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。

- NFSは、読み取り専用ビットが有効になっているファイルを書き込み権限ビットすべてが無効になっているファイルとして扱います。
- NFSクライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも1つが以前有効であったら、そのファイルの読み取り専用ビットは有効になります。

- NFSクライアントがすべての書き込み権限ビットを有効にすると、そのファイルの読み取り専用ビットは無効になります。
- あるファイルの読み取り専用ビットが有効になっているときに、NFSクライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットはNFSクライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットがNFSクライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときに、SMBクライアントがこの読み取り専用ビットを無効にすると、そのファイルに対する所有者の書き込み権限ビットが有効になります。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、rootのみです。

注: ファイル権限の変更は、SMBクライアントではすぐに反映されますが、NFSクライアントが属性のキャッシュを有効にしている場合はNFSクライアントではすぐに反映されないことがあります。

## 共有パス コンポーネントのロックの処理に関するData ONTAPとWindowsの違い

Windowsとは異なり、Data ONTAPでは、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作はSMB共有パスにも影響します。

Data ONTAPではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパス コンポーネントの名前を変更できます。このため、特定のアプリケーションで問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。これにより、共有にアクセスできなくなる場合があります。

パス コンポーネントの名前変更で生じる問題を回避するには、ユーザまたはアプリケーションが重要なディレクトリの名前を変更できないようにするセキュリティ設定を適用します。

## ロックに関する情報の表示

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロック モード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイル ロックに関する情報を表示できます。

### タスク概要

NFSv4またはNFSv4.1を使用して確立されたロックについては、クライアントIPアドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンド パラメータを使用すると、特定のStorage Virtual Machine (SVM) のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。パラメータを何も指定しない場合、このコマンドでは次の情報が表示されます。

- SVM名
- FlexVolのボリューム名またはInfinite Volumeのネームスペース コンスティチュエントの名前
- ロックされたオブジェクトのパス
- 論理インターフェイス名
- ロックの確立に使用されたプロトコル
- ロックの種類
- クライアント

vserver locks showコマンドでは、次の4種類のロックに関する情報が表示されます。

- バイト範囲ロック。ファイルの一部のみをロックします。

- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。SMBを使用してクライアント側キャッシュを制御します。
- 委譲。NFSv4.xを使用してクライアント側キャッシュを制御します。

オプションのパラメータを指定すると、これらの各種のロックに関する重要な情報を確認できます。詳細については、コマンドのマニュアル ページを参照してください。

## 手順

1. `vserver locks show`コマンドを使用して、ロックに関する情報を表示します。

### 例

次の例では、パス `/vol1/file1` のファイルに対する NFSv4 ロックについての概要情報を表示します。共有ロックのアクセス モードは `write-deny_none` であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol Lock Type  Client
-----
vol1    /vol1/file1                 lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     Delegation Type: write          delegation -
```

次の例では、パス `/data2/data2_2/intro.pptx` のファイルに対する SMB ロックについての `oplock` および共有ロックの詳細情報を表示します。IP アドレスが `10.3.1.3` のクライアントに対して、共有ロックのアクセス モードを `write-deny_none` として、永続性ハンドルが許可されています。バッチの `oplock` レベルで `oplock` リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
ByteLock Starting Offset: -
Number of Bytes Locked: -
ByteLock is Mandatory: -
ByteLock is Exclusive: -
ByteLock is Superlock: -
ByteLock is Soft: -
Oplock Level: -
Shared Lock Access Mode: write-deny_none
Shared Lock is Soft: false
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: durable
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/test.pptx
Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
Lock Protocol: cifs
Lock Type: op-lock
Node Holding Lock State: node3
Lock State: granted
ByteLock Starting Offset: -
Number of Bytes Locked: -
ByteLock is Mandatory: -
ByteLock is Exclusive: -
ByteLock is Superlock: -
ByteLock is Soft: -
Oplock Level: batch
```



```
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## ロックの解除

ファイル ロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

### タスク概要

`vserver locks break` コマンドは、advanced以上の権限レベルでのみ使用できます。詳細については、コマンドのマニュアル ページを参照してください。

### 手順

1. ロックを解除するために必要な情報を確認するには、`vserver locks show` コマンドを使用します。  
詳細については、コマンドのマニュアル ページを参照してください。

2. 権限レベルをadvancedに設定します。

**set -privilege advanced**

3. 次のいずれかを実行します。

| ロックを解除するための指定項目             | 入力するコマンド                                                                                                             |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------|
| SVM名、ボリューム名、LIF名、およびファイル パス | <b>vserver locks break -vserver <i>vserver_name</i> -volume <i>volume_name</i> -path <i>path</i> -lif <i>lif</i></b> |
| ロックID                       | <b>vserver locks break -lockid <i>UUID</i></b>                                                                       |

-vserver *vserver\_name*には、SVM名を指定します。

-volume *volume\_name*では、FlexVolのボリューム名、またはInfinite Volumeのネームスペース コンスティチュエントの名前を指定します。

-path *path*では、パスを指定します。

-lif *lif*には、論理インターフェイスを指定します。

-lockidでは、ロックのUniversally Unique Identifier(UUID)を指定します。

4. admin権限レベルに戻ります。

**set -privilege admin**

## SMBアクティビティの監視

SMBアクティビティの監視では、SMBセッションと開いているファイルの情報を表示できます。また、SMB統計の情報を表示することもできます。

## SMBセッション情報の表示

SMB接続、SMBセッションID、セッションを使用しているワークステーションのIPアドレスなど、確立されたSMBセッションに関する情報を表示できます。セッションのSMBプロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

### タスク概要

Storage Virtual Machine(SVM)上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションの `-fields` パラメータを使用して、選択したフィールドの出力を表示できます。  
`-fields ?`と入力すると、使用できるフィールドを確認できます。
- `-instance` パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます。
- `-fields` パラメータまたは `-instance` パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

### 手順

1. 次のいずれかを実行します。

| 確立されたセッションのSMBセッション情報を表示する対象 | 入力するコマンド                                                                                                                                                                                                                                                                            |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SVM上のすべてのセッション (要約形式)        | <code>vserver cifs session show -vserver <i>vserver_name</i></code>                                                                                                                                                                                                                 |
| 指定した接続IDのセッション               | <code>vserver cifs session show -vserver <i>vserver_name</i> -connection-id <i>integer</i></code>                                                                                                                                                                                   |
| 指定したワークステーションのIPアドレスからのセッション | <code>vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i></code>                                                                                                                                                                          |
| 指定したLIF IPアドレスのセッション         | <code>vserver cifs session show -vserver <i>vserver_name</i> -lif-address <i>LIF_IP_address</i></code>                                                                                                                                                                              |
| 指定したノード上のファイル                | <code>vserver cifs session show -vserver <i>vserver_name</i> -node {<i>node_name</i> local}</code>                                                                                                                                                                                  |
| 指定したWindowsユーザからのセッション       | <code>vserver cifs session show -vserver <i>vserver_name</i> -windows-user <i>user_name</i></code><br><br><i>user_name</i> の形式は[domain]\userです。                                                                                                                                     |
| 指定した認証メカニズムを使用しているセッション      | <code>vserver cifs session show -vserver <i>vserver_name</i> -auth-mechanism <i>authentication_mechanism</i></code><br><br>-auth-mechanismには、次のいずれかの値を指定できます。 <ul style="list-style-type: none"> <li>• NTLMv1</li> <li>• NTLMv2</li> <li>• Kerberos</li> <li>• Anonymous</li> </ul> |

| 確立されたセッションのSMB<br>セッション情報を表示する対<br>象    | 入力するコマンド                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 指定したプロトコル バージョ<br>ンを使用しているセッション         | <pre>vserver cifs session show -vserver <i>vserver_name</i> -<br/>protocol-version <i>protocol_version</i></pre> <p>-protocol-versionには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"><li>• <b>SMB1</b></li><li>• <b>SMB2</b></li><li>• <b>SMB2_1</b></li><li>• <b>SMB3</b></li></ul> <p><b>注:</b> 継続的可用性を備えた保護は、SMB 3.0セッションでのみ使用で<br/>きます。該当するすべてのセッションの継続的可用性を備えた保護<br/>のステータスを表示するには、このパラメータの値を<b>SMB3</b>に設定し<br/>ます。</p>                                                                                                                                 |
| 指定したレベルの継続的<br>可用性を備えた保護を使用し<br>ているファイル | <pre>vserver cifs session show -vserver <i>vserver_name</i> -<br/>continuously-available<br/>continuously_available_protection_level</pre> <p>-continuously-availableには、次のいずれかの値を指定でき<br/>ます。</p> <ul style="list-style-type: none"><li>• <b>No</b></li><li>• <b>Yes</b></li><li>• <b>Partial</b></li></ul> <p><b>注:</b> 継続的可用性のステータスが<b>Partial</b>の場合、継続的可用性<br/>を使用して開かれたファイルが1つ以上セッションにあるが、継続的<br/>可用性を備えた保護を使用せずに開かれたファイルもセッションに<br/>あることを意味します。vserver cifs sessions file show<br/>コマンドを使用すると、確立されたセッションのファイルのうち、継続<br/>的可用性を備えた保護を使用せずに開かれたファイルを確認できま<br/>す。</p> |
| 指定したSMB署名セッション<br>ステータスのセッション           | <pre>vserver cifs session show -vserver <i>vserver_name</i> -<br/>is-session-signed {true false}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279  1      10.1.1.1      DOMAIN\joe      2      23s
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。この接続はドメイン コンピュータ アカウントを使用して行われています。

```
cluster1::> vserver cifs session show -instance -continuously-available Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

次のコマンドを実行すると、SVM vs1上のSMB 3.0を使用しているセッションに関するセッション情報が表示されます。ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するためには、Kerberos認証を使用して接続を行う必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151272607
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

## 関連タスク

[開いているSMBファイルに関する情報の表示](#) (308ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver cifs session show - Display established CIFS sessions](#)

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver cifs session close - Close an open CIFS session](#)

## 開いているSMBファイルに関する情報の表示

SMB接続、SMBセッションID、ホスティング ボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する

情報も表示できます。この情報は、開いているファイルがノンストップ オペレーションをサポートする状態であるかどうか確認するのに役立ちます。

### タスク概要

確立されたSMBセッションで開いているファイルに関する情報を表示できます。これは、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと、継続的可用性を備えた保護を使用せずに開いているファイルがある場合 (vserver cifs session show コマンド出力の -continuously-available フィールドの値は **Partial** になります)、このコマンドによって、継続的可用性に対応していないファイルを特定できます。

オプションのパラメータを何も指定せずに vserver cifs session file show コマンドを実行することで、Storage Virtual Machine (SVM) 上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションの -fields パラメータを使用して、選択したフィールドの出力を表示できます。このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。
- -instance パラメータを使用して、開いているSMBファイルに関する詳細情報を表示できます。このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。

### 手順

1. 次のいずれかを実行します。

| 表示する開いているSMBファイル       | 入力するコマンド                                                                                            |
|------------------------|-----------------------------------------------------------------------------------------------------|
| SVM上のファイル(要約形式)        | <code>vserver cifs session file show -vserver vserver_name</code>                                   |
| 指定したノード上のファイル          | <code>vserver cifs session file show -vserver vserver_name -node {node_name local}</code>           |
| 指定したファイルIDのファイル        | <code>vserver cifs session file show -vserver vserver_name -file-id integer</code>                  |
| 指定したSMB接続IDのファイル       | <code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>            |
| 指定したSMBセッションIDのファイル    | <code>vserver cifs session file show -vserver vserver_name -session-id integer</code>               |
| 指定したホスティング アグリゲートのファイル | <code>vserver cifs session file show -vserver vserver_name -hosting-aggregate aggregate_name</code> |
| 指定したボリュームのファイル         | <code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>       |
| 指定したSMB共有のファイル         | <code>vserver cifs session file show -vserver vserver_name -share share_name</code>                 |
| 指定したSMBパスのファイル         | <code>vserver cifs session file show -vserver vserver_name -path path</code>                        |

## 表示する開いているSMBファイル

## 入力するコマンド

指定したレベルの継続的可用性を備えた保護を使用しているファイル

```
vserver cifs session file show -vserver  
vserver_name -continuously-available  
continuously_available_status
```

-continuously-availableには、次のいずれかの値を指定できます。

- No
- Yes

**注:** 継続的可用性のステータスがNoの場合、それらの開いているファイルが、テイクオーバーやギブバックからのシステム停止不要のリカバリに対応していないことを意味します。また、可用性の高い関係のパートナー間における一般的なアグリゲートの再配置からリカバリすることもできません。

## 指定した再接続の状態のファイル

```
vserver cifs session file show -vserver  
vserver_name -reconnected reconnected_state
```

-reconnectedには、次のいずれかの値を指定できます。

- No
- Yes

**注:** 再接続の状態がNoの場合、その開いているファイルは、切断の発生後に再接続されていません。つまり、そのファイルは一度も切断されていないか、切断されてから再接続できなかったことを意味します。再接続の状態がYesの場合、その開いているファイルは、切断の発生後に正常に再接続されたことを意味します。

ほかにも、出力結果を詳細に指定するためのオプションのパラメータがあります。詳細については、マニュアル ページを参照してください。

## 例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File ID     File Type      Open Mode  Hosting Volume  Share      Continuously
-----
41          Regular          r          data          data       data       Yes
Path: \mytest.rtf
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82 -instance
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
```

```

Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No

```

## 関連タスク

[SMBセッション情報の表示](#) (306ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver cifs session file show - Display opened CIFS files](#)

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver cifs session file close - Close an open CIFS file](#)

## 使用可能な統計オブジェクトと統計カウンタの確認

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得し、パフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| 確認する項目               | コマンド                                                             |
|----------------------|------------------------------------------------------------------|
| 使用可能なオブジェクト          | <code>statistics catalog object show</code>                      |
| 使用可能な特定のオブジェクトに関する情報 | <code>statistics catalog object show -object object_name</code>  |
| 使用可能なカウンタ            | <code>statistics catalog counter show -object object_name</code> |

使用可能なオブジェクトとカウンタの詳細については、マニュアル ページを参照してください。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

### 例

次のコマンドを実行すると、advanced権限レベルで表示したときの、クラスタ内のCIFSおよびSMBアクセスに関連する特定の統計オブジェクトの説明が表示されます。

```

cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed
to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
audit_ng
CM object for exporting audit_ng performance
counters

cluster1::*> statistics catalog object show -object cifs
cifs
The CIFS object reports activity of the
Common Internet File System protocol
subsystem. This is the Microsoft file-sharing
protocol that evolved from the Server Message
Block (SMB) application layer network
protocol to connect PCs to Network Attached

```

```

cluster1::*> statistics catalog nblade_cifs
Storage devices (NAS). This object reports activity for both SMB and SMB2 revisions of the CIFS protocol. For information related only to SMB, see the 'smb1' object. For information related only to SMB2, see the 'smb2' object.

cluster1::*> statistics catalog smb1
object show -object nblade_cifs
The Common Internet File System (CIFS) protocol is an implementation of the Server Message Block (SMB) protocol. It is a standard application layer file system protocol used to share files with Windows(TM) systems. This object tracks the data transfer performance at the CIFS protocol layer, in Ontap's Nblade network component. These counters are relevant to the entire node, rather than individual virtual servers.

cluster1::*> statistics catalog smb2
object show -object smb1
These counters report activity from the SMB revision of the protocol. For information specific to SMB2, see the 'smb2' object. To see an overview across both revisions, see the 'cifs' object.

cluster1::*> statistics catalog hashd
object show -object smb2
These counters report activity from the SMB2/SMB3 revision of the protocol. For information specific to SMB, see the 'smb1' object. To see an overview across all revisions, see the 'cifs' object.

cluster1::*> statistics catalog hashd
object show -object hashd
The hashd object provides counters to measure the performance of the BranchCache hash daemon.

cluster1::*> set -privilege admin

```

次のコマンドを実行すると、advanced権限レベルで表示したときの、cifsオブジェクトの一部のカウンタに関する情報が表示されます。

注: この例で表示されているのは、cifsオブジェクトに使用できるカウンタの一部であり、出力は省略されています。

```

cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
Counter          Description
-----
active_searches  Number of active searches over SMB and SMB2
auth_reject_too_many Authentication refused after too many requests were made in rapid succession
avg_directory_depth Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data. It does not include attempts to fetch hash data that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch hash data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients requesting hashes.
branchcache_missing_hash_bytes Total number of bytes of data that had to be read by the client because the hash for that content was not available on the server.
change_notifications_outstanding Number of active change notifications over SMB and SMB2
cifs_latency     Average latency for CIFS operations
cifs_latency_base Total observed CIFS operations to be used as a base counter for CIFS average latency calculation
cifs_ops         Total number of CIFS operations

```



```
cifs_read_ops      Total number of CIFS read operations
cifs_write_ops     Total number of CIFS write operations
[...]
```

関連タスク

[統計情報の表示](#) (313ページ)

関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: statistics catalog object show - Display the list of objects](#)  
[clustered Data ONTAP 8.3.1 マニュアル ページ: statistics catalog counter show - Display the list of counters in an object](#)

統計情報の表示

CIFSとSMB、監査、およびBranchCacheハッシュに関する統計など、さまざまな統計を表示して、パフォーマンスを監視し、問題を診断することができます。

開始する前に

オブジェクトに関する情報を表示する前に、`statistics start` コマンドと、オプションの `statistics stop` コマンドを使用してデータ サンプルを収集しておく必要があります。これらのコマンドの詳細については、『*clustered Data ONTAP システム アドミニストレーション ガイド* (クラスタ管理)』を参照してください。

手順

- 1. 権限レベルをadvancedに設定します。  
`set -privilege advanced`
- 2. 次のいずれかを実行します。

| 統計を表示する対象            | コマンド                                             |
|----------------------|--------------------------------------------------|
| SMBのすべてのバージョン        | <code>statistics show -object cifs</code>        |
| SMB 1.0              | <code>statistics show -object smb1</code>        |
| SMB 2.xとSMB 3.0      | <code>statistics show -object smb2</code>        |
| ノードのCIFSサブシステム       | <code>statistics show -object nblade_cifs</code> |
| マルチプロトコルの監査          | <code>statistics show -object audit_ng</code>    |
| BranchCacheハッシュ サービス | <code>statistics show -object hashd</code>       |

詳細については、各コマンドのマニュアル ページを参照してください。

- 3. admin権限レベルに戻ります。  
`set -privilege admin`

関連タスク

[使用可能な統計オブジェクトと統計カウンタの確認](#) (311ページ)  
[SMB署名済みセッションの統計の監視](#) (92ページ)  
[BranchCache統計の表示](#) (359ページ)

[統計を使用した自動ノードリファール アクティビティの監視\(377ページ\)](#)

[統計を使用したHyper-VおよびSQL Server over SMBアクティビティの監視\(418ページ\)](#)

#### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: statistics show - Display performance data for a time interval](#)

## CIFSクライアントベースのサービスの導入

Windowsの[プロパティ]の[以前のバージョン]タブを使用したSnapshotコピーのファイルへのアクセスや、オフライン フォルダ、移動プロファイル、およびフォルダ リダイレクトの設定など、さまざまなCIFSクライアントベースのサービスを導入できます。

### オフライン ファイルを使用したオフラインで使用するファイルのキャッシング

Data ONTAPでは、オフラインで使用するファイルをローカル ホストにキャッシュできるMicrosoftのオフライン ファイル機能(クライアント側キャッシング)がサポートされます。オフライン ファイル機能を使用すると、ネットワークから切断された状態でも作業を継続できます。

Windowsのユーザドキュメントやプログラムを共有に自動でキャッシュするのか、キャッシュするファイルを手動で選択するのかを指定することができます。新規の共有では、手動キャッシングがデフォルトで有効になります。オフラインで利用可能となったファイルは、Windowsクライアントのローカル ディスクと同期されます。同期は、所定のストレージ システム共有へのネットワーク接続が復元すると行われます。

オフラインのファイルおよびフォルダに対するアクセス権限はCIFSサーバに保存されているファイルおよびフォルダと同じになるため、オフラインのファイルおよびフォルダに対して処理を行うときは、CIFSサーバに保存されているファイルおよびフォルダに対する十分な権限が必要になります。

ネットワーク上の他のユーザと同じファイルに対して変更を行った場合、ネットワークにローカルのバージョンのファイルを保存するか、他の バージョンを残すか、または両方を保存するかを選択することができます。両方のバージョンを残す場合は、ローカル ユーザが変更した新しいファイルがローカルに保存され、キャッシュされていたファイルがCIFSサーバに保存されたバージョンで上書きされて変更が反映されます。

オフライン ファイルについては、共有ごとに共有の設定を行えます。共有を作成または変更するときに、次の4つのオフライン フォルダ設定の中からいずれかを選択できます。

- キャッシュしない  
共有のクライアント側キャッシングを無効にします。クライアントのローカルにファイルやフォルダが自動的にキャッシュされず、ユーザがファイルやフォルダをローカルにキャッシュすることもできません。
- 手動キャッシング  
共有にキャッシュするファイルを手動で選択できるようにします。これがデフォルト設定です。デフォルトでは、ファイルやフォルダはローカル クライアントにキャッシュされません。オフラインで使用するためにローカルにキャッシュするファイルやフォルダをユーザが選択できます。
- ドキュメントの自動キャッシング  
ユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイルとフォルダだけです。
- プログラムの自動キャッシング  
プログラムおよびユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイル、フォルダ、およびプログラムだけです。また、この設定を選択した場合、クライアントがネットワークに接続されていても、ローカルにキャッシュされた実行ファイルが実行されます。

Windowsサーバおよびクライアントでのオフライン ファイルの設定の詳細については、Microsoft TechNetライブラリを参照してください。

## 関連コンセプト

[移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザ プロファイルの一元的な格納](#)(319ページ)

[フォルダ リダイレクトを使用したCIFSサーバへのデータの格納](#)(320ページ)

[BranchCacheを使用したブランチ オフィスでのSMB共有のコンテンツのキャッシュ](#)(344ページ)

## 関連情報

[Microsoft TechNetライブラリ: technet.microsoft.com/ja-jp/library/](https://technet.microsoft.com/ja-jp/library/)

## オフライン ファイルを使用するための要件

CIFSサーバでMicrosoftのオフライン ファイル機能を使用する前に、この機能をサポートするData ONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。

### Data ONTAPのバージョン要件

オフライン ファイルは、Data ONTAP 8.2以降のリリースでサポートされます。

### SMBプロトコルのバージョン

FlexVolを備えたStorage Virtual Machine (SVM)については、すべてのバージョンのSMBでオフライン ファイルがサポートされます。

Infinite Volumeを備えたSVMについては、SMB 1.0でオフライン ファイルがサポートされます。

### Windowsクライアントの要件

Windowsクライアントでオフライン ファイルがサポートされている必要があります。

オフライン ファイル機能をサポートするWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)) を参照してください。

## オフライン ファイルを導入する際の考慮事項

ホーム ディレクトリにshowsnapshot共有プロパティが設定されているホーム ディレクトリ共有でオフライン ファイルを導入する場合は、以下の重要な考慮事項について理解しておく必要があります。

オフライン ファイルを設定したホーム ディレクトリ共有でshowsnapshot共有プロパティを指定している場合、Windowsクライアントでは、すべてのSnapshotコピーがユーザのホーム ディレクトリ内の~snapshotフォルダの下にキャッシュされます。

次のいずれかに該当する場合、Windowsクライアントでは、すべてのSnapshotコピーがホーム ディレクトリの下にキャッシュされます。

- ユーザが、ホーム ディレクトリを クライアントからオフラインで利用できるようにしている。  
この場合、ホーム ディレクトリ内の~snapshotフォルダのコンテンツも、オフラインで利用できるようになります。
- ユーザが、My DocumentsなどのフォルダをCIFSサーバ共有にあるホーム ディレクトリのルートにリダイレクトするようにフォルダ リダイレクトを設定している。  
Windowsクライアントによっては、リダイレクトされるフォルダが自動的にオフラインで利用できるようになる場合があります。フォルダがホーム ディレクトリのルートにリダイレクトされる場合、~snapshotフォルダは、キャッシュされるオフライン コンテンツに含まれます。

**注:** ~snapshotフォルダがオフライン ファイルに含まれる場合は、オフライン ファイルの導入を避ける必要があります。~snapshotフォルダ内のSnapshotコピーには、Data ONTAPがSnapshotコピーを作成した時点のボリューム上にあったデータがすべて含まれています。そのため、

~snapshotフォルダのオフライン コピーを作成すると、クライアント上のローカル ストレージを大量に使用し、オフライン ファイルの同期中にネットワーク帯域幅を消費するうえ、オフライン ファイルの同期にかかる時間も長くなります。

## CLIを使用したSMB共有でのオフライン ファイル サポートの設定

SMB共有の作成時に、または既存のSMB 共有の変更時にいつでも、Data ONTAP CLIを使用して、4つのオフライン ファイル設定のいずれかを指定することによって、オフライン ファイルのサポートを設定できます。オフライン ファイルのサポートのデフォルト設定は手動(manual)です。

### タスク概要

オフライン ファイルのサポートを設定する場合は、次の4つのオフライン ファイル設定のいずれかを選択できます。

| 設定               | 説明                                                                                                               |
|------------------|------------------------------------------------------------------------------------------------------------------|
| <b>none</b>      | Windowsクライアントがこの共有のファイルをキャッシュすることを禁止します。                                                                         |
| <b>manual</b>    | Windowsクライアントのユーザが、キャッシュするファイルを手動で選択できるようにします。                                                                   |
| <b>documents</b> | Windowsクライアントがオフライン アクセスのために 使用するユーザのドキュメントをキャッシュすることを許可します。                                                     |
| <b>programs</b>  | Windowsクライアントがオフライン アクセスのために 使用するプログラムをキャッシュすることを許可します。クライアントは、共有が使用可能な場合 でも、キャッシュしたプログラム ファイルをオフライン モードで使用できます。 |

選択できるオフライン ファイル設定は1つだけです。既存のSMB共有でオフライン ファイル設定を変更すると、元の設定が新しいオフライン ファイル設定に置き換えられます。他の既存のSMB共有設定および共有プロパティは、削除も置換もされません。これらは明示的に削除または変更しないかぎり、有効なままです。

### 手順

- 適切な処理を実行します。

| オフライン ファイルを設定する対象 | 入力するコマンド                                                                                                                                       |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しいSMB共有          | <code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none manual documents programs}</code> |
| 既存のSMB共有          | <code>vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none manual documents programs}</code>            |

- SMB共有の設定が正しいことを確認します。

```
vserver cifs share show -vserver vserver_name -share-name share_name -instance
```

#### 例

次のコマンドでは、オフライン ファイル設定をdocumentsにして「data1」という名前のSMB共有を作成します。

```
cluster1::> vsriver cifs share create -vsriver vs1 -share-name data1 -path /
data1 -comment "Offline files" -offline-files documents

cluster1::> vsriver cifs share show -vsriver vs1 -share-name data1 -instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: documents
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

次のコマンドでは、「data1」という名前の既存のSMB共有について、オフライン ファイル設定をmanualに変更し、ファイル モードおよびディレクトリ モードの生成マスクの値を追加します。

```
cluster1::> vsriver cifs share modify -vsriver vs1 -share-name data1 -
offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vsriver cifs share show -vsriver vs1 -share-name data1 -instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: 644
Directory Mode Creation Mask: 777
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

#### 関連タスク

[CIFSサーバでのSMB共有の作成](#)(180ページ)

[既存のSMB共有に対する共有プロパティの追加または削除](#)(187ページ)

## コンピュータの管理MMCを使用したSMB共有でのオフライン ファイル サポートの設定

オフラインで使用するためにファイルをローカルにキャッシュすることをユーザに許可する場合は、コンピュータの管理MMC (Microsoft 管理コンソール) を使用してオフライン ファイルのサポートを設定できます。

#### 手順

1. WindowsサーバでMMCを開くには、エクスプローラでローカル コンピュータのアイコンを右クリックし、[管理]を選択します。

2. 左側のパネルで、**[コンピュータの管理]**を選択します。
3. **[操作] > [別のコンピュータへ接続]**を選択します。  
[コンピュータの選択]ダイアログ ボックスが表示されます。
4. CIFSサーバの名前を入力するか、**[参照]**をクリックしてCIFSサーバを指定します。  
CIFSサーバの名前がStorage Virtual Machine (SVM) ホスト名と同じである場合は、SVM名を入力します。CIFSサーバの名前がSVMホスト名と異なる場合は、CIFSサーバの名前を入力します。
5. **[OK]**をクリックします。
6. コンソール ツリーで、**[システム ツール] > [共有フォルダ]**をクリックします。
7. **[共有]**をクリックします。
8. 結果ペインで、共有を右クリックします。
9. **[プロパティ]**をクリックします。  
選択した共有のプロパティが表示されます。
10. **[全般]**タブで、**[オフラインの設定]**をクリックします。  
[オフラインの設定]ダイアログ ボックスが表示されます。
11. 必要に応じて、オフラインの可用性に関するオプションを設定します。
12. **[OK]**をクリックします。

## 移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザ プロファイルの一元的な格納

Data ONTAPでは、Windowsの移動プロファイルの格納をサポートしており、それらをStorage Virtual Machine (SVM)に関連付けられたCIFSサーバに格納することができます。ユーザ移動プロファイルを設定すると、ユーザはログイン先に関係なく自動でリソースを利用できるようになります。また、ユーザ プロファイルの管理が簡単になり、管理者にとってもメリットがあります。

移動ユーザ プロファイルには、次のような利点があります。

- 自動でリソースを利用できる  
Windows 8、Windows 7、Windows Vista、Windows 2000、またはWindows XPを実行するコンピュータであれば、ネットワーク上のどのコンピュータにログインしても、各ユーザの一意のプロファイルを自動で利用できます。ネットワークで使用するコンピュータごとに 個別にプロファイルを作成する必要はありません。
- コンピュータの交換が簡単である  
ユーザのすべてのプロファイル情報が ネットワークに別途保存されているため、交換後の新しいコンピュータにユーザのプロファイルを簡単にダウンロードできます。ユーザが新しいコンピュータに 初めてログインしたときに、サーバに保存されているユーザのプロファイル が新しいコンピュータにコピーされます。

### 関連コンセプト

[オフライン ファイルを使用したオフラインで使用するファイルのキャッシング](#)(315ページ)

[フォルダリダイレクトを使用したCIFSサーバへのデータの格納](#)(320ページ)

## 移動プロファイルを使用するための要件

CIFSサーバでMicrosoftの移動プロファイルを使用する前に、この機能をサポートするData ONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。

### Data ONTAPのバージョン要件

移動プロファイルは、Data ONTAP 8.2以降でサポートされます。

### SMBプロトコルのバージョン

FlexVolを備えたStorage Virtual Machine (SVM)については、すべてのバージョンのSMBで移動プロファイルがサポートされます。

Infinite Volumeを備えたSVMについては、SMB 1.0で移動プロファイルがサポートされます。

### Windowsクライアントの要件

移動プロファイルを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。

移動プロファイルをサポートするWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix)) を参照してください。

## 移動プロファイルの設定

ユーザがネットワーク上の任意のコンピュータにログオンしたときにそのユーザのプロファイルを自動的に使用可能にする場合には、[Active Directoryユーザーとコンピュータ]MMCスナップインで移動プロファイルを設定できます。Windows Server 2012で移動プロファイルを設定する場合は、Active Directory管理センターを使用できます。

### 手順

1. Windowsサーバで、[Active Directoryユーザーとコンピュータ]MMC (またはWindows Server 2012以降のサーバではActive Directory管理センター)を開きます。
2. 移動プロファイルを設定するユーザを見つけます。
3. ユーザを右クリックし、[プロパティ]をクリックします。
4. [プロファイル]タブで、ユーザの移動プロファイルを格納する共有のプロファイル パスを入力し、そのあとに%username%を続けます。

たとえば、プロファイル パスは\\vs1.example.com\profiles\%username%のようになります。ユーザが初めてログインしたときに、%username%はそのユーザの名前に置き換えられます。

**注:** パス\\vs1.example.com\profiles\%username%\profilesは、すべてのメンバーにフル コントロール権限が設定されているStorage Virtual Machine (SVM) vs1上の共有の共有名です。

5. [OK]をクリックします。

## フォルダ リダイレクトを使用したCIFSサーバへのデータの格納

Data ONTAPでは、Microsoftのフォルダ リダイレクトをサポートしています。ユーザや管理者は、この機能を使用して、ローカル フォルダのパスをCIFSサーバの場所にリダイレクトできます。リダイ



レクトされたフォルダは、データがSMB共有に格納されていても、ローカルのWindowsクライアントに格納されたフォルダのように扱うことができます。

フォルダ リダイレクトは、主に、ホーム ディレクトリをすでに導入している組織が既存のホーム ディレクトリ環境との互換性を維持する目的で使用します。

- たとえば、ドキュメント、デスクトップ、スタート メニューといったフォルダをリダイレクトできます。
- ユーザは、それぞれのWindowsクライアントからフォルダをリダイレクトできます。
- 管理者は、Active DirectoryのGPOを設定して、フォルダ リダイレクトを一元的に設定および管理できます。
- 移動プロファイルを設定している場合、管理者は、ユーザ データとプロファイル データを分けることができます。
- フォルダ リダイレクトとオフライン ファイルを使用して、管理者はローカル フォルダのデータ ストレージをCIFSサーバにリダイレクトし、ユーザはコンテンツをローカルにキャッシュできます。

#### 関連コンセプト

[オフライン ファイルを使用したオフラインで使用するファイルのキャッシング](#)(315ページ)

[移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザ プロファイルの一元的な格納](#)(319ページ)

## フォルダ リダイレクトを使用するための要件

CIFSサーバでMicrosoftのフォルダ リダイレクトを使用する前に、この機能をサポートするData ONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。

#### Data ONTAPのバージョン要件

Microsoftのフォルダ リダイレクトは、clustered Data ONTAP 8.2以降でサポートされます。

#### SMBプロトコルのバージョン

Flex Volを備えたStorage Virtual Machine (SVM)については、すべてのバージョンのSMBでMicrosoftのフォルダ リダイレクトがサポートされます。

Infinite Volumeを備えたSVMについては、SMB 1.0でMicrosoftのフォルダ リダイレクトがサポートされます。

#### Windowsクライアントの要件

Microsoftのフォルダ リダイレクトを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。

フォルダ リダイレクトをサポートするWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix))を参照してください。

## フォルダ リダイレクトの設定

Windowsの[プロパティ]ウィンドウを使用して、フォルダ リダイレクトを設定できます。この方法を使用する利点は、WindowsユーザがSVM管理者のサポートがなくてもフォルダ リダイレクトを設定できることです。

#### 手順

1. エクスプローラで、ネットワーク共有にリダイレクトするフォルダを右クリックします。

## 2. [プロパティ]をクリックします。

選択した共有のプロパティが表示されます。

## 3. [ショートカット]タブで[リンク先]をクリックし、選択したフォルダをリダイレクトするネットワーク上の場所のパスを指定します。

たとえば、フォルダをQ:\にマッピングされているホーム ディレクトリ内のdataフォルダにリダイレクトする場合は、リンク先としてQ:\dataを指定します。

## 4. [OK]をクリックします。

オフライン フォルダの設定の詳細については、Microsoft TechNetライブラリを参照してください。

## 関連情報

[Microsoft TechNetライブラリ: technet.microsoft.com/ja-jp/library/](https://technet.microsoft.com/ja-jp/library/)

## SMB 2.xを使用するWindowsクライアントからの~snapshotディレクトリへのアクセス方法

SMB 2.xを使用するWindowsクライアントからの~snapshotディレクトリへのアクセスに使用する方法は、SMB 1.0の場合に使用する方法とは異なります。SMB 2.x接続を使用してSnapshotコピーに格納されたデータに正常にアクセスするために~snapshotディレクトリにアクセスする方法について理解しておく必要があります。

SVM管理者は、**showsnapshot** 共有プロパティを有効または無効にすることで、Windowsクライアントのユーザが共有の~snapshotディレクトリを表示してアクセスすることができるかどうかを制御します。

**showsnapshot** 共有プロパティが無効になっている場合、SMB 2.xを使用するWindowsクライアントのユーザは、~snapshotディレクトリのパスまたはディレクトリ内の特定のSnapshotコピーのパスを手動で入力しても、~snapshotディレクトリを表示できず、~snapshotディレクトリ内のSnapshotコピーにアクセスできません。

**showsnapshot** 共有プロパティが有効になっている場合でも、SMB 2.xを使用するWindowsクライアントのユーザは、共有のルートにある、または共有のルートより下のジャンクションまたはディレクトリ内にある~snapshotディレクトリを表示できません。ただし、共有に接続したあと、共有パスの末尾に手動で~snapshotを追加することで、非表示の~snapshotディレクトリにアクセスできます。非表示の~snapshotディレクトリには、2つのエントリ ポイントからアクセスできます。

- 共有のルート
- 共有スペースのすべてのジャンクション ポイント

非表示の~snapshotディレクトリには、共有内のジャンクション以外のサブディレクトリからはアクセスできません。

### 例

次の例に示す設定では、「eng」共有へのSMB 2.x接続を使用するWindowsクライアントのユーザが、共有パス(共有のルートおよびパス内すべてのジャンクション ポイント)に手動で~snapshotを追加することで、~snapshotディレクトリにアクセスできます。非表示の~snapshotディレクトリには、次の3つのパスからアクセスできます。

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume      junction-path
-----
vs1      vs1_root          /
vs1      vs1_vol1      /eng
vs1      vs1_vol2      /eng/projects1
vs1      vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share  Path  Properties  Comment  ACL
-----
vs1      eng    /eng  oplocks     -         Everyone / Full Control
        chgnotif
        browsable
        showsnapshot
```

## 以前のバージョン機能を使用したファイルとフォルダのリカバリ

Microsoftの以前のバージョン機能は、Snapshotコピーを何らかの形でサポートしているファイルシステムで、それらが有効になっている場合に使用できます。SnapshotテクノロジーはData ONTAPに不可欠なテクノロジーの1つです。ユーザは、WindowsクライアントでMicrosoftの以前のバージョン機能を使用して、Snapshotコピーからファイルとフォルダをリカバリできます。

以前のバージョン機能を使用すると、ストレージ管理者の手を借りなくても、一連のSnapshotコピーを参照したり、Snapshotコピーからデータをリストアしたりできます。以前のバージョン機能は、任意に設定することはできず、常に有効になります。ユーザは、ストレージ管理者がSnapshotコピーを共有で使用できるようにしたあとに、以前のバージョン機能を使用して次の作業を実行できます。

- 誤って削除したファイルをリカバリする。
- 誤って上書きしたファイルをリカバリする。
- 作業中にファイルのバージョンを比較する。

Snapshotコピーに格納されたデータは読み取り専用です。ファイルに変更を加えるときは、ファイルのコピーを別の場所に保存する必要があります。Snapshotコピーは定期的に削除されるため、前のバージョンのファイルを残しておく場合は、以前のバージョン機能で格納されたファイルのコピーを作成しておく必要があります。

## Microsoftの以前のバージョン機能を使用するための要件

CIFSサーバでMicrosoftの以前のバージョン機能を使用する前に、この機能をサポートするData ONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。また、Snapshotコピーの設定の要件についても確認しておく必要があります。

### Data ONTAPのバージョン要件

[以前のバージョン]は、Data ONTAP 8.2以降でサポートされます。

### SMBプロトコルのバージョン

FlexVolを備えたStorage Virtual Machine(SVM)については、すべてのバージョンのSMBで[以前のバージョン]機能がサポートされます。

Infinite Volumeを備えたSVMについては、SMB 1.0で[以前のバージョン]機能がサポートされます。

## Windowsクライアントの要件

[以前のバージョン]機能を使用してSnapshotコピーのデータにアクセスするには、Windowsクライアントでこの機能がサポートされている必要があります。

[以前のバージョン]機能をサポートするWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix))を参照してください。

## Snapshotコピーの設定の要件

[以前のバージョン]機能を使用してSnapshotコピーのデータにアクセスするには、Snapshotポリシーが有効になっていて、データを含むボリュームに関連付けられている必要があります。また、クライアントからSnapshotのデータにアクセスできること、およびSnapshotコピーが存在することが前提になります。

## [以前のバージョン]タブを使用したSnapshotコピー データの表示および管理

Windowsクライアント マシンでは、Windowsの[プロパティ]ウィンドウの[以前のバージョン]タブを使用してStorage Virtual Machine (SVM) 管理者の手を借りなくても、Snapshotコピーに格納されたデータをユーザがリストアできます。

### タスク概要

SVMに格納されたSnapshotコピーのデータを[以前のバージョン]タブで表示および管理できるのは、管理者が共有を含むボリュームでSnapshotコピーを有効にし、Snapshotコピーを表示するように共有を設定している場合のみです。

### 手順

1. エクスプローラで、CIFSサーバに格納されたデータのマッピングされたドライブの内容を表示します。
2. Snapshotコピーを表示または管理するマッピングされたネットワークドライブのファイルまたはフォルダを右クリックします。
3. [プロパティ]をクリックします。  
選択したファイルまたはフォルダのプロパティが表示されます。
4. [以前のバージョン]タブをクリックします。  
選択したファイルまたはフォルダの利用可能なSnapshotコピーの一覧が[フォルダーのバージョン]ボックスに表示されます。一覧に表示されたSnapshotコピーは、Snapshotコピー名のプレフィックスと作成時のタイムスタンプで識別できます。
5. [フォルダーのバージョン]ボックスで、管理作業を行うファイルまたはフォルダのコピーを右クリックします。
6. 適切な処理を実行します。

| 状況                       | 操作             |
|--------------------------|----------------|
| Snapshotコピーのデータを表示する     | [開く]をクリックします。  |
| Snapshotコピーのデータのコピーを作成する | [コピー]をクリックします。 |

Snapshotコピーのデータは読み取り専用です。[以前のバージョン]タブの一覧に表示されたファイルやフォルダに変更を加える場合は、変更するファイルおよびフォルダのコピーを書き込み可能な場所に保存してから、そのコピーに対して変更を行う必要があります。

7. Snapshotのデータの管理作業が終了したら、[OK]をクリックして[プロパティ]ダイアログ ボックスを閉じます。

[以前のバージョン]タブを使用したSnapshotのデータの表示と管理の詳細については、Microsoft TechNetライブラリを参照してください。

## 関連情報

[Microsoft TechNetライブラリ: technet.microsoft.com/ja-jp/library/](http://technet.microsoft.com/ja-jp/library/)

## Snapshotコピーが以前のバージョン機能で利用できるかどうかの確認

[以前のバージョン]タブからSnapshotコピーを表示できるのは、共有を格納しているボリュームに有効なSnapshotポリシーが適用されている場合、およびボリューム設定でSnapshotコピーへのアクセスを許可している場合のみです。Snapshot コピーの使用可否を確認すると、以前のバージョン機能を使用してアクセス可能かどうか確認できます。

## 手順

1. 共有データが存在するボリュームでSnapshotコピーが自動的に有効になるかどうか、およびクライアントがSnapshotディレクトリにアクセスできるかどうかを確認します。

```
volume show -vserver vs1 -volume volume-name -fields
vserver, volume, snapdir-access, snapshot-policy, snapshot-count
```

出力には、ボリュームに関連付けられているSnapshotポリシー、クライアントのSnapshotディレクトリ アクセスが有効かどうか、および使用可能なSnapshotコピーの数が表示されます。

2. 関連付けられているSnapshotポリシーが有効かどうかを確認します。

```
volume snapshot policy show -policy policy-name
```

3. 使用可能なSnapshotコピーの一覧を表示します。

```
volume snapshot show -volume volume_name
```

SnapshotポリシーおよびSnapshotスケジュールの設定と管理の詳細については、『*clustered Data ONTAP データ保護ガイド*』を参照してください。

## 例

次の例では、「data1」という名前のボリュームに関連付けられたSnapshotポリシーに関する情報を表示します。これには、「data1」上の共有データと使用可能なSnapshotコピーが含まれます。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver, volume, snapdir-access, snapdir-access, snapshot-policy, snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
Policy Name      Number of Is
                  Schedules Enabled Comment
-----
default                3 true    Default policy with hourly, daily &
weekly schedules.
Schedule      Count      Prefix      SnapMirror Label
-----
hourly         6      hourly      -
daily          2      daily       daily
weekly         2      weekly      weekly

cluster1::> volume snapshot show -volume data1
Vserver  Volume  Snapshot                                State      Size  ---Blocks---
-----
vs1      data1
          weekly.2012-12-16_0015         valid      408KB    0%    1%
          daily.2012-12-22_0010         valid      420KB    0%    1%
          daily.2012-12-23_0010         valid      192KB    0%    0%
```

|                        |       |       |    |    |
|------------------------|-------|-------|----|----|
| weekly.2012-12-23_0015 | valid | 360KB | 0% | 1% |
| hourly.2012-12-23_1405 | valid | 196KB | 0% | 0% |
| hourly.2012-12-23_1505 | valid | 196KB | 0% | 0% |
| hourly.2012-12-23_1605 | valid | 212KB | 0% | 0% |
| hourly.2012-12-23_1705 | valid | 136KB | 0% | 0% |
| hourly.2012-12-23_1805 | valid | 200KB | 0% | 0% |
| hourly.2012-12-23_1905 | valid | 184KB | 0% | 0% |

## 関連タスク

[以前のバージョン機能のアクセスを有効にするSnapshot設定の作成](#)(326ページ)

## 以前のバージョン機能のアクセスを有効にするSnapshot設定の作成

Snapshotコピーへのクライアント アクセスが有効であり、Snapshotコピーが存在する場合は、常に以前のバージョン機能を使用できます。Snapshotコピーの設定がこれらの要件を満たしていない場合は、要件を満たすようにSnapshotコピーの設定を作成できます。

### 手順

1. 以前のバージョン機能からのアクセスを許可する共有が格納されているボリュームに、Snapshotポリシーが関連付けられていない場合は、`volume modify`コマンドを使用して、Snapshotポリシーをボリュームに関連付け、ポリシーを有効にします。  
  
`volume modify`コマンドの使用の詳細については、マニュアル ページを参照してください。
2. `volume modify`コマンドを使用して`-snap-dir`オプションを`true`に設定することで、Snapshotコピーへのアクセスを有効にします。  
  
`volume modify`コマンドの使用の詳細については、マニュアル ページを参照してください。
3. `volume show`コマンドと`volume snapshot policy show`コマンドを使用して、Snapshotポリシーが有効になっていること、およびSnapshotディレクトリへのアクセスが有効になっていることを確認します。  
  
`volume show`コマンドと`volume snapshot policy show`コマンドの使用の詳細については、マニュアル ページを参照してください。  
  
SnapshotポリシーとSnapshotスケジュールの設定および管理の詳細については、*clustered Data ONTAP データ保護ガイド*を参照してください。

## ジャンクションを含むディレクトリをリストアする場合の考慮事項

以前のバージョンを使用して、ジャンクション ポイントを含むフォルダをリストアする場合は、一定の考慮事項について理解しておく必要があります。

以前のバージョンを使用して、ジャンクション ポイントである子フォルダを含むフォルダをリストアすると、Access Deniedエラーでリストアが失敗することがあります。

リストアしようとしているフォルダにジャンクションが含まれているかどうかを確認するには、`-parent`オプションを指定して`vol show`コマンドを実行します。また、`vserver security trace`コマンドを使用して、ファイルおよびフォルダのアクセス問題に関する詳細なログを作成することもできます。

### 関連コンセプト

[NASネームスペースでのデータ ボリュームの作成と管理](#)(150ページ)

## CIFSサーバベースのサービスの導入

CIFS環境の機能強化に役立つさまざまなCIFSサーバベースのサービスを導入できます。CIFSサーバベースのサービスには、動的ホーム ディレクトリ、UNIXシンボリックリンクへのSMBアクセス、BranchCacheのリモート オフィス キャッシュ、自動ノード リファラール、ODXコピー オフロード、Access-Based Enumeration (ABE; アクセスベースの列挙)を使用したフォルダのセキュリティなどがあります。

### ホーム ディレクトリの管理

Data ONTAPホーム ディレクトリの機能を使用すると、CIFSサーバ上にユーザのホーム ディレクトリを作成し、各ユーザにホーム ディレクトリの動的共有を自動的に割り当てることができます。これにより、ユーザごとに個別のSMB共有を作成する必要がなくなります。

#### clustered Data ONTAPにおける動的ホーム ディレクトリの仕組み

clustered Data ONTAPのホーム ディレクトリを使用すると、SMB共有を設定し、ユーザと一連の変数に基づいてさまざまなディレクトリにマッピングすることができます。ユーザごとに別個の共有を作成する必要はありません。1つの共有を設定し、いくつかのホーム ディレクトリ パラメータを指定して、エントリ ポイント(共有)とユーザのホーム ディレクトリ(Storage Virtual Machine (SVM) 上のディレクトリ)間の関係をユーザ単位で定義します。

ユーザとディレクトリのマッピング方法を指定する4つの変数があります。

##### 共有名

作成する共有の名前で、ユーザの接続先です。この共有にはホーム ディレクトリのプロパティを設定する必要があります。

共有名には、次の動的な名前を使用できます。

- %w(ユーザのWindowsユーザ名)
- %d(ユーザのWindowsドメイン名)
- %u(ユーザのマッピングされたUNIXユーザ名)

すべてのホーム ディレクトリ間で一意になるようにするため、シェア名には%wまたは%u変数を使用する必要があります。シェア名には%d変数と%w 変数の両方を使用することでも(%d/%wなど)、または固定部分と変数部分で構成することも(home\_%wなど)できます。

##### 共有パス

共有によって定義される、つまり、共有名の1つに関連付けられる相対パスです。各検索パスに付加されて、SVMのルートからのユーザのホーム ディレクトリの完全パスを生成します。静的(例:home)、動的(例:%w)、またはこの2つの組み合わせ(例:eng/%w)で指定できます。

##### 検索パス

SVMのルートからの絶対パスのセットで、clustered Data ONTAPではこのパスに基づいてホーム ディレクトリが検索されます。vserver cifs home-directory search-path addコマンドを使用して1つ以上の検索パスを指定します。複数の検索パスを指定すると、有効なパスが見つかるまで、指定された順で各検索パスが試行されます。

##### ディレクトリ

ユーザに対して作成する、そのユーザのホーム ディレクトリです。通常はユーザ名です。検索パスによって定義されるディレクトリの1つに作成する必要があります。



たとえば、次のように設定します。

- ユーザ: John Smith
- ユーザのドメイン: acme
- ユーザ名: jsmith
- SVM名: vs1
- ホーム ディレクトリ共有名#1: home\_%w - 共有パス: %w
- ホーム ディレクトリ共有名#2: %w - 共有パス: %d/%w
- 検索パス#1: /aggr0home/home
- 検索パス#2: /aggr1home/home
- 検索パス#3: /aggr2home/home
- ホーム ディレクトリ: /aggr1home/home/jsmith

シナリオ1: ユーザは\\vs1\home\_jsmithに接続します。これは最初のホーム ディレクトリ共有名に一致し、相対パスjsmithが生成されます。各検索パスが順に確認され、jsmithという名前のディレクトリが検索されます。

- /aggr0home/home/jsmithは存在しないので、検索パス#2に進みます。
- /aggr1home/home/jsmithは存在します。したがって、検索パス#3は確認されません。これでユーザは自分のホーム ディレクトリに接続されました。

シナリオ2: ユーザが\\vs1\jsmithに接続します。これは、2番目のホーム ディレクトリの共有名に一致し、相対パスacme/jsmithが生成されます。各検索パスが順に確認され、acme/jsmithという名前のディレクトリが検索されます。

- /aggr0home/home/acme/jsmithは存在しないので、検索パス#2に進みます。
- /aggr1home/home/acme/jsmithは存在しないので、検索パス#3に進みます。
- /aggr2home/home/acme/jsmithも存在しません。ホーム ディレクトリが存在しないため、接続は失敗します。

#### 関連タスク

[ホーム ディレクトリ共有の追加](#) (328ページ)

[ホーム ディレクトリ検索パスの追加](#) (330ページ)

[%w変数と%d変数を使用したホーム ディレクトリ設定の作成](#) (331ページ)

[%u変数を使用したホーム ディレクトリの設定](#) (333ページ)

## ホーム ディレクトリ共有の追加

SMBホーム ディレクトリ機能を使用する場合、共有プロパティにホーム ディレクトリ プロパティを含む共有を少なくとも1つ追加する必要があります。

#### タスク概要

ホーム ディレクトリ共有を作成する場合、新規作成するときはvserver cifs share createコマンドを使用します。既存の共有を利用する場合は、vserver cifs share modifyコマンドを使用すれば、いつでも変更することができます。

ホーム ディレクトリ共有を作成する場合、共有を作成または変更するときにhomedirectory値を-share-propertiesオプションに指定する必要があります。共有名と共有パスは変数を使用して



指定できます。変数はユーザがそれぞれのホーム ディレクトリに接続するときに動的に変換されます。パスに使用できる変数は、%w(Windowsのユーザ名)、%d(ドメイン)、および%u(マッピングされたUNIXのユーザ名)です。

## 手順

### 1. ホーム ディレクトリ共有を追加します。

```
vserver cifs share create -vserver vserver -share-name share_name -path path -share-properties homedirectory[,...]
```

-vserver *vserver*には、検索パスを追加するCIFS対応のStorage Virtual Machine(SVM)を指定します。

-share-name *share\_name*には、ホーム ディレクトリ共有名を指定します。

必須の変数に加えて%w、%u、または%dのいずれかのリテラル文字列も共有名に含める場合は、リテラル文字列の先頭に%(パーセント)文字を付けて変数として処理されないようにする必要があります(例:%w)。

- 共有名には、%wまたは%uのどちらかの変数を含める必要があります。
- さらに%d変数(例:%d/%w)または固定要素(例:home1\_%w)を含めることができます。
- 管理者が、他のユーザのホーム ディレクトリに接続するために、またはユーザが他のユーザのホーム ディレクトリに接続するのを許可するために共有を使用する場合は、動的な共有名のパターンの先頭にチルダ(~)を付ける必要があります。  
このアクセスを有効にするには、vserver cifs home-directory modifyを使用して、-is-home-dirs-access-for-admin-enabledオプションをtrueに設定するか、advanced オプション-is-home-dirs-access-for-public-enabledをtrueに設定します。

-path *path*には、ホーム ディレクトリの相対パスを指定します。

-share-properties **homedirectory**[,...]は、その共有の共有プロパティを指定します。**homedirectory**の値を指定する必要があります。追加の共有プロパティをカンマで区切って指定できます。

### 2. vserver cifs share showコマンドを使用して、ホーム ディレクトリ共有が追加されたことを確認します。

#### 例

次のコマンドを実行すると、%wという名前のホーム ディレクトリ共有が作成されます。**homedirectory**共有プロパティに加えて、**oplocks**、**browsable**、**changenotify**の各共有プロパティも設定しています。

**注:** この例で表示されているのは、SVMの共有の出力の一部です。出力は省略されています。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w -share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vserver cifs share show -vserver vs1
Vserver   Share   Path   Properties   Comment   ACL
-----
vs1       %w      %w      oplocks      -          Everyone / Full
Control
          browsable
          changenotify
          homedirectory
```

## 関連コンセプト

[clustered Data ONTAPにおける動的ホーム ディレクトリの仕組み](#)(327ページ)

[自動ノードリファールを使用する際の要件と考慮事項](#)(374ページ)

## 関連タスク

[CIFSサーバでのSMB共有の作成](#)(180ページ)

[ホーム ディレクトリ検索パスの追加](#)(330ページ)

[ユーザのホーム ディレクトリへのアクセスの管理](#)(337ページ)

## ホーム ディレクトリ共有での一意なユーザ名の要件

%w(Windowsユーザ名)変数または%u(UNIXユーザ名)変数を使用してホーム ディレクトリ共有を動的に生成するときは、一意なユーザ名を割り当てるように注意してください。共有名はユーザ名にマッピングされます。

静的共有名とユーザ名が同じである場合、次の2つの問題が起きる可能性があります。

- ユーザがnet viewコマンドを使用してクラスタ上の共有の一覧を表示すると、同じユーザ名が付いた2つの共有が表示されます。
- ユーザがその共有名に接続すると、常に静的共有に接続され、同じ名前のホーム ディレクトリ共有にはアクセスできません。

たとえば、「administrator」という名前の共有があり、ユーザのWindowsユーザ名が「administrator」だとします。ユーザがホーム ディレクトリ共有を作成してその共有に接続すると、自分の「administrator」ホーム ディレクトリ共有ではなく、「administrator」静的共有に接続されます。

共有名の重複の問題を解決するには、次のいずれかの手順を実行します。

- 静的共有の名前を変更し、ユーザのホーム ディレクトリ共有と競合しないようにします。
- ユーザに新しいユーザ名を割り当て、静的共有名と競合しないようにします。
- %wパラメータを使用する代わりに、「home」などの静的な名前を使用してCIFSホーム ディレクトリ共有を作成し、共有名との競合を回避します。

## アップグレード後に静的ホーム ディレクトリ共有名が受ける影響

clustered Data ONTAP 8.3以降では、ホーム ディレクトリ共有名が動変数%wまたは%uを含む必要があります。新しい要件があるclustered Data ONTAPのバージョンにアップグレードした後、既存の静的ホーム ディレクトリ共有名が受ける影響について認識しておく必要があります。

ホーム ディレクトリ構成に静的共有名が含まれており、clustered Data ONTAP 8.3以降にアップグレードする場合、静的ホーム ディレクトリ共有名は変更されませんが、共有は有効なままになります。ただし、変数%wと%uをどちらも含まない新しいホーム ディレクトリ共有は作成できません。

ユーザのホーム ディレクトリ共有名にどちらかの変数を含めるという必須条件によって、すべての共有名がホーム ディレクトリ構成全体で一意であることが保証されます。必要に応じて、静的ホーム ディレクトリ共有名を変数%wまたは%uを含むように変更することができます。

## ホーム ディレクトリ検索パスの追加

Data ONTAPのSMBホーム ディレクトリを使用する場合は、ホーム ディレクトリ検索パスを少なくとも1つ追加する必要があります。

### タスク概要

ホーム ディレクトリ検索パスを追加するには、vserver cifs home-directory search-path addコマンドを使用します。

`vserver cifs home-directory search-path add`コマンドでは、コマンドの実行時に`-path`オプションで指定したパスがチェックされます。指定したパスが存在しない場合は、続行するかどうを確認するメッセージが表示されます。`y`または`n`を選択します。`y`を選択して続行すると、Data ONTAPによって検索パスが作成されます。ただし、ホーム ディレクトリの設定で検索パスを使用するには、あらかじめディレクトリ構造を作成しておく必要があります。`n`を選択して続行しない場合、コマンドは失敗し、検索パスは作成されません。その場合は、パス ディレクトリ構造を作成してから`vserver cifs home-directory search-path add`コマンドを再実行できます。

#### 手順

1. 次のコマンドを入力して、ホーム ディレクトリ検索パスを追加します。  
**`vserver cifs home-directory search-path add -vserver vserver -path path`**  
`-vserver vserver`には、検索パスを追加するCIFS対応のStorage Virtual Machine (SVM)を指定します。  
`-path path`では、検索パスへのディレクトリ パスを指定します。
2. `vserver cifs home-directory search-path show`コマンドを使用して、検索パスが正常に追加されたことを確認します。

#### 例

次の例では、SVM `vs1`でホーム ディレクトリの設定にパス`/home1`を追加します。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1
-path /home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

次の例では、SVM `vs1`でホーム ディレクトリの設定にパス`/home2`を追加することを試みます。このパスは存在しません。続行しないように選択します。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1
-path /home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

#### 関連コンセプト

[clustered Data ONTAPにおける動的ホーム ディレクトリの仕組み](#) (327ページ)

#### 関連タスク

[ホーム ディレクトリ共有の追加](#) (328ページ)

### %w変数と%d変数を使用したホーム ディレクトリ設定の作成

%w変数と%d変数を使用して、ホーム ディレクトリの設定を作成できます。これにより、ユーザは、動的に作成された共有を使用して、ホーム ディレクトリ共有に接続できます。

#### 手順

1. オプション: 次のコマンドを入力して、ユーザのホーム ディレクトリを含むqtreeを作成します。

```
volume qtree create -vserver vsriver_name -qtree-path qtree_path
```

2. オプション: 次のコマンドを入力して、正しいセキュリティ形式がqtreeで使用されていることを確認します。

```
volume qtree show
```

3. オプション: 適切なセキュリティ形式がqtreeで使用されていない場合は、volume qtree securityコマンドを使用してセキュリティ形式を変更します。

4. 次のコマンドを入力して、ホーム ディレクトリ共有を追加します。

```
vserver cifs share create -vserver vsriver -share-name %w -path %d/%w -share-properties homedirectory[,...]
```

-vserver vsriverには、検索パスを追加するCIFS対応のStorage Virtual Machine(SVM)を指定します。

-share-name %wは、ホーム ディレクトリ共有名を指定します。ユーザがホーム ディレクトリに接続すると、ユーザごとに共有名が動的に作成されます。共有名はwindows\_user\_nameの形式になります。

-path %d/%wは、ホーム ディレクトリの相対パスを指定します。ユーザがホーム ディレクトリに接続すると、ユーザごとにdomain/windows\_user\_nameの形式で相対パスが動的に作成されます。

-share-properties homedirectory[,...]は、その共有の共有プロパティを指定します。homedirectoryの値を指定する必要があります。追加の共有プロパティをカンマで区切って指定できます。

5. vsriver cifs share showコマンドを使用して、共有の設定が適切であることを確認します。

6. 次のコマンドを入力して、ホーム ディレクトリ検索パスを追加します。

```
vserver cifs home-directory search-path add -vserver vsriver -path path
```

-vserver vsriverには、検索パスを追加するCIFS対応のSVMを指定します。

-path pathには、検索パスの絶対ディレクトリパスを指定します。

7. vsriver cifs home-directory search-path showコマンドを使用して、検索パスが正常に追加されたことを確認します。

8. ユーザにホーム ディレクトリがある場合は、ホーム ディレクトリを含むように指定したqtreeまたはボリュームに対応するディレクトリを作成します。

たとえば、/vol/vol1/usersというパスのqtreeを作成した場合に、ディレクトリの作成対象となるユーザのユーザ名がmydomain\user1であるときは、/vol/vol1/users/mydomain/user1というパスを使用してディレクトリを作成します。

/home1にマウントされる「home1」という名前のボリュームを作成した場合は、/home1/mydomain/user1というパスを使用してディレクトリを作成します。

9. ドライブをマッピングするか、UNCパスを使用して、ユーザがホーム ディレクトリ共有に正常に接続できることを確認します。

たとえば、ユーザmydomain\user1が、SVM vs1上にあるディレクトリ(手順8で作成)に接続する場合は、UNCパス\\vs1\user1を使用して接続します。

#### 例

次の例のコマンドでは、以下の設定を使用してホーム ディレクトリの設定を作成します。

- 共有名は%w

- 相対ホーム ディレクトリ パスは%d/%w
- ホーム ディレクトリ/home1を含むように指定した検索パスは、NTFSセキュリティ形式で設定されたボリューム
- 設定はSVM vs1上に作成

ユーザがWindowsホストからホーム ディレクトリにアクセスする場合には、このようなホーム ディレクトリの設定を使用できます。また、ユーザがWindowsホストとUNIXホストからホーム ディレクトリにアクセスし、ファイルシステム管理者がWindowsベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合にも、このような設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %d/%w
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

          Vserver: vs1
          Share: %w
CIFS Server NetBIOS Name: VS1
          Path: %d/%w
    Share Properties: oplocks
                     browsable
                     changenotify
                     homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /
home1

cluster::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1          /home1
```

## 関連コンセプト

[追加のホーム ディレクトリの設定](#)(336ページ)

## 関連タスク

[%u変数を使用したホーム ディレクトリの設定](#)(333ページ)

[SMBユーザのホーム ディレクトリパスに関する情報の表示](#)(337ページ)

## %u変数を使用したホーム ディレクトリの設定

ホーム ディレクトリの設定を作成する際、%w変数を使用して共有名を指定し、%u変数を使用してホーム ディレクトリ共有の相対パスを指定することができます。これにより、ユーザは、ホーム ディレクトリの実際の名前やパスを意識することなく、Windowsユーザ名を使用して動的に作成された共有を利用するホーム ディレクトリ共有に接続できます。

## 手順

1. オプション: 次のコマンドを入力して、ユーザのホーム ディレクトリを含むqtreeを作成します。

```
volume qtree create -vserver vserver_name -qtree-path qtree_path
```

2. オプション: 次のコマンドを入力して、正しいセキュリティ形式がqtreeで使用されていることを確認します。

```
volume qtree show
```

3. オプション: 適切なセキュリティ形式がqtreeで使用されていない場合は、`volume qtree security`コマンドを使用してセキュリティ形式を変更します。

4. 次のコマンドを入力して、ホーム ディレクトリ共有を追加します。

```
vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory,...
```

-vserver *vserver*には、検索パスを追加するCIFS対応のStorage Virtual Machine(SVM)を指定します。

-share-name *%w*は、ホーム ディレクトリ共有名を指定します。ユーザがホーム ディレクトリに接続すると、ユーザごとに*windows\_user\_name*の形式で共有名が動的に作成されます。

注: -share-nameオプションに*%u*変数を使用することもできます。これにより、マッピング先のUNIXユーザ名を使用して相対共有パスが作成されます。

-path *%u*は、ホーム ディレクトリの相対パスを指定します。ユーザがホーム ディレクトリに接続すると、ユーザごとに*mapped\_UNIX\_user\_name*の形式で共有名が動的に作成されます。

注: このオプションの値には静的な要素を含めることもできます。たとえば、*eng/%u*のように指定できます。

-share-properties *homedirectory[, ...]*は、その共有の共有プロパティを指定します。*homedirectory*の値を指定する必要があります。追加の共有プロパティをカンマで区切って指定できます。

5. `vserver cifs share show`コマンドを使用して、共有の設定が適切であることを確認します。

6. 次のコマンドを入力して、ホーム ディレクトリ検索パスを追加します。

```
vserver cifs home-directory search-path add -vserver vserver -path path
```

-vserver *vserver*には、検索パスを追加するCIFS対応のSVMを指定します。

-path *path*には、検索パスの絶対ディレクトリパスを指定します。

7. `vserver cifs home-directory search-path show`コマンドを使用して、検索パスが正常に追加されたことを確認します。

8. オプション: UNIXユーザが存在しない場合は、`vserver services unix-user create`コマンドを使用してUNIXユーザを作成します。

注: ユーザをマッピングするには、Windowsユーザ名のマッピング先となるUNIXユーザ名があらかじめ存在している必要があります。

9. オプション: 次のコマンドを使用して、UNIXユーザへのWindowsユーザのネーム マッピングを作成します。

```
vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name
```

注: WindowsユーザをUNIXユーザにマッピングするネーム マッピングがすでに存在する場合は、このマッピング手順を実行する必要はありません。

Windowsユーザ名は対応するUNIXユーザ名にマッピングされます。Windowsユーザは、ホーム ディレクトリ共有に接続すると、Windowsユーザ名に対応する共有名を使用して動的に作成されたホーム ディレクトリに接続することになります。その際、ディレクトリ名がUNIXユーザ名に対応していることはユーザにはわかりません。

10. ユーザにホーム ディレクトリがある場合は、ホーム ディレクトリを含むように指定したqtreeまたはボリュームに対応するディレクトリを作成します。

たとえば、/vol/vol1/usersというパスのqtreeを作成した場合に、ディレクトリの作成対象となるユーザのマッピング先UNIXユーザ名が「unixuser1」であるときは、/vol/vol1/users/unixuser1というパスを使用してディレクトリを作成します。

「/home1」にマウントされるhome1という名前のボリュームを作成した場合は、/home1/unixuser1というパスを使用してディレクトリを作成します。

11. ドライブをマッピングするか、UNCパスを使用して、ユーザがホーム ディレクトリ共有に正常に接続できることを確認します。

たとえば、UNIXユーザunixuser1にマッピングされるユーザmydomain\user1が、SVM vs1上にあるディレクトリ(手順10で作成)に接続する場合は、UNCパス\\vs1\user1を使用して接続します。

### 例

次の例のコマンドでは、以下の設定を使用してホーム ディレクトリの設定を作成します。

- 共有名は%w
- 相対ホーム ディレクトリ パスは%uです。
- ホーム ディレクトリ/home1を含めるために使用する検索パスは、UNIXセキュリティ形式で設定されるボリュームです。
- 設定はSVM vs1上に作成

ユーザがWindowsホストから、またはWindowsホストとUNIXホストからホーム ディレクトリにアクセスし、ファイルシステム管理者がUNIXベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合には、このようなホーム ディレクトリの設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

          Vserver: vs1
          Share: %w
CIFS Server NetBIOS Name: VS1
          Path: %u
    Share Properties: oplocks
                     browsable
                     changenotify
                     homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /
home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver      Position Path
-----
vs1          1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
```

| Vserver | Direction | Position |                                          |
|---------|-----------|----------|------------------------------------------|
| -----   | -----     | -----    |                                          |
| vs1     | win-unix  | 5        | Pattern: user1<br>Replacement: unixuser1 |

## 関連コンセプト

[追加のホーム ディレクトリの設定](#)(336ページ)

## 関連タスク

[%w変数と%d変数を使用したホーム ディレクトリ設定の作成](#)(331ページ)

[SMBユーザのホーム ディレクトリパスに関する情報の表示](#)(337ページ)

## 追加のホーム ディレクトリの設定

%w、%d、および%u変数を使用して追加のホーム ディレクトリの設定を作成することで、ニーズに合わせてホーム ディレクトリの設定をカスタマイズできます。

共有名と検索パスで変数と静的文字列の組み合わせを使用して、多数のホーム ディレクトリの設定を作成できます。次の表に、さまざまなホーム ディレクトリの設定を作成する例を示します。

| /vol1/userにホーム ディレクトリを含める場合に作成するパス                                    | 共有コマンド                                                                                                                      |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| ユーザを/vol1/user/win_usernameに転送する共有パス\\vs1\~win_usernameを作成する場合        | <b>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,home directory</b>   |
| ユーザを\\vs1\win_usernameに転送する共有パス /vol1/user/domain/win_usernameを作成する場合 | <b>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,home directory</b> |
| ユーザを\\vs1\win_usernameに転送する共有パス /vol1/user/unix_usernameを作成する場合       | <b>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,home directory</b>    |
| ユーザを\\vs1\unix_usernameに転送する共有パス /vol1/user/unix_usernameを作成する場合      | <b>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,home directory</b>    |

## 検索パスの管理用コマンド

CIFSホーム ディレクトリの設定の検索パスを管理するためにコマンドが存在します。たとえば、検索パスに関する情報を追加、削除、表示するためのコマンドがあります。また、検索パスの順序を変更するためのコマンドもあります。

| 状況        | 使用するコマンド                                            |
|-----------|-----------------------------------------------------|
| 検索パスを追加する | <b>vserver cifs home-directory search-path add</b>  |
| 検索パスを表示する | <b>vserver cifs home-directory search-path show</b> |



| 状況           | 使用するコマンド                                                     |
|--------------|--------------------------------------------------------------|
| 検索パスの順序を変更する | <code>vserver cifs home-directory search-path reorder</code> |
| 検索パスを削除する    | <code>vserver cifs home-directory search-path remove</code>  |

詳細については、各コマンドのマニュアル ページを参照してください。

## SMBユーザのホーム ディレクトリ パスに関する情報の表示

Storage Virtual Machine (SVM) 上のSMBユーザのホーム ディレクトリ パスを表示できます。これは、複数のCIFSホーム ディレクトリ パスが設定されている場合に、ユーザのホーム ディレクトリが含まれるパスを確認するときに役立ちます。

### 手順

1. `vserver cifs home-directory show-user`コマンドを使用して、ホーム ディレクトリ パスを表示します。

### 例

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

| Vserver | User  | Home Dir Path |
|---------|-------|---------------|
| -----   | ----- | -----         |
| vs1     | user1 | /home/user1   |

### 関連タスク

[ユーザのホーム ディレクトリへのアクセスの管理](#) (337ページ)

## ユーザのホーム ディレクトリへのアクセスの管理

デフォルトでは、ユーザのホーム ディレクトリはそのユーザとWindows管理者のみアクセスできます。動的な共有名の前にチルダ(~)が付いている共有の場合、Windows管理者や他のユーザ(パブリック アクセス)によるユーザのホーム ディレクトリへのアクセスを有効または無効にできます。

### 開始する前に

Storage Virtual Machine (SVM) のホーム ディレクトリ共有に、動的な共有名の前にチルダ(~)を追加した共有名を設定する必要があります。共有名の要件は次のとおりです。

| ホーム ディレクトリの共有名      | 共有に接続するコマンドの例                                                       |
|---------------------|---------------------------------------------------------------------|
| <code>~%d~%w</code> | <code>net use * //IPAddress/<br/>~domain-user /u:credentials</code> |
| <code>~%w</code>    | <code>net use * //IPAddress/~user /<br/>u:credentials</code>        |
| <code>abc~%w</code> | <code>net use * //IPAddress/abc-user /<br/>u:credentials</code>     |

### 手順

1. 適切な処理を実行します。

| ユーザのホーム ディレクトリへのアクセスを有効化または無効化する対象 | 入力するコマンド                                                                                                                                                                                                                                                                                                  |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows管理者                         | <pre>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-admin-enabled {true false}</pre> <p>デフォルトはtrueです。</p>                                                                                                                                                              |
| 任意のユーザ(パブリック アクセス)                 | <p>a. 権限レベルをadvancedに設定します。</p> <pre>set -privilege advanced</pre> <p>b. アクセスを有効化または無効化します。</p> <pre>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true false}</pre> <p>デフォルトはfalseです。</p> <p>c. admin権限レベルに戻ります。</p> <pre>set -privilege admin</pre> |

**例**

次の例は、Windows管理者によるユーザのホーム ディレクトリへのアクセスを有効化します。

```
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-admin-enabled false
```

**例**

次の例は、ユーザのホーム ディレクトリへのパブリック アクセスを有効化します。

```
set -privilege advanced
```

```
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public-enabled true
```

```
set -privilege admin
```

**関連タスク**

[SMBユーザのホーム ディレクトリパスに関する情報の表示](#) (337ページ)

## UNIXシンボリック リンクへのSMBクライアント アクセスの設定

SMBクライアントがUNIXシンボリック リンクにアクセスできるようにCIFSサーバを設定できます。シンボリック リンクでは、共有を含むボリューム内のファイル、またStorage Virtual Machine (SVM) 上の他のボリュームに格納されているファイル、あるいは他のSVMに含まれているボリュームも参照できます。

## Data ONTAPを使用してUNIXシンボリック リンクへのSMBクライアント アクセスを提供する方法

Data ONTAPでシンボリック リンクがどのように扱われるかについて、その概念を理解しておく必要があります。Storage Virtual Machine (SVM) に接続しているSMBユーザにシンボリック リンクへのアクセスを提供する際に重要となります。

シンボリック リンクはUNIX環境で作成されるファイルで、別のファイルまたはディレクトリへの参照が含まれます。シンボリック リンクにアクセスしたクライアントは、シンボリック リンクが参照するターゲット ファイルまたはディレクトリにリダイレクトされます。

Data ONTAPには、SMBクライアントがSVMで設定されているUNIXのシンボリック リンクをたどるための機能が用意されています。この機能は任意で、次の設定のいずれかを使用して、共有ごとに設定できます。

- 読み取り / 書き込みアクセスで有効化
- 読み取り専用アクセスで有効化
- SMBクライアントに対してシンボリック リンクを非表示にして無効化
- SMBクライアントからシンボリック リンクへのアクセス権なしで無効化

シンボリック リンクには次の2つのタイプがあります。

### 相対

相対シンボリック リンクには、親ディレクトリに対して相対的なファイルまたはディレクトリへの参照が含まれています。したがって、参照しているファイルのパスの先頭はスラッシュ(/)ではありません。共有でシンボリック リンクを有効にした場合、相対シンボリック リンクは追加の設定なしで機能します。

### 絶対

絶対シンボリック リンクには、ファイルまたはディレクトリへの参照が絶対パスの形式で含まれています。したがって、参照しているファイルのパスの先頭はスラッシュ(/)です。ファイルシステムのルートからの、ファイルの絶対パスの場所として扱われます。絶対シンボリック リンクは、シンボリック リンクのファイルシステム内外のファイルまたはディレクトリを参照できます。ターゲットが同じローカル ファイルシステムにないシンボリック リンクは、**ワイドリンク**と呼ばれます。共有でシンボリック リンクを有効にただけでは、絶対シンボリック リンクは機能しません。最初に、シンボリック リンクのUNIXパスからデスティネーションCIFSパスへのマッピングを作成する必要があります。絶対シンボリック リンクのマッピングを作成する場合、ローカル リンクかワイドリンクかを指定します。ローカル共有外のファイルまたはディレクトリへの絶対シンボリック リンクを作成しても、局所性をローカルに設定すると、Data ONTAPはターゲットへのアクセスを許可しません。

クライアントがローカル シンボリック リンク(絶対または相対)を削除しようとした場合、シンボリック リンクのみが削除され、ターゲット ファイルまたはターゲット ディレクトリは削除されません。それに対して、クライアントがワイドリンクを削除しようとした場合には、ワイドリンクが参照する実際のターゲット ファイルやターゲット ディレクトリが削除されることがあります。クライアントはSVM外のターゲット ファイルまたはディレクトリを明示的に開いて削除できるため、Data ONTAPではこの操作を制御できません。

### 関連コンセプト

[SMB共有の作成時に必要な情報](#)(179ページ)

## SMBアクセス用にUNIXシンボリック リンクを設定する場合の制限

SMBアクセス用にUNIXシンボリック リンクを設定する際は、一定の制限事項を理解しておく必要があります。

| 最大値 | 説明                                                                                                                              |
|-----|---------------------------------------------------------------------------------------------------------------------------------|
| 45  | CIFSサーバ名のFQDNを使用して指定できるCIFSサーバ名の最大文字数。<br>注: 代わりに、CIFSサーバ名をNetBIOS名として指定できますが、その場合は15文字に制限されます。                                 |
| 80  | 共有名の最大文字数。                                                                                                                      |
| 256 | UNIXパスのシンボリック リンクの作成時、または既存のシンボリック リンクの変更時に指定できるパスの最大文字数。<br>UNIXパスは「/」(スラッシュ)で開始し、「/」で終了する必要があります。先頭と末尾のスラッシュは、256文字の制限に含まれます。 |
| 256 | CIFSパスのシンボリック リンクの作成時、または既存のシンボリック リンクの変更時に指定できるパスの最大文字数。<br>CIFSパスは「/」で開始し、「/」で終了する必要があります。先頭と末尾のスラッシュは、256文字の制限に含まれます。        |

### 関連タスク

[SMB共有のシンボリック リンク マッピングの作成](#)(343ページ)

## CIFSサーバ オプションを使用してclustered Data ONTAPでDFSの自動通知を制御する方法

共有に接続するSMBクライアントに対してDFS対応を通知する方法を制御するCIFSサーバ オプションが追加されています。clustered Data ONTAPでは、クライアントがSMB経由でシンボリック リンクにアクセスするときにDFSリファールを使用するため、このオプションを無効または有効にしたときの影響を理解しておく必要があります。

clustered Data ONTAP 8.2～8.2.2では、Storage Virtual Machine(SVM)上のCIFSサーバは、DFSに対応していることを常にSMBクライアントに通知します。ただし、CIFSサーバはDFSに対応していることを常に通知しますが、SMBのシンボリック リンク アクセスは、共有パラメータを設定することによって共有ごとに管理されます。共有パラメータを使用すると、SMBのシンボリック リンク アクセスを次の3つのアクセス レベルのいずれかに設定できます。

- 読み取り / 書き込みアクセスに対して有効
- 読み取り専用アクセスに対して有効
- 無効。このパラメータの値を設定してシンボリック リンクを非表示にするか、パラメータをnull (「 」)に設定

8.2リリース ファミリーのData ONTAP 8.2.3以降およびData ONTAP 8.3以降では、DFSに対応していることをCIFSサーバがSMBクライアントに自動通知するかどうかは、CIFSサーバ オプションで指定します。デフォルトでは、このオプションは有効になっており、CIFSサーバはDFSに対応していることを常にSMBクライアントに(たとえシンボリック リンクへのアクセスが無効になっている共有に接続する場合でも)通知します。シンボリック リンクへのアクセスが有効になっている共有にクライアントが接続する場合にのみ、DFSに対応していることをCIFSサーバがクライアントに通知するようにするには、このオプションを無効にします。

このオプションを無効にすると次のような影響があることに留意してください。

- シンボリックリンクの共有設定は変わりません。
- シンボリックリンクアクセス(読み取り / 書き込みアクセスまたは読み取り専用アクセス)を許可するように共有パラメータが設定されている場合、CIFSサーバは、その共有に接続するクライアントにDFS対応を通知します。  
シンボリックリンクへのクライアントの接続とアクセスは中断せずに続行されます。
- シンボリックリンクアクセスを許可しないように共有パラメータが設定されている場合(アクセスを無効にしているか共有パラメータの値がnullの場合)、CIFSサーバは、その共有に接続するクライアントにDFS対応を通知しません。  
クライアントは、CIFSサーバがDFSに対応しているというキャッシュされた情報を保持しており、CIFSサーバはそのことを通知しなくなるので、シンボリックリンクアクセスが無効になっている共有に接続されたクライアントは、CIFSサーバオプションが無効になったあとでそれらの共有にアクセスできなくなることがあります。オプションが無効になったあとで、それらの共有に接続されたクライアントを再起動し、キャッシュされた情報を消去する必要があります。

これらの変更はSMB 1.0の接続には適用されません。

## CIFSサーバによるDFS対応の自動通知の管理

CIFSサーバオプションを設定して、CIFSサーバが共有に接続するSMB 2.xおよびSMB 3.0クライアントに自動的にDFS対応を通知するかどうかを決定できます。DFS対応を通知する共有に接続しないアプリケーションの場合は、自動通知を無効にすることができます。

### タスク概要

clustered Data ONTAPでは、SMBアクセス用のシンボリックリンクの実装でDFSリファールが使用されます。このオプションを有効または無効にする場合は、次の点に注意する必要があります。

- 自動DFS通知を有効にすると、共有でシンボリックリンクによるCIFSへのアクセスが有効かどうかに関わらず、CIFSサーバはその共有に接続するSMB 2.xおよびSMB 3.0クライアントに常にDFS対応を通知します。  
これがデフォルト設定です。
- 自動DFS通知を無効にすると、CIFSサーバはクライアントがシンボリックリンクアクセス(読み取り / 書き込みアクセスまたは読み取り専用アクセス)が有効になっている共有に接続する場合にのみ、SMB 2.xおよびSMB 3.0クライアントにDFS対応を通知します。シンボリックリンクアクセスが無効になっている共有に接続するクライアントには、DFS対応を通知しません。

シンボリックリンクアクセスが無効になっている共有に接続しているクライアントは、CIFSサーバオプションが無効になるとその共有にアクセスできなくなる可能性があります。これは、クライアントがCIFSサーバがDFS対応であるという情報をキャッシュしているにもかかわらず、サーバがDFSに対応していることを通知しなくなったためです。その結果、SMB共有への再接続が失敗します。これには、次の2つの対応方法があります。

- オプションを無効にする前に、すべての共有で読み取り / 書き込みまたは読み取り専用アクセスのどちらかを許可するように共有設定を変更します。
- シンボリックリンクアクセスが無効になっている共有の設定を変更できない場合は、オプションを無効にしたあとで、共有に接続していて影響を受けたクライアントをすべてリブートしてキャッシュ情報をクリアします。

### 手順

- 権限レベルをadvancedに設定します。  
`set -privilege advanced`
- DFSリファール オプションを設定します。

```
vserver cifs options modify -vserver vserver_name -is-advertise-dfs-enabled {true|false}
```

3. オプションが目的の値に設定されていることを確認します。

```
vserver cifs options show -vserver vserver_name
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

## SMB共有でのUNIXシンボリック リンク サポートの設定

SMB共有の作成時に、または既存のSMB共有の変更によりいつでも、シンボリックリンクの共有プロパティ設定を指定することによって、SMB共有でUNIXシンボリックリンクのサポートを設定できます。UNIXシンボリックリンクのサポートはデフォルトで有効になっています。UNIXシンボリックリンクのサポートを共有で無効にすることもできます。

### タスク概要

SMB共有でUNIXシンボリックリンクのサポートを設定する場合は、次の設定のいずれかを選択できます。

| 設定            | 説明                                                                                     |
|---------------|----------------------------------------------------------------------------------------|
| enable        | 読み取り / 書き込みアクセスに対してシンボリックリンクが有効であることを指定します。これがデフォルト設定です。                               |
| read_only     | 読み取り専用アクセスに対してシンボリックリンクが有効であることを指定します。この設定はワイドリンクには適用されません。ワイドリンクアクセスは常に読み取り / 書き込みです。 |
| hide          | SMBクライアントにシンボリックリンクが表示されないようにします。                                                      |
| "" (null、未設定) | シンボリックリンクを共有で無効にします。                                                                   |
| - (未設定)       | シンボリックリンクを共有で無効にします。                                                                   |

### 手順

1. シンボリックリンク サポートを設定または無効化します。

| 条件       | コマンド                                                                                                                                                |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しいSMB共有 | <pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink-properties {enable hide read_only "" -}, ...]</pre> |
| 既存のSMB共有 | <pre>vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable hide read_only "" -}, ...]</pre>            |

2. SMB共有の設定が正しいことを確認します。

```
vserver cifs share show -vserver vserver_name -share-name share_name -instance
```

#### 例

次のコマンドでは、UNIXシンボリックリンクの設定をenableにして「data1」という名前のSMB共有を作成します。

```
cluster1::> vservers cifs share create -vservers vs1 -share-name data1 -path /
data1 -symlink-properties enable

cluster1::> vservers cifs share show -vservers vs1 -share-name data1 -instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

## 関連タスク

[CIFSサーバでのSMB共有の作成](#) (180ページ)

[SMB共有のシンボリックリンク マッピングの作成](#) (343ページ)

## SMB共有のシンボリックリンク マッピングの作成

SMB共有に対するUNIXシンボリックリンクのマッピングを作成できます。親フォルダに対して相対的なファイルまたはフォルダを参照する相対シンボリックリンクを作成することも、絶対パスを使用してファイルまたはフォルダを参照する絶対シンボリックリンクを作成することもできます。

### タスク概要

SMB 2.xを使用している場合、Mac OS Xクライアントからワイドリンクにアクセスすることはできません。Mac OS Xクライアントからワイドリンクを使用して共有に接続しようすると、接続に失敗します。ただし、SMB 1を使用している場合は、Mac OS Xクライアントでワイドリンクを使用できます。

### 手順

1. SMB共有のシンボリックリンク マッピングを作成するには、次のコマンドを入力します。

```
vservers cifs symlink create -vservers virtual_server_name -unix-path path
-share-name share_name -cifs-path path [-cifs-server server_name] [-
locality {local|widelink}] [-home-directory {true|false}]
```

-vservers *virtual\_server\_name*には、Storage Virtual Machine (SVM) 名を指定します。

-unix-path *path*には、UNIXパスを指定します。UNIXパスは、先頭をスラッシュ(/)にする必要があり、末尾もスラッシュ(/)にする必要があります。

-share-name *share\_name*には、マッピングするSMB共有の名前を指定します。

-cifs-path *path*には、CIFSパスを指定します。CIFSパスは、先頭をスラッシュ(/)にする必要があり、末尾もスラッシュ(/)にする必要があります。

-cifs-server *server\_name*には、CIFSサーバ名を指定します。CIFSサーバ名として指定できるのは、DNS名 (例: mynetwork.cifs.server.com)、IPアドレス、またはNetBIOS名です。NetBIOS名は、vservers cifs showコマンドを使用して確認できます。このオプションのパラメータを指定しない場合、デフォルト値のローカルCIFSサーバのNetBIOS名が使用されます。



-locality {local|widelink}は、ローカル シンボリック リンクとワイドシンボリック リンクのどちらを作成するかを指定します。ローカル シンボリック リンクはローカルSMB共有にマッピングされ、ワイドシンボリック リンクはネットワーク上の任意のSMB共有にマッピングされます。このオプションのパラメータを指定しない場合、デフォルト値のwidelinkが使用されます。

-home-directory {true|false}は、ターゲットの共有がホーム ディレクトリであるかどうかを指定します。このパラメータは省略可能ですが、ターゲットの共有をホーム ディレクトリとして設定する場合は、このパラメータをtrueに設定する必要があります。デフォルトはfalseです。

#### 例

次のコマンドを実行すると、vs1という名前のSVM上にシンボリック リンク マッピングが作成されます。このマッピングは、UNIXパスが/src/、SMB共有名が「SOURCE」、CIFSパスが/mycompany/source/、CIFSサーバのIPアドレスが123.123.123.123で、ワイドリンクです。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/ -share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server 123.123.123.123 -locality widelink
```

#### 関連コンセプト

[Data ONTAPを使用してUNIXシンボリック リンクへのSMBクライアント アクセスを提供する方法](#) (339ページ)

#### 関連タスク

[SMB共有でのUNIXシンボリック リンク サポートの設定](#) (342ページ)

## シンボリック リンクのマッピングの管理用コマンド

シンボリック リンクのマッピングを管理するための、特定のData ONTAPコマンドが存在します。

| 状況                          | 使用するコマンド                    |
|-----------------------------|-----------------------------|
| シンボリック リンクのマッピングを作成する       | vserver cifs symlink create |
| シンボリック リンクのマッピングに関する情報を表示する | vserver cifs symlink show   |
| シンボリック リンクのマッピングを変更する       | vserver cifs symlink modify |
| シンボリック リンクのマッピングを削除する       | vserver cifs symlink delete |

詳細については、各コマンドのマニュアル ページを参照してください。

## BranchCacheを使用したブランチ オフィスでのSMB共有のコンテンツのキャッシュ

BranchCacheは、要求元のクライアントのローカル コンピュータにコンテンツをキャッシュできるようにするためにMicrosoftが開発した機能です。Data ONTAPにBranchCacheを実装すると、Storage Virtual Machine (SVM)に格納されたコンテンツにSMBを使用してブランチ オフィスのユーザがアクセスする際に、Wide-Area Network (WAN; 広域ネットワーク)の使用量を抑え、アクセス応答時間を短縮することができます。

BranchCacheを設定すると、Windows BranchCacheクライアントはまずSVMのコンテンツを取得し、次に取得したコンテンツをブランチ オフィスのコンピュータにキャッシュします。ブランチ オフィスの別のBranchCache対応クライアントが同じコンテンツを要求すると、SVMは最初に要求元ユーザの



認証と許可を実行します。次にSVMは、キャッシュされたコンテンツが最新のものであるかどうかを確認し、最新のものである場合はそのコンテンツに関するメタデータをクライアントに送信します。クライアントは、そのメタデータを使用して、ローカルのキャッシュから直接コンテンツを取得します。

#### 関連コンセプト

[オフライン ファイルを使用したオフラインで使用するファイルのキャッシング](#)(315ページ)

### 要件、考慮事項、および推奨事項

FlexVolを備えたStorage Virtual Machine(SVM)でBranchCache機能を使用する前に、一定の要件、考慮事項、および推奨事項について確認しておく必要があります。たとえば、その機能に対するData ONTAPのサポートについて把握している必要があります。また、SMBのバージョンのサポートやサポートされるWindowsホストについても確認しておかなければなりません。

#### 関連タスク

[CIFSサーバでのBranchCacheの設定](#)(348ページ)

#### BranchCacheのバージョンのサポート

Data ONTAPでサポートされるBranchCacheのバージョンを確認しておく必要があります。

Data ONTAPでは、BranchCache 1と強化されたBranchCache 2がサポートされています。

- Storage Virtual Machine(SVM)のCIFSサーバでBranchCacheを設定する場合、BranchCache 1、BranchCache 2、またはすべてのバージョンを有効にすることができます。  
デフォルトでは、すべてのバージョンが有効になっています。
- BranchCache 2のみを有効にする場合は、リモート オフィスのWindowsクライアント マシンでBranchCache 2がサポートされている必要があります。  
BranchCache 2をサポートするのはSMB 3.0以降のクライアントだけです。

BranchCacheのバージョンの詳細については、Microsoft TechNetライブラリを参照してください。

#### 関連情報

[Microsoft TechNetライブラリ: \*technet.microsoft.com/ja-jp/library/\*](https://technet.microsoft.com/ja-jp/library/)

#### ネットワーク プロトコルのサポート要件

Data ONTAP BranchCacheを実装するときは、ネットワーク プロトコルの要件を考慮する必要があります。

Data ONTAP BranchCache機能は、SMB 2.1以降を使用して、IPv4およびIPv6のネットワークに実装できます。

BranchCacheの実装に含まれるすべてのCIFSサーバとブランチ オフィスのマシンで、SMB 2.1以降のプロトコルを有効にする必要があります。SMB 2.1では、プロトコルの機能拡張により、クライアントをBranchCache環境に含めることができます。SMB 2.1は、BranchCacheをサポートするSMBの最小バージョンです。SMB 2.1は、BranchCacheバージョン1をサポートします。

BranchCacheバージョン2を使用する場合は、サポートするSMBの最小バージョンはSMB 3.0になります。BranchCache 2の実装に含まれるすべてのCIFSサーバとブランチ オフィスのマシンで、SMB 3.0以降を有効にする必要があります。

リモートオフィスでSMB2.1のみサポートするクライアント、SMB3.0をサポートするクライアントが混在する場合は、BranchCache 1とBranchCache 2の両方のキャッシングをサポートするCIFSサーバにBranchCache構成を実装することができます。

**注:** Microsoft BranchCache機能ではファイル アクセス プロトコルとしてHTTP / HTTPSとSMBプロトコルの両方がサポートされますが、Data ONTAP BranchCacheでサポートされるのはSMB 2.1のみです。

### Data ONTAPとWindowsホストのバージョン要件

BranchCacheを設定するには、Data ONTAPやブランチ オフィスのWindowsホストが特定のバージョン要件を満たしている必要があります。

BranchCacheを設定するには、クラスタのData ONTAPのバージョンや対象となるブランチ オフィスのクライアントで、SMB 2.1以降とBranchCacheの機能をサポートしている必要があります。さらに、ホスト型キャッシュ モードを設定する場合は、サポートされるホストをキャッシュ サーバに使用する必要があります。

BranchCache 1は、次のData ONTAPバージョンとWindowsホストでサポートされています。

- コンテンツ サーバ: Data ONTAP 8.2以降を実行しているStorage Virtual Machine (SVM)
- キャッシュ サーバ: Windows Server 2008 R2またはWindows Server 2012以降
- ピアまたはクライアント: Windows 7 Enterprise、Windows 7 Ultimate、Windows 8、Windows Server 2008 R2、またはWindows Server 2012以降

BranchCache 2は、次のData ONTAPバージョンとWindowsホストでサポートされています。

- コンテンツ サーバ: Data ONTAP 8.2以降を実行しているSVM
- キャッシュ サーバ: Windows Server 2012以降
- ピアまたはクライアント: Windows 8またはWindows Server 2012以降

BranchCacheをサポートするWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix)) を参照してください。

### Data ONTAPでBranchCacheハッシュが無効になる理由

Data ONTAPでどのような場合にハッシュが無効になるかを理解すると、BranchCacheの設定を計画するときに役立ちます。この情報に基づいて、設定すべき動作モードの決定と、BranchCacheを有効にする共有を選択するかどうかの検討の助けになります。

Data ONTAPは、BranchCacheハッシュが有効なものであるかを管理しています。有効でないハッシュが見つかったら、そのハッシュは無効化され、次のコンテンツの要求時に新しいハッシュが計算されます (BranchCacheが有効な場合)。

Data ONTAPは、以下の場合にハッシュを無効にします。

- サーバ キーが変更された場合。  
サーバ キーが変更された場合は、ハッシュ ストア内のすべてのハッシュが無効になります。
- BranchCacheのハッシュ ストアの最大サイズに達したために、ハッシュがキャッシュからフラッシュされた場合。  
このパラメータは調整可能で、ビジネス要件に合わせて変更することができます。
- SMBまたはNFS経由のアクセスでファイルが変更された場合。
- 有効なハッシュを持つファイルがsnap restoreコマンドを使用してリストアされた場合。
- BranchCache対応のSMB共有を含むボリュームがsnap restoreコマンドを使用してリストアされた場合。

## ハッシュストアの場所を選択する際の考慮事項

BranchCacheを設定する場合は、ハッシュを格納する場所とハッシュストアのサイズを選択します。ハッシュストアの場所とサイズを選択する際の一定の考慮事項について理解しておく、CIFS対応のStorage Virtual Machine(SVM)でBranchCacheの設定を計画するのに役立ちます。

- ハッシュストアは、atimeアップデートが許可されるボリューム上に配置する必要があります。ハッシュストアでは、ハッシュファイルへのアクセス時間を使用して、アクセス頻度の高いファイルを管理します。atimeアップデートが無効になっている場合、作成時間がこの目的に使用されます。使用頻度の高いファイルを追跡するためにatimeを使用することを推奨します。
- SnapMirrorデスティネーションやSnapLockボリュームなどの読み取り専用のファイルシステムにはハッシュを格納できません。
- ハッシュストアが最大サイズに達すると、新しいハッシュ用のスペースを確保するために古いハッシュがフラッシュされます。ハッシュストアの最大サイズを増やすと、キャッシュからフラッシュされるハッシュの量を減らすことができます。
- ハッシュを格納するボリュームが使用できないか、いっぱいである場合、またはクラスタ内通信に問題があり、BranchCacheサービスでハッシュ情報を取得できない場合、BranchCacheサービスは使用できません。  
ボリュームは、オフラインであるため、またはストレージ管理者がハッシュストアの新しい場所を指定したために、使用できないことがあります。  
この場合はファイルアクセスに関する問題は発生しません。ハッシュストアに正常にアクセスできない場合は、Data ONTAPからクライアントにMicrosoft定義のエラーが返され、クライアントは通常のSMB読み取り要求を使用してファイルを要求します。

## 関連コンセプト

[BranchCacheの設定の管理および監視](#)(355ページ)

## 関連タスク

[CIFSサーバでのBranchCacheの設定](#)(348ページ)

## BranchCacheの推奨事項

BranchCacheを設定する前に、BranchCacheキャッシュを有効にするSMB共有の決定時に考慮する必要がある推奨事項がいくつかあります。

使用する動作モードとBranchCacheを有効にするSMB共有の決定時には、次の推奨事項を考慮してください。

- リモートからキャッシュするデータが頻繁に変更されると、BranchCacheの利点が十分には生かされません。
- BranchCacheサービスは、複数のリモート オフィス クライアントによって再利用されるファイル コンテンツ、または単一のリモート ユーザが繰り返しアクセスするファイル コンテンツを含む共有の場合に役立ちます。
- SnapshotコピーのデータやSnapMirrorデスティネーションのデータなどの読み取り専用コンテンツのキャッシュを有効にすることを検討してください。

## BranchCacheの設定

CIFSサーバでBranchCacheを設定するには、Data ONTAPコマンドを使用します。BranchCacheを実装するには、コンテンツをキャッシュするブランチ オフィスでクライアントおよびホスト型キャッシュ サーバ(オプション)の設定も行う必要があります。

共有ごとにキャッシュを有効にするようにBranchCacheを設定する場合は、BranchCacheキャッシュサービスの対象となるSMB共有でBranchCacheを有効にする必要があります。

### BranchCacheを設定するための前提条件

BranchCacheのセットアップを開始する前に、いくつかの前提条件を満たす必要があります。

Storage Virtual Machine (SVM) のCIFSサーバでBranchCacheを設定するには、次の要件を満たしている必要があります。

- クラスタ内のすべてのノードにData ONTAP 8.2以降がインストールされている必要があります。
- CIFSのライセンスが有効になっていて、CIFSサーバが設定されている必要があります。
- IPv4またはIPv6のネットワーク接続が設定されている必要があります。
- BranchCache 1の場合、SMB 2.1以降が有効になっている必要があります。
- BranchCache 2の場合、SMB 3.0が有効になっていて、リモートのWindowsクライアントでBranchCache 2がサポートされている必要があります。

### CIFSサーバでのBranchCacheの設定

BranchCacheサービスを共有ごとに提供するようにBranchCacheを設定できます。また、すべてのSMB共有でキャッシュを自動的に有効にするようにBranchCacheを設定することもできます。

#### タスク概要

BranchCacheはFlexVolを備えたSVMで設定できます。

- CIFSサーバ上のすべてのSMB共有に格納されたすべてのコンテンツに対してキャッシュ サービスを提供する場合は、すべての共有のBranchCache設定を作成できます。
- CIFSサーバ上の選択したSMB共有に格納されたコンテンツに対してキャッシュ サービスを提供する場合は、共有ごとのBranchCache設定を作成できます。

BranchCacheの設定時には、次のパラメータを指定する必要があります。

| 必須パラメータ     | 説明                                                                  |
|-------------|---------------------------------------------------------------------|
| <i>SVM名</i> | BranchCacheはSVMごとに設定します。BranchCacheサービスを設定するCIFS対応のSVMを指定する必要があります。 |

| 必須パラメータ     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ハッシュ ストアのパス | <p>BranchCacheハッシュはSVMボリューム上の通常のファイルに格納されます。ハッシュ データが格納される既存のディレクトリのパスを指定する必要があります。</p> <p>BranchCacheハッシュ パスは読み取り / 書き込み可能である必要があります。Snapshotディレクトリなどの読み取り専用パスは指定できません。他のデータが含まれているボリュームにハッシュ データを格納するか、ハッシュ データを格納するための別のボリュームを作成することができます。</p> <p>SVMがSVMディザスタリカバリ ソースである場合、ハッシュ パスをルート ボリューム上に配置することはできません。これは、ルート ボリュームがディザスタリカバリ デスティネーションにレプリケートされないためです。</p> <p>ハッシュ パスには、空白を含む任意のファイル名に有効な文字を含めることができます。</p> |

必要に応じて、次のパラメータを指定できます。

| オプションのパラメータ    | 説明                                                                                                                                                                                                                                                                                   |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サポート対象のバージョン   | <p>Data ONTAPでは、BranchCache 1および2がサポートされています。バージョン1、バージョン2、または両方のバージョンを有効にできます。デフォルトでは、両方のバージョンが有効になります。</p>                                                                                                                                                                         |
| ハッシュ ストアの最大サイズ | <p>ハッシュ データ ストアに使用するサイズを指定できます。ハッシュ データがこの値を超えると、古いハッシュが削除され、新しいハッシュを格納するスペースが確保されます。ハッシュ ストアのデフォルトサイズは1GBです。</p> <p>ハッシュが過剰に破棄されない方が、BranchCacheのパフォーマンスは向上します。ハッシュ ストアがいっぱいになるのが原因でハッシュが頻繁に破棄されていると判断した場合は、BranchCacheの設定を変更して、ハッシュ ストアのサイズを大きくすることができます。</p>                      |
| サーバ キー         | <p>クライアントがBranchCacheサーバを偽装できないようにするためにBranchCacheサービスによって使用されるサーバ キーを指定できます。指定しない場合、サーバ キーはBranchCacheの設定の作成時にランダムに生成されます。</p> <p>サーバ キーを特定の値に設定すると、複数のサーバが同じファイルのBranchCacheデータを提供している場合に、クライアントがその同じサーバ キーを使用してサーバのハッシュを使用できるようになります。サーバ キーにスペースを含める場合は、サーバ キーを引用符で囲む必要があります。</p> |
| 動作モード          | <p>デフォルトでは、BranchCacheは共有ごとに有効になります。</p> <ul style="list-style-type: none"> <li>BranchCacheを共有ごとに有効にするBranchCacheの設定を作成するには、このオプション パラメータを指定しないようにするか、<b>per-share</b>を指定します。</li> <li>BranchCacheをすべての共有で自動的に有効にするには、動作モードを<b>all-shares</b>に設定する必要があります。</li> </ul>                |

## 手順

1. 必要に応じてSMB 2.1および3.0を有効にします。

- a. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- b. 設定されたSVMのSMB設定を確認し、必要なすべてのバージョンのSMBが有効になっているかどうかを判断します。

```
vserver cifs options show -vserver vs1
```

- c. 必要に応じてSMB 2.1を有効にします。

```
vserver cifs options modify -vserver vs1 -smb2-enabled true
```

このコマンドを実行すると、SMB 2.0とSMB 2.1の両方が有効になります。

- d. 必要に応じてSMB 3.0を有効にします。

```
vserver cifs options modify -vserver vs1 -smb3-enabled true
```

- e. admin権限レベルに戻ります。

```
set -privilege admin
```

2. BranchCacheを設定します。

```
vserver cifs branchcache create -vserver vs1 -hash-store-path  
path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-  
enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-  
share|all-shares}
```

指定したハッシュ ストレージのパスが存在し、SVMによって管理されているボリューム上にある必要があります。また、パスは読み取り / 書き込み可能なボリュームにある必要があります。パスが読み取り専用であるか、または存在しない場合、コマンドは失敗します。

SVM BranchCacheの追加設定で同じサーバ キーを使用する場合は、サーバ キーとして入力した値を記録しておきます。BranchCacheの設定に関する情報を表示する際に、サーバ キーは表示されません。

3. BranchCacheの設定が正しいことを確認します。

```
vserver cifs branchcache show -vserver vs1
```

#### 例

次のコマンドを実行すると、SMB 2.1と3.0の両方が有効になっていることが確認され、SVM vs1上のすべてのSMB共有でキャッシュを自動的に有効にするようにBranchCacheが設定されます。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /
hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
```

```

Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: all_shares

```

次のコマンドを実行すると、SMB 2.1と3.0の両方が有効になっていることが確認され、SVM vs1上の共有ごとにキャッシュを有効にするようにBranchCacheが設定されて、BranchCacheの設定が確認されます。

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path /
hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share

```

## 関連コンセプト

[要件、考慮事項、および推奨事項](#) (345ページ)

[リモート オフィスでのBranchCacheの設定に関する情報の参照先](#) (351ページ)

[BranchCacheの設定の管理および監視](#) (355ページ)

[SVMでのBranchCacheの無効化と有効化](#) (365ページ)

[SVMのBranchCache設定の削除](#) (367ページ)

## 関連タスク

[BranchCacheが有効なSMB共有の作成](#) (352ページ)

[既存のSMB共有でのBranchCacheの有効化](#) (353ページ)

## リモート オフィスでのBranchCacheの設定に関する情報の参照先

BranchCacheは、CIFSサーバで設定したあと、リモート オフィスのクライアント コンピュータおよびキャッシュ サーバ(オプション)にもインストールして設定する必要があります。リモート オフィスでBranchCacheを設定する手順については、Microsoftから説明が提供されています。

BranchCacheを使用するようにブランチ オフィスのクライアントおよびキャッシュ サーバ(オプション)を設定する手順については、MicrosoftのBranchCacheのWebサイト([technet.microsoft.com/EN-US/NETWORK/DD425028](http://technet.microsoft.com/EN-US/NETWORK/DD425028))を参照してください。

## BranchCache対応のSMB共有の設定

CIFSサーバとブランチ オフィスでBranchCacheを設定したら、ブランチ オフィスのクライアントによるコンテンツのキャッシュを許可するSMB共有でBranchCacheを有効にすることができます。

BranchCacheキャッシュは、CIFSサーバ上のすべてのSMB共有で有効にするか、共有ごとに有効にすることができます。

- BranchCacheを共有ごとに有効にする場合、BranchCacheは共有の作成時に有効にするか、既存の共有を変更して有効にすることができます。  
既存のSMB共有でキャッシュを有効にすると、その共有でBranchCacheを有効にした時点で、Data ONTAPによるハッシュの計算と要求元クライアントへのメタデータの送信が開始されます。
- 共有へのSMB接続をすでに確立しているクライアントは、それ以降にその共有でBranchCacheが有効になった場合、BranchCacheのサポートを得ることができません。  
Data ONTAPは、SMBセッションがセットアップされたときに共有のBranchCacheのサポートをアドバタイズします。BranchCacheが有効化されたときにすでにセッションを確立していたクライアントは、キャッシュされていた内容をこの共有で使用するために、接続をいったん解除したあとに再度接続する必要があります。

**注:** その後SMB共有に対するBranchCacheを無効にすると、Data ONTAPによる要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツ サーバ (CIFSサーバ) から直接データを取得します。

## BranchCacheが有効なSMB共有の作成

SMB共有を作成するときに、**branchcache**共有プロパティを設定して、共有でBranchCacheを有効にすることができます。

### タスク概要

- SMB共有でBranchCacheを有効にする場合は、共有のオフライン ファイル設定を手動キャッシュに設定する必要があります。  
これは、共有を作成するときのデフォルト設定です。
- BranchCacheが有効な共有を作成するときに、オプションの共有パラメータを追加で指定することもできます。
- Storage Virtual Machine (SVM) でBranchCacheが設定されておらず、有効になっていない場合でも、共有の**branchcache**プロパティを設定できます。  
ただし、共有でキャッシュされたコンテンツを提供するには、SVMでBranchCacheを設定して有効にする必要があります。
- `-share-properties`パラメータを使用する場合、共有に適用されるデフォルトの共有プロパティはないため、**branchcache**共有プロパティのほかに共有に適用する他のすべての共有プロパティをカンマで区切って指定する必要があります。
- 詳細については、`vserver cifs share create`コマンドのマニュアル ページを参照してください。

### 手順

1. BranchCacheが有効なSMB共有を作成するには、次のコマンドを入力します。

```
vserver cifs share create -vserver vserver_name -share-name share_name -  
path path -share-properties branchcache[,...]
```

- `-path path`には、共有のパスを指定します。



- パスの区切り文字には、スラッシュまたはバックスラッシュを使用できますが、Data ONTAP では、どちらもスラッシュとして表示されます。
2. `vserver cifs share show`コマンドを使用して、SMB共有に対してBranchCache共有プロパティが設定されていることを確認します。

#### 例

次のコマンドを実行すると、SVM vs1のパス/dataに「data」という名前のBranchCacheが有効なSMB共有が作成されます。デフォルトでは、オフラインファイルの設定は`manual`に設定されます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /
data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name
data
      Vserver: vs1
      Share: data
      CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                        oplocks
                        browsable
                        changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

#### 関連タスク

[CIFSサーバでのSMB共有の作成](#) (180ページ)

[単一のSMB共有でのBranchCacheの無効化](#) (364ページ)

#### 既存のSMB共有でのBranchCacheの有効化

既存のSMB共有でBranchCacheを有効にするには、既存の共有プロパティリストに**branchcache**共有プロパティを追加します。

#### タスク概要

- SMB共有でBranchCacheを有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。  
既存の共有のオフラインファイル設定が手動キャッシュに設定されていない場合は、共有を変更して設定する必要があります。
- Storage Virtual Machine (SVM) でBranchCacheが設定されておらず、有効になっていない場合でも、共有の**branchcache**プロパティを設定できます。  
ただし、共有でキャッシュされたコンテンツを提供するには、SVMでBranchCacheを設定して有効にする必要があります。
- 共有に**branchcache**共有プロパティを追加するときに、既存の共有設定と共有プロパティは維持されます。  
BranchCache共有プロパティは既存の共有プロパティリストに追加されます。`vserver cifs share properties add`コマンドの使用の詳細については、マニュアル ページを参照してください。

**手順**

1. 必要に応じて、オフライン ファイルの共有設定を手動キャッシュに設定します。
  - a. `vserver cifs share show`コマンドを使用して、オフライン ファイルの共有設定を確認します。
  - b. オフライン ファイルの共有設定が手動に設定されていない場合は、必要な値に変更します。
 

```
vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual
```
2. 既存のSMB共有でBranchCacheを有効にします。
 

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache
```
3. SMB共有でBranchCache共有プロパティが設定されていることを確認します。
 

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

**例**

次のコマンドを実行すると、SVM vs1のパス/data2にある「data2」という名前の既存のSMB共有でBranchCacheが有効になります。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

**関連タスク**

[既存のSMB共有に対する共有プロパティの追加または削除](#) (187ページ)

[単一のSMB共有でのBranchCacheの無効化](#) (364ページ)

**BranchCacheの設定の管理および監視**

BranchCacheの設定の管理では、BranchCache パラメータの変更、サーバシークレット キーの変更、BranchCacheでのハッシュの仮計算の設定、ハッシュ キャッシュの削除、BranchCache GPOの設定などの管理ができます。また、BranchCache統計の情報を表示することもできます。

**関連コンセプト**

[ハッシュ ストアの場所を選択する際の考慮事項](#) (347ページ)

**BranchCacheの設定の変更**

Storage Virtual Machine (SVM) 上のBranchCacheサービスの設定では、ハッシュ ストア ディレクトリのパス、最大サイズ、動作モード、サポートするBranchCacheのバージョンなどの設定を変更できます。また、ハッシュ ストアを含めるボリュームのサイズを増やすこともできます。

**手順**

1. 適切な処理を実行します。

| 状況                       | 入力するコマンド                                                                                                                                                                                                                                                          |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ハッシュ ストア ディレクトリのサイズ変更    | <code>vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB MB GB TB PB]}</code>                                                                                                                                                 |
| ハッシュ ストアを含めるボリューム サイズの増加 | <code>volume size -vserver vserver_name -volume volume_name -new-size new_size[k m g t]</code><br><br>ハッシュ ストアを含めるボリュームに空き容量がない場合は、ボリューム サイズを増やします。追加するボリューム サイズは、数字と単位で指定します。<br><br>ボリューム サイズの増加の詳細については、『 <i>clustered Data ONTAP 論理ストレージ管理ガイド</i> 』を参照してください。 |

| 状況                        | 入力するコマンド                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ハッシュ ストア ディレクトリのパス変更      | <pre><b>vserver cifs branchcache modify -vserver</b><br/><b>vserver_name -hash-store-path path -flush-hashes</b><br/><b>{true false}</b></pre> <p>SVMがSVMディザスタリカバリ ソースである場合、ハッシュ パスをルート ボリューム上に配置することはできません。これは、ルート ボリュームがディザスタリカバリ デスティネーションにレプリケートされないためです。</p> <p>BranchCacheハッシュ パスには、ファイル名に使用できる文字と空白を含めることができます。</p> <p>ハッシュ パスを変更する場合、ONTAP Dataに元のハッシュ ストアの場所からハッシュを削除させるかどうかを、<code>-flush-hashes</code>パラメータで指定する必要があります。<code>-flush-hashes</code>パラメータには、次の値を設定できます。</p> <ul style="list-style-type: none"> <li>• <b>true</b>を指定すると、Data ONTAPは元の場所にあるハッシュを削除し、BranchCache対応クライアントが指定した新しい場所に新しいハッシュを新しいリクエストとして作成します。</li> <li>• <b>false</b>を指定すると、ハッシュは削除されません。<br/>この場合、後で、ハッシュ ストア ディレクトリのパスを元の場所に戻して、既存のハッシュを再利用することができます。</li> </ul> |
| 動作モードの変更                  | <pre><b>vserver cifs branchcache modify -vserver</b><br/><b>vserver_name -operating-mode mode</b></pre> <p><code>-operating-mode</code>には、次の値を指定できます。</p> <ul style="list-style-type: none"> <li>• <b>per-share</b></li> <li>• <b>all-shares</b></li> <li>• <b>disable</b></li> </ul> <p>注: 動作モードを変更する場合は、以下の点に注意してください。</p> <ul style="list-style-type: none"> <li>• SMBセッションのセットアップ時に、Data ONTAPによって、BranchCacheが共有のサポートをアドバタイズします。</li> <li>• BranchCacheが有効化されたときにすでにセッションを確立していたクライアントは、キャッシュされていた内容をこの共有で使用するために、接続をいったん解除したあとに再度接続する必要があります。</li> </ul>                                                                                                                                                                                          |
| サポートするBranchCacheバージョンの変更 | <pre><b>vserver cifs branchcache modify -vserver</b><br/><b>vserver_name -versions {v1-enable v2-enable </b><br/><b>enable-all}</b></pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

2. `vserver cifs branchcache show`コマンドを使用して、設定の変更を確認します。

## BranchCache設定に関する情報の表示

FlexVolを備えたStorage Virtual Machine (SVM) のBranchCache設定に関する情報を表示できます。この情報は、設定を検証する場合や、設定を変更する前に現在の設定を確認する場合に役立ちます。

### 手順

1. 次のいずれかを実行します。

| 表示する項目                                | コマンド                                                           |
|---------------------------------------|----------------------------------------------------------------|
| すべてのSVMの<br>BranchCache設定に関する<br>概要情報 | <b>vserver cifs branchcache show</b>                           |
| 特定のSVMの設定に関する<br>詳細情報                 | <b>vserver cifs branchcache show -vserver<br/>vserver_name</b> |

**例**

次の例では、SVM vs1のBranchCache設定に関する情報を表示します。

```
cluster1::> vserver cifs branchcache show -vserver vs1
Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

**BranchCacheサーバキーの変更**

BranchCacheサーバキーを変更するには、Storage Virtual Machine (SVM) でBranchCacheの設定を変更し、別のサーバキーを指定します。

**タスク概要**

サーバキーを特定の値に設定すると、複数のサーバが同じファイルのBranchCacheデータを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。

サーバキーを変更する場合は、ハッシュ キャッシュをフラッシュすることも必要になります。ハッシュのフラッシュ後、BranchCache対応クライアントによって新しい要求が行われると、Data ONTAPによって新しいハッシュが作成されます。

**手順**

1. 次のコマンドを使用して、サーバキーを変更します。

```
vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true
```

- -server-key textでは、サーバキーとして使用するテキスト文字列を指定します。
- サーバキーにスペースを含める場合は、サーバキーを引用符で囲みます。
- 新しいサーバキーを設定する場合は、-flush-hashesも指定して値をtrueに設定する必要があります。

2. vserver cifs branchcache showコマンドを使用して、BranchCacheの設定が正しいことを確認します。

**例**

次の例では、SVM vs1でスペースを含む新しいサーバキーを設定し、ハッシュ キャッシュをフラッシュします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true
cluster1::> vserver cifs branchcache show -vserver vs1
```

```

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share

```

## 関連コンセプト

[Data ONTAPでBranchCacheハッシュが無効になる理由](#) (346ページ)

## 指定したパスのBranchCacheハッシュの事前計算

単一のファイル、ディレクトリ、またはディレクトリ構造内のすべてのファイルを対象に、ハッシュを事前に計算するようにBranchCacheサービスを設定することができます。これは、BranchCache対応の共有にあるデータのハッシュをピーク以外の時間帯に計算するのに役立ちます。

### 開始する前に

ハッシュの統計を表示する前にデータ サンプルを収集する場合、`statistics start` コマンドとオプションの `statistics stop` コマンドを使用する必要があります。これらのコマンドの詳細については、『*clustered Data ONTAP システム アドミニストレーション ガイド(クラスタ管理)*』を参照してください。

### タスク概要

- ハッシュを事前に計算する対象のStorage Virtual Machine (SVM) とパスを指定する必要があります。
- また、ハッシュを再帰的に計算するかどうかについても指定する必要があります。
- ハッシュを再帰的に計算する場合、BranchCache サービスでは、指定されたパスの下でのディレクトリ ツリー全体を参照し、対象となる各オブジェクトのハッシュを計算します。

### 手順

1. 適切なコマンドを実行します。

| ハッシュを事前に計算する対象          | 入力するコマンド                                                                                          |
|-------------------------|---------------------------------------------------------------------------------------------------|
| 単一のファイルまたはディレクトリ        | <code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</code> |
| ディレクトリ構造内のすべてのファイル(再帰的) | <code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse true</code>  |

`-path path` には絶対パスを指定します。

2. `statistics` コマンドを使用して、ハッシュが計算されていることを確認します。
  - a. 目的のSVMインスタンスの`hashd`オブジェクトの統計を表示します。
 

```
statistics show -object hashd -instance vserver_name
```
  - b. コマンドを繰り返し実行して、作成済みのハッシュの数が増加していることを確認します。

### 例

次に、パス `/data` および SVM `vs1` に格納されているすべてのファイルとサブディレクトリを対象にハッシュを作成する例を示します。

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data -
recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1
```

| Counter                         | Value                                |
|---------------------------------|--------------------------------------|
| branchcache_hash_created        | 85                                   |
| branchcache_hash_files_replaced | 0                                    |
| branchcache_hash_rejected       | 0                                    |
| branchcache_hash_store_bytes    | 0                                    |
| branchcache_hash_store_size     | 0                                    |
| instance_name                   | vs1                                  |
| node_name                       | node1                                |
| node_uuid                       | 11111111-1111-1111-1111-111111111111 |
| process_name                    | -                                    |

```
cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1
```

| Counter                         | Value                                |
|---------------------------------|--------------------------------------|
| branchcache_hash_created        | 92                                   |
| branchcache_hash_files_replaced | 0                                    |
| branchcache_hash_rejected       | 0                                    |
| branchcache_hash_store_bytes    | 0                                    |
| branchcache_hash_store_size     | 0                                    |
| instance_name                   | vs1                                  |
| node_name                       | node1                                |
| node_uuid                       | 11111111-1111-1111-1111-111111111111 |
| process_name                    | -                                    |

## SVM BranchCacheハッシュ ストアからのハッシュのフラッシュ

Storage Virtual Machine (SVM) 上の BranchCache ハッシュ ストアから、キャッシュされたハッシュをすべてフラッシュできます。これは、ブランチ オフィスの BranchCache の設定を変更した場合に役立ちます。たとえば、最近キャッシュ モードを分散キャッシュからホスト型キャッシュ モードに再設定した場合は、ハッシュ ストアをフラッシュする必要があります。

### タスク概要

ハッシュのフラッシュ後、BranchCache 対応クライアントによって新しい要求が行われると、Data ONTAP によって新しいハッシュが作成されます。

### 手順

1. BranchCache ハッシュ ストアからハッシュをフラッシュします。

```
vserver cifs branchcache hash-flush -vserver vserver_name
```

### 例

```
vserver cifs branchcache hash-flush -vserver vs1
```

## BranchCache 統計の表示

BranchCache 統計を表示すると、さまざまな目的の中でも、キャッシュが適切に機能しているかどうかの確認、キャッシュ コンテンツをクライアントに提供しているかどうかの確認、新しいハッシュ デ

一タのスペースを確保するためにハッシュ ファイルが削除されたかどうかの確認に特に役立ちます。

### タスク概要

**hashd**統計オブジェクトには、BranchCacheハッシュに関する統計情報を提供するカウンタが含まれています。**cifs**統計オブジェクトには、BranchCache関連のアクティビティに関する統計情報を提供するカウンタが含まれています。これらのオブジェクトに関する情報は、advanced権限レベルで収集して表示できます。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

#### 例

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. **statistics catalog counter show**コマンドを使用して、BranchCache関連のカウンタを表示します。

統計カウンタの詳細については、このコマンドのマニュアル ページを参照してください。

#### 例

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
Counter      Description
-----
branchcache_hash_created    Number of times a request to generate
                             BranchCache hash for a file succeeded.
branchcache_hash_files_replaced    Number of times a BranchCache hash file was
                             deleted to make room for more recent hash
                             data. This happens if the hash store size is
                             exceeded.
branchcache_hash_rejected    Number of times a request to generate
                             BranchCache hash data failed.
branchcache_hash_store_bytes    Total number of bytes used to store hash data.
branchcache_hash_store_size    Total space used to store BranchCache hash
                             data for the Vserver.
instance_name                Instance Name
instance_uuid                 Instance UUID
node_name                     System node name
node_uuid                     System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
Counter      Description
-----
active_searches                Number of active searches over SMB and SMB2
auth_reject_too_many            Authentication refused after too many
                             requests were made in rapid succession
avg_directory_depth            Average number of directories crossed by SMB
                             and SMB2 path-based commands
avg_junction_depth            Average number of junctions crossed by SMB
                             and SMB2 path-based commands
branchcache_hash_fetch_fail    Total number of times a request to fetch hash
                             data failed. These are failures when
                             attempting to read existing hash data. It
```



```

branchcache_hash_fetch_ok    does not include attempts to fetch hash data
                             that has not yet been generated.
branchcache_hash_sent_bytes  Total number of times a request to fetch hash
                             data succeeded.
branchcache_missing_hash_bytes Total number of bytes sent to clients
                             requesting hashes.
                             Total number of bytes of data that had to be
                             read by the client because the hash for that
                             content was not available on the server.
....Output truncated....

```

3. `statistics start`コマンドと`statistics stop`コマンドを使用して、BranchCache関連の統計を収集します。

統計の収集の詳細については、『*clustered Data ONTAP システム アドミニストレーション ガイド (クラスタ管理)*』を参照してください。

#### 例

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. `statistics show`コマンドを使用して、収集したBranchCache統計を表示します。

統計情報の表示の詳細については、『*clustered Data ONTAP システム アドミニストレーション ガイド (クラスタ管理)*』を参照してください。

#### 例

```

cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

Counter                                     Value
-----
branchcache_hash_sent_bytes                 0
branchcache_hash_sent_bytes                 0
branchcache_hash_sent_bytes                 0
branchcache_hash_sent_bytes                 0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

Counter                                     Value
-----
branchcache_missing_hash_bytes              0
branchcache_missing_hash_bytes              0
branchcache_missing_hash_bytes              0
branchcache_missing_hash_bytes              0

```

5. `admin`権限レベルに戻ります。

```
set -privilege admin
```

**例**

```
cluster1::*> set -privilege admin
```

**関連タスク**

[統計情報の表示](#) (313ページ)

**BranchCacheグループ ポリシー オブジェクトのサポート**

Data ONTAP BranchCacheでは、BranchCacheのグループ ポリシー オブジェクト(GPO)をサポートしており、特定のBranchCacheの設定パラメータを一元的に管理できます。BranchCacheのGPOには、BranchCacheのハッシュの発行GPOとBranchCacheのハッシュ バージョン サポートGPOの2つがあります。

**BranchCacheのハッシュの発行GPO**

BranchCacheのハッシュの発行GPOは、-operating-modeパラメータに対応します。GPOの更新が行われると、グループ ポリシーが適用される組織単位(OU)に含まれるStorage Virtual Machine(SVM)オブジェクトにこの値が適用されます。

**BranchCacheのハッシュ バージョン サポートGPO**

BranchCacheのハッシュ バージョン サポートGPOは、-versionsパラメータに対応します。GPOの更新が行われると、グループ ポリシーが適用される組織単位に含まれるSVMオブジェクトにこの値が適用されます。

**関連コンセプト**

[CIFSサーバへのグループポリシー オブジェクトの適用](#) (115ページ)

**BranchCacheグループ ポリシー オブジェクトに関する情報の表示**

CIFSサーバのグループ ポリシー オブジェクト(GPO)設定に関する情報を表示して、CIFSサーバが属しているドメインでBranchCache GPOが定義されているかどうか、また定義されている場合は許容値を確認できます。また、BranchCache GPO設定がCIFSサーバに適用されているかどうかを確認できます。

**タスク概要**

CIFSサーバが属しているドメイン内でGPO設定が定義されていても、CIFS対応のStorage Virtual Machine(SVM)が含まれるOrganizational Unit(OU;組織単位)に適用されているとは限りません。適用されるGPO設定は、CIFS対応のSVMに適用されているすべての定義済みGPOの一部です。GPOを介して適用されたBranchCache設定は、CLIを介して適用された設定よりも優先されます。

**手順**

1. `vserver cifs group-policy show-defined`コマンドを使用して、Active Directoryドメインで定義されているBranchCache GPO設定を表示します。

**例**

注: この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----
      GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
      Advanced Audit Settings:
```

```

Object Access:
  Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

GPO Name: Resultant Set of Policy
Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

```

2. `vserver cifs group-policy show-applied`コマンドを使用して、CIFSサーバに適用されているBranchCache GPO設定を表示します。

#### 例

注: この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1
Vserver: vs1
-----
  GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

  GPO Name: Resultant Set of Policy
    Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

```

#### 関連タスク

[CIFSサーバ上でのGPOサポートの有効化と無効化](#) (120ページ)

## SMB共有でのBranchCacheの無効化

特定のSMB共有でBranchCacheキャッシュ サービスを提供する必要がなくなったが、あとでそれらの共有でキャッシュ サービスが必要になる可能性がある場合は、共有単位でBranchCacheを無効にすることができます。すべての共有でキャッシュを提供するようにBranchCacheを設定している

が、一時的にすべてのキャッシュ サービスを無効にする必要がある場合は、BranchCache設定を変更してすべての共有で自動キャッシュを停止することができます。

SMB共有で有効になっていたBranchCacheをあとから無効にすると、Data ONTAPによる要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツ サーバ(Storage Virtual Machine (SVM) 上のCIFSサーバ)から直接データを取得します。

## 関連コンセプト

[BranchCache対応のSMB共有の設定](#)(352ページ)

## 単一のSMB共有でのBranchCacheの無効化

キャッシュ コンテンツを使用できるようにしていた特定の共有でキャッシュ サービスを提供する必要がなくなった場合は、既存のSMB共有でBranchCacheを無効にすることができます。

## 手順

1. 次のコマンドを入力します。

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache
```

BranchCache共有プロパティが削除されます。適用されているその他の共有プロパティは有効なままです。

## 例

次のコマンドでは、「data2」という名前の既存のSMB共有でBranchCacheを無効にします。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
```

```
File Attribute Cache Lifetime: 10s
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

## すべてのSMB共有での自動キャッシュの停止

FlexVolを備えたStorage Virtual Machine (SVM)のすべてのSMB共有に対してBranchCacheキャッシュを自動的に有効にするように設定している場合、BranchCacheの設定を変更することで、すべてのSMB共有に対するコンテンツの自動キャッシュを停止することができます。

### タスク概要

すべてのSMB共有に対する自動キャッシュを停止するには、BranchCacheの動作モードを共有ごとのキャッシュに変更します。

### 手順

1. 次のコマンドを入力して、すべてのSMB共有に対する自動キャッシュを停止するようにBranchCacheを設定します。

```
vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share
```

2. BranchCacheの設定が正しいことを確認します。

```
vserver cifs branchcache show -vserver vserver_name
```

### 例

次のコマンドは、Storage Virtual Machine (SVM、旧Vserver) vs1のBranchCache設定を変更し、すべてのSMB共有で自動キャッシュを停止します。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode per-share

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

## SVMでのBranchCacheの無効化と有効化

Storage Virtual Machine (SVM)でキャッシュ サービスの提供を一時的に停止する場合は、そのSVMでBranchCacheを無効にすることができます。あとで、SVMでBranchCacheを有効にすることで、キャッシュ サービスの提供を簡単に再開できます。

### CIFSサーバでBranchCacheを無効または再度有効にしたときの動作

BranchCacheを設定したあとに、ブランチ オフィスのクライアントがキャッシュされたコンテンツを使用できないようにするには、CIFSサーバでキャッシュを無効にします。BranchCacheを無効にするときは、それを実行した場合の動作について理解しておく必要があります。

BranchCacheを無効にすると、Data ONTAPによるハッシュの計算や要求元クライアントへのメタデータの送信が行われなくなります。ただし、ファイル アクセスは中断されません。以降に、BranchCache対応クライアントからアクセスするコンテンツのメタデータ情報を要求すると、Microsoftのエラーが返されます。この場合は、クライアントでもう一度要求を送信して、実際のコン

テンツを要求します。これに対する応答として、CIFSサーバからStorage Virtual Machine (SVM)に格納されている実際のコンテンツが送信されます。

CIFSサーバでBranchCacheを無効にした後は、SMB共有でBranchCacheの機能がアドバタイズされなくなります。新しいSMB接続でデータにアクセスするには、通常のSMB読み取り要求を行います。

BranchCacheは、CIFSサーバでいつでも再度有効にすることができます。

- BranchCacheを無効にしてもハッシュストアは削除されないため、要求されたハッシュがまだ有効であれば、BranchCacheを再度有効にしたあとに、格納されたハッシュを使用してハッシュの要求に応答することができます。
- BranchCache対応の共有に対するSMB接続を確立したクライアントで接続を確立した時にBranchCacheが無効になっていたクライアントの場合には、以降にBranchCacheを再度有効にしても、BranchCacheのサポートは有効になりません。  
これは、SMBセッションのセットアップ時に共有に対するBranchCacheのサポートがアドバタイズされるからです。BranchCacheを無効にしたときにBranchCache対応の共有に対するセッションを確立していた場合、その共有のキャッシュされたコンテンツを使用するには、いったん切断してから接続し直す必要があります。

**注:** CIFSサーバでBranchCacheを無効にしたあとにハッシュストアを保存しておく必要がない場合は、手動で削除することができます。BranchCacheを再度有効にするときは、ハッシュストアのディレクトリが存在することを確認する必要があります。BranchCacheを再度有効にすると、BranchCache対応の共有でBranchCacheの機能がアドバタイズされるようになります。BranchCache対応クライアントから新しい要求が行われると、Data ONTAPで新しいハッシュが作成されます。

## BranchCacheの無効化または有効化

FlexVolを備えたStorage Virtual Machine (SVM)でBranchCacheを無効にするには、BranchCacheの動作モードを**disabled**に変更します。BranchCacheサービスを共有単位で提供するか、すべての共有で自動的に提供するように動作モードを変更すると、いつでもBranchCacheを有効にすることができます。

### 手順

1. 該当するコマンドを実行します。

| 状況                         | 入力するコマンド                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| BranchCacheを無効にする場合        | <b>vserver cifs branchcache modify -vserver <i>vserver_name</i> -operating-mode disable</b>    |
| 共有単位でBranchCacheを有効にする場合   | <b>vserver cifs branchcache modify -vserver <i>vserver_name</i> -operating-mode per-share</b>  |
| すべての共有でBranchCacheを有効にする場合 | <b>vserver cifs branchcache modify -vserver <i>vserver_name</i> -operating-mode all-shares</b> |

2. BranchCacheの動作モードが適切な設定になっていることを確認します。

**vserver cifs branchcache show -vserver *vserver\_name***

### 例

次の例では、SVM vs1でBranchCacheを無効にします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable
cluster1::> vserver cifs branchcache show -vserver vs1
```

```

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable

```

## SVMのBranchCache設定の削除

Storage Virtual Machine (SVM) でキャッシュ サービスを提供する必要がなくなった場合、BranchCache設定を削除できます。

### BranchCache設定を削除したときの動作

BranchCacheを設定したあとに、Storage Virtual Machine (SVM) からのキャッシュされたコンテンツの提供を中止する場合は、CIFSサーバでBranchCache設定を削除します。設定を削除するときは、それを実行した場合の動作について理解しておく必要があります。

設定を削除すると、そのSVMの設定情報がクラスタから削除され、BranchCacheサービスが停止します。SVMのハッシュストアについては、削除するかどうかを選択することができます。

BranchCache設定を削除しても、BranchCache対応クライアントによるアクセスは中断されません。以降に、BranchCache対応クライアントから既存のSMB接続でキャッシュ済みのコンテンツのメタデータ情報を要求すると、Microsoftのエラーが返されます。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、CIFSサーバからSVMに格納されている実際のコンテンツが送信されます。

BranchCache設定を削除すると、SMB共有でBranchCacheの機能がアドバタイズされなくなります。キャッシュされていないコンテンツに新しいSMB接続でアクセスするには、通常のSMB読み取り要求を行います。

### BranchCache設定の削除

Storage Virtual Machine (SVM) でBranchCacheサービスの削除に使用するコマンドは、既存のハッシュを削除するか、保持するかによって異なります。

#### 手順

1. 該当するコマンドを実行します。

| 状況                               | 入力するコマンド                                                                                |
|----------------------------------|-----------------------------------------------------------------------------------------|
| BranchCache設定を削除し、既存のハッシュを削除する   | <b>vserver cifs branchcache delete -vserver <i>vserver_name</i> -flush-hashes true</b>  |
| BranchCache設定を削除するが、既存のハッシュは保持する | <b>vserver cifs branchcache delete -vserver <i>vserver_name</i> -flush-hashes false</b> |

#### 例

次の例では、SVM vs1でBranchCache設定を削除し、既存のハッシュをすべて削除します。

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes true
```

## リバートした場合のBranchCacheの動作

Data ONTAPをBranchCacheがサポートされないリリースにリバートするときは、それを実行した場合の動作について理解しておくことが重要です。

- Data ONTAPをBranchCacheがサポートされないバージョンにリバートすると、BranchCache対応クライアントに対してSMB共有でBranchCacheの機能がアドバタイズされなくなります。そのため、クライアントからハッシュ情報が要求されることはありません。  
クライアントでは、代わりに、通常のSMB読み取り要求を使用して実際のコンテンツを要求します。これに対する応答として、CIFSサーバからStorage Virtual Machine (SVM)に格納されている実際のコンテンツが送信されます。
- ハッシュストアをホストするノードをBranchCacheがサポートされないリリースにリバートする場合、リバート時に出力されるコマンドを使用して、ストレージ管理者が手動でBranchCacheの設定をリバートする必要があります。  
このコマンドでは、BranchCacheの設定とハッシュが削除されます。  
リバートの完了後、必要に応じて、ハッシュストアが格納されていたディレクトリを手動で削除できます。

### 関連コンセプト

[SVMのBranchCache設定の削除](#) (367ページ)

## Microsoftリモート コピーのパフォーマンスの向上

Microsoft Offloaded Data Transfer (ODX; オフロード データ転送) は *コピー オフロード* と呼ばれ、この機能を使用すると、互換性があるストレージ デバイス内やストレージ デバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

Data ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXをサポートしています。ソースとデスティネーションのどちらについても、CIFSサーバとLUNの両方に対応しています。

ODX以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションに転送します。つまり、クライアントコンピュータがソースからデータを読み取り、デスティネーションに書き込みます。ODXファイル転送では、データはソースからデスティネーションに直接コピーされます。

ODXオフロード コピーはソース ストレージとデスティネーション ストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量 (CPU、メモリ) の削減、ネットワークI/O帯域幅の使用量の削減などが挙げられます。

SMB環境では、この機能は、クライアントとストレージ サーバの両方でSMB 3.0およびODX機能がサポートされている場合にのみ使用できます。SAN環境では、この機能は、クライアントとストレージ サーバの両方でODX機能がサポートされている場合にのみ使用できます。ODXがサポートされていて有効になっているクライアントコンピュータでは、ファイルの移動やコピーを行う際に、オフロード ファイル転送が自動的にかつ透過的に使用されます。ODXは、ファイルをエクスプローラでドラッグ アンドドロップしたか、コマンドラインのファイル コピー コマンドを使用したか、クライアントアプリケーションによってファイル コピー 要求が開始されたかに関係なく使用されます。

### 関連コンセプト

[Auto LocationでSMB自動ノード リファールを提供することでクライアントの応答時間を改善](#) (373ページ)

[Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピー オフロードの使用方法](#) (390ページ)



## ODXの仕組み

ODXコピー オフロードでは、トークンベースのメカニズムを使用して、ODX対応のCIFSサーバ内またはCIFSサーバ間でデータの読み取りおよび書き込みを行います。CIFSサーバは、ホストを介してデータをルーティングするのではなく、データを表す小さなトークンをクライアントに送信します。ODXクライアントがそのトークンをデスティネーションサーバに提示すると、サーバはそのトークンによって表されるデータをソースからデスティネーションに転送できます。

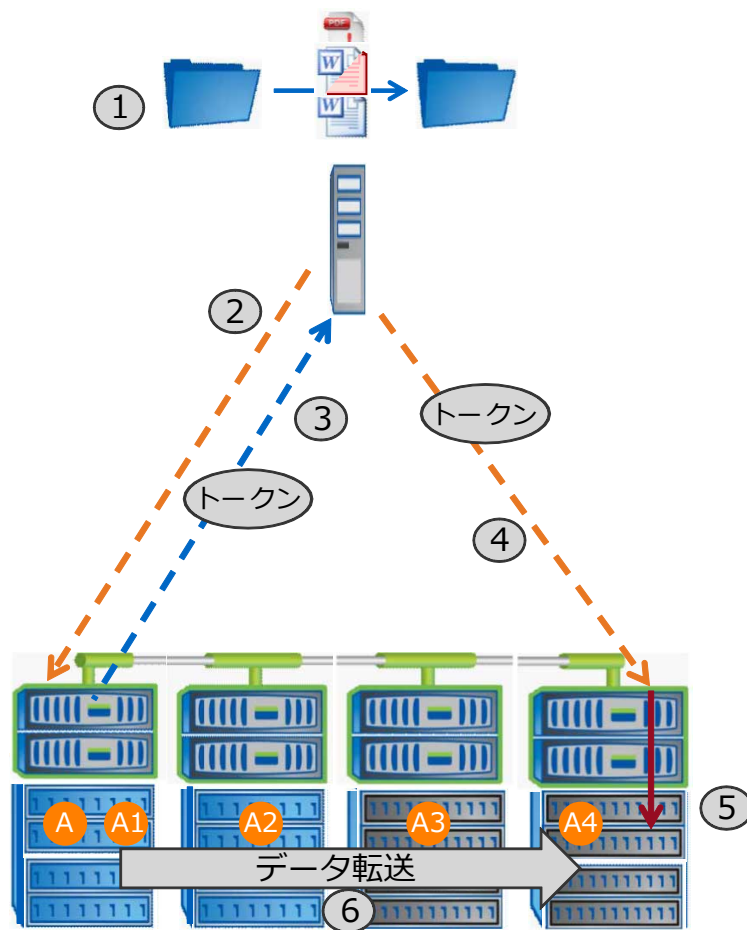
ODXクライアントは、CIFSサーバがODX対応であると認識すると、ソースファイルを開いてCIFSサーバのトークンを要求します。デスティネーションファイルを開いたら、クライアントはトークンを使用して、データをソースからデスティネーションに直接コピーするようにサーバに指示します。

注: ソースとデスティネーションは、コピー処理の範囲に応じて、同じStorage Virtual Machine (SVM)上に存在する場合も異なるSVM上に存在する場合があります。

トークンはデータの特定时点の状態を表すものとして機能します。たとえば、ノード間でデータをコピーする場合、データセグメントを表すトークンが要求元クライアントに返され、そのトークンをクライアントがデスティネーションにコピーするため、クライアントを介して基になるデータをコピーする必要がありません。

Data ONTAPでは、8MBのデータを表すトークンがサポートされます。8MBを超えるODXコピーは、8MBのデータを表すトークンを複数使用して実行されます。

次の図で、ODXコピー処理に関連するステップについて説明します。



1. エクスプローラを使用するか、コマンドライン インターフェイスを使用するか、仮想マシンの移行の一環として、ユーザがファイルをコピーまたは移動します。または、アプリケーションによってファイルのコピーまたは移動が開始されます。

2. ODX対応のクライアントが、この転送要求をODX要求に自動的に変換します。  
CIFSサーバに送信されるODX要求には、トークン要求が含まれています。
3. CIFSサーバでODXが有効になっており、接続がSMB 3.0経由の場合は、ソースのデータを論理的に表したものであるトークンがCIFSサーバによって生成されます。
4. クライアントは、データを表すトークンを受信し、書き込み要求を使用してそのトークンをデスティネーションCIFSサーバに送信します。  
ネットワーク経由でソースからクライアントにコピーされ、クライアントからデスティネーションにコピーされるのは、このデータだけです。
5. トークンがストレージ サブシステムに送信されます。
6. コピーまたは移動がSVMによって内部的に実行されます。  
コピーまたは移動されるファイルが8MBより大きい場合、コピーを実行するには複数のトークンが必要になります。コピーが完了するまで、必要に応じてステップ2～6が繰り返されます。

注: ODXオフロード コピーでエラーが発生した場合、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。同様に、デスティネーションCIFSサーバでODXがサポートされていない場合、またはODXが無効になっている場合は、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。

## ODXの使用要件

FlexVolを備えたStorage Virtual Machine(SVM)でODXによるコピー オフロードを使用する前に、一定の要件について確認しておく必要があります。

### Data ONTAPのバージョン要件

ODXによるコピー オフロードは、clustered Data ONTAP 8.2以降のリリースでサポートされます。

### SMBのバージョンの要件

- clustered Data ONTAPでは、SMB 3.0以降でODXがサポートされます。
- ODXを有効にする前に、CIFSサーバでSMB 3.0を有効にしておく必要があります。
  - ODXを有効にするとSMB 3.0も有効になります(まだ有効になっていない場合)。
  - SMB 3.0を無効にするとODXも無効になります。

### Windowsサーバおよびクライアントの要件

ODXによるコピー オフロードを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。ODXは、Windows Server 2012およびWindows 8からサポートされるようになりました。

ODXをサポートするWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix))を参照してください。

### ボリュームの要件

- ソース ボリュームは1.25GB以上でなければなりません。
- コピー オフロードに使用するボリュームで重複排除を有効にする必要があります。
- コピー オフロードに使用するボリュームで圧縮を有効にしてはなりません。

## ODXを使用する場合の考慮事項

コピー オフロードにODXを使用する場合は、一定の考慮事項について理解しておく必要があります。たとえば、ODXを使用できるボリュームのタイプや、クラスタ内およびクラスタ間のODXに関する考慮事項を把握する必要があります。

### ボリュームに関する考慮事項

- 次の項目に該当する場合はコピー オフロードにODXを使用できません。
  - ソース ボリューム サイズが1.25GB未満である  
ODXを使用するには、ボリューム サイズが1.25GB以上である必要があります。
  - 読み取り専用ボリューム  
負荷共有ミラー、SnapMirrorデスティネーション ボリューム、またはSnapVaultデスティネーション ボリュームに存在するファイルやフォルダにはODXを使用できません。
  - ソース ボリュームが圧縮されている場合
  - ソース ボリュームが重複排除されていない場合
- ODXコピーはクラスタ内のコピーにのみ対応しています。  
ODXを使用して、ファイルまたはフォルダを別のクラスタ内のボリュームにコピーすることはできません。
- ODXは、FlexVolを備えたStorage Virtual Machine (SVM) でサポートされています。  
ODXを使用して、Infinite Volumeを備えたSVMとの間でデータをコピーすることはできません。

### その他の考慮事項

- SMB環境では、コピー オフロードにODXを使用するには、256KB以上のファイルである必要があります。  
このサイズよりも小さいファイルは従来のコピー処理を使用して転送します。
- ODXコピー オフロードでは、コピー プロセスの一部として重複排除が実行されます。  
データのコピーまたは移動時にSVMのボリュームで重複排除が発生しないようにする場合は、そのSVMでODXコピー オフロードを無効にする必要があります。
- データ転送を実行するアプリケーションは、ODXをサポートするように記述する必要があります。  
ODXがサポートされるアプリケーション処理は次のとおりです。
  - Virtual Hard Disk (VHD; 仮想ハード ディスク) の作成および変換、Snapshotコピーの管理、仮想マシン間でのファイルのコピーなど、Hyper-Vの管理処理
  - Windowsエクスペローラでの操作
  - Windows PowerShellのcopyコマンド
  - Windowsコマンド プロンプトのcopyコマンド  
Windowsコマンド プロンプトのRobocopyはODXをサポートしています。

**注:** ODXをサポートするWindowsサーバまたはクライアント上でアプリケーションを実行する必要があります。

Windowsサーバおよびクライアント上でサポートされるODXアプリケーションの詳細については、Microsoft TechNetライブラリを参照してください。

### 関連情報

Microsoft TechNetライブラリ: [technet.microsoft.com/ja-jp/library/](https://technet.microsoft.com/ja-jp/library/)

## ODXのユースケース

FlexVolを備えたSVMでODXを使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODXをサポートするWindowsサーバおよびクライアントでは、リモートサーバ間でデータをコピーする際に、デフォルトでコピー オフロードが使用されます。WindowsサーバおよびクライアントでODXがサポートされていない場合や、ODXコピー オフロードが任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODXコピーおよび移動の使用は、以下のユースケースでサポートされます。

- ボリューム内  
ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。
- ボリュームが異なり、ノードとSVMは同じ  
ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。
- ボリュームとノードが異なり、SVMは同じ  
ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。
- SVMが異なり、ノードは同じ  
ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは異なるSVMに所有されます。
- SVMとノードが異なる  
ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは異なるSVMに所有されます。

さらに、いくつかの特殊なユースケースがあります。

- Data ONTAPのODXの実装でODXを使用すると、SMB共有とFCまたはiSCSIで接続された仮想ドライブとの間でファイルをコピーできます。  
Windowsエクスプローラ、Windows CLI(PowerShell)、Hyper-V、またはODXをサポートするその他のアプリケーションでODXコピー オフロードを使用すると、SMB共有と接続されたLUNが同じクラスタにある場合に、それらの間でシームレスにファイルをコピーまたは移動できます。
- Hyper-Vでは、さらに次のようなユースケースでもODXコピー オフロードが使用されます。
  - Hyper-VでODXコピー オフロードのパススルーを使用して、VHDファイル内およびVHDファイル間でのデータのコピー、または同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でのデータのコピーを実行できます。  
これにより、ゲスト オペレーティング システムからのコピーを基盤となるストレージに渡すことができます。
  - 容量固定VHDを作成する際に、ODXを使用して、既知の初期化済みトークンによってディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合に、ODXコピー オフロードを使用して、仮想マシンのストレージを移行します。

**注:** Hyper-VでのODXコピー オフロードのパススルーの用途を活用するには、ゲスト オペレーティング システムでODXがサポートされている必要があります。また、ゲスト オペレーティング システムのディスクが、ODXをサポートするストレージ(SMBまたはSAN)から作成されたSCSIディスクである必要があります。ゲスト オペレーティング システムのディスクがIDEディスクの場合、ODXのパススルーはサポートされません。

## ODXの有効化と無効化

FlexVolを備えたStorage Virtual Machine (SVM)でODXを有効または無効にすることができます。デフォルトでは、SMB 3.0が有効になっている場合は、ODXコピー オフロードのサポートも有効になっています。

### 開始する前に

SMB 3.0が有効になっている必要があります。

### タスク概要

SMB 3.0を無効にすると、SMB ODXも無効になります。SMB 3.0を再度有効にする場合は、SMB ODXを手動で再度有効にする必要があります。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| ODXコピー オフロードの設定 | 入力するコマンド                                                                                   |
|-----------------|--------------------------------------------------------------------------------------------|
| 有効              | <code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>  |
| 無効              | <code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code> |

3. admin権限レベルに戻ります。

```
set -privilege admin
```

### 例

次の例では、SVM vs1でODXコピー オフロードを有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload-enabled
true

cluster1::*> set -privilege admin
```

### 関連参照情報

[使用できるCIFSサーバオプション](#)(71ページ)

## Auto LocationでSMB自動ノード リファールを提供することでクライアントの応答時間を改善

Auto Locationは、SMB自動ノード リファールを使用して、FlexVolを備えたStorage Virtual Machine (SVM) 上でのSMBクライアントのパフォーマンスを向上します。自動ノード リファール

は、要求しているクライアントを、データが存在するFlexVolをホストしているノードSVM上のLIFに自動的にリダイレクトします。これにより、クライアントの応答時間を改善できます。

SMBクライアントがSVM上でホストされているSMB共有に接続するときに、要求されたデータを所有していないノード上のLIFを使用して接続することがあります。クライアントが接続しているノードは、クラスタネットワークを使用して別のノードが所有しているデータにアクセスします。SMB接続が要求されたデータを含むノード上にあるLIFを使用している場合、クライアントへの応答時間が短縮されます。

- Data ONTAPでは、MicrosoftのDFSリファールを使用して、要求されたファイルやフォルダがネームスペース内のどこか別の場所でホストされていることをSMBクライアントに通知することで、この機能を実現します。  
ノードがリファールを作成するのは、データを含むノード上にSVMのLIFがあることを特定した場合です。
- 自動ノード リファールでは、IPv4とIPv6のLIFのIPアドレスがサポートされます。
- リファールは、クライアント接続が経由する、共有のルートの場合に基づいて作成されます。
- リファールは、SMBネゴシエーション中に発生します。  
リファールは、接続が確立される前に作成されます。Data ONTAPがターゲット ノードに参照先のSMBクライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先LIFパスを介してデータにアクセスします。これにより、クライアントにはより高速なデータ アクセスが提供され、クラスタの余分な通信も回避されます。

**注:** 共有が複数のジャンクション ポイントにまたがっていて、ジャンクションの一部が他のノードに格納されているボリュームを参照する場合、共有内のデータは複数のノードに分散されます。Data ONTAPは共有のルートに対してローカルなリファールを提供するため、これらのローカルでないボリュームに含まれるデータを取得するには、クラスタネットワークを使用する必要があります。

このタイプのネームスペース アーキテクチャでは、自動ノード リファールによる大幅なパフォーマンス向上は望めない場合があります。

データをホストするノードに使用可能なLIFがない場合、Data ONTAPは、クライアントが選択したLIFを使用して接続を確立します。ファイルがSMBクライアントによって開かれると、クライアントは参照された同じ接続を介してファイルへのアクセスを継続します。

何らかの理由でCIFSサーバがリファールを作成できない場合でも、SMBサービスが中断されることはありません。自動ノード リファールが有効でない場合と同様にSMB接続が確立されます。

## 関連コンセプト

[Microsoftリモート コピーのパフォーマンスの向上](#) (368ページ)

## 自動ノード リファールを使用する際の要件と考慮事項

SMB自動ノード リファール(オートロケーション)を使用する前に、この機能をサポートするData ONTAPのバージョンなど、一定の要件について確認しておく必要があります。サポートされるSMBプロトコルのバージョンやその他の特別な考慮事項についても確認しておく必要があります。

### Data ONTAPのバージョンとライセンスの要件

- SMB自動ノード リファールは、Data ONTAP 8.2以降のリリースでサポートされます。
- クラスタ内のすべてのノードで、自動ノード リファールがサポートされているバージョンのData ONTAPが実行されている必要があります。
- Storage Virtual Machine(SVM)にCIFSのライセンスがあり、CIFSサーバが配置されている必要があります。



## SMBプロトコルのバージョン

- FlexVolを備えたSVMについては、すべてのバージョンのSMBで自動ノードリファールがサポートされます。
- Infinite Volumeを備えたSVMについては、SMB 1.0で自動ノードリファールがサポートされます。

## SMBクライアントの要件

SMB自動ノードリファールは、Data ONTAPでサポートされるすべてのMicrosoftクライアントでサポートされます。

Data ONTAPでサポートされるWindowsクライアントに関する最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix))を参照してください。

## データLIFの要件

データLIFをCIFSクライアントのリファールとして使用する可能性がある場合は、NFSとCIFSの両方を有効にしたデータLIFを作成する必要があります。

自動ノードリファールは、ターゲットノードのデータLIFでNFSプロトコルまたはCIFSプロトコルのどちらかが有効になっていない場合は機能しないことがあります。

この要件が満たされない場合でも、データアクセスには影響がありません。SMBクライアントは、SVMへの接続に使用した元のLIFを使用して共有をマッピングします。

## 参照されたSMB接続を確立する際のNTLM認証の要件

CIFSサーバを含むドメインと自動ノードリファールを使用するクライアントを含むドメインで、NTLM認証が許可されている必要があります。

リファールを作成するには、CIFSサーバからWindowsクライアントに参照先のIPアドレスが渡されます。IPアドレスを使用した接続にはNTLM認証が使用されるため、参照された接続に対してはKerberos認証は実行されません。

これは、WindowsクライアントではKerberosで使用するサービスプリンシパル名 (service/NetBIOS nameおよびservice/FQDNの形式) を作成できず、クライアントからサービスにKerberosチケットを要求できないためです。

## 自動ノードリファールでホームディレクトリ機能を使用する場合の考慮事項

ホームディレクトリ共有プロパティを有効にして共有を設定した場合、ホームディレクトリの設定で1つ以上のホームディレクトリ検索パスを設定できます。この検索パスで、SVMのボリュームを含む各ノードに格納されているボリュームを指定できます。クライアントはリファールを受け取り、使用できるアクティブなローカルデータLIFがあれば、ホームユーザのホームディレクトリに対してローカルな、参照されたLIFを介して接続します。

SMB 1.0クライアントで自動ノードリファールを有効にして動的ホームディレクトリにアクセスする場合は注意が必要です。SMB 1.0クライアントでは、認証を行う前、すなわちCIFSサーバに対してユーザの名前が指定されていない段階で自動ノードリファールが必要になるからです。SMB 1.0クライアントでCIFSホームディレクトリへのアクセスが正常に機能するのは、次の条件に該当する場合です。

- ドメイン名の形式の「%d\%w」(ドメイン名\ユーザ名)のような名前ではなく、「%w」(Windowsユーザ名)または「%u」(マッピングされたUNIXユーザ名)のような単純な名前を使用するようにCIFSホームディレクトリが設定されている。
- ホームディレクトリ共有の作成時に、「HOME」のような静的な名前ではなく、変数(「%w」または「%u」)を使用してCIFSホームディレクトリ共有の名前が設定されている。

SMB 2.xクライアントとSMB 3.0クライアントの場合は、自動ノード リファールを使用してホーム ディレクトリにアクセスする際に特別な考慮事項はありません。

#### 参照接続が確立されているCIFSサーバで自動ノード リファールを無効にする場合の考慮事項

自動ノード リファールのオプションを有効から無効に切り替えた場合、参照LIFに現在接続されているクライアントでは参照接続が維持されます。Data ONTAPではSMB自動ノード リファールのメカニズムとしてDFSリファールを使用しているため、オプションを無効にしたあとも、参照接続用にクライアントにキャッシュされているDFSリファールがタイムアウトするまでは参照LIFに再接続できます。これは、自動ノード リファールがサポートされないバージョンのData ONTAPにリバートした場合も同様です。クライアントは、クライアントのキャッシュからDFSリファールがタイムアウトするまで、引き続きリファールを使用します。

#### Mac OSクライアントで自動ノード リファールを使用する際の考慮事項

Mac OSはMicrosoftのDistributed File System (DFS;分散ファイルシステム)をサポートしていますが、Mac OS XクライアントはSMB自動ノード リファールをサポートしていません。Windowsクライアントは、SMB共有に接続する前にDFSリファール要求を行います。clustered Data ONTAPは、要求されたデータをホストしているノード上で見つかったデータLIFへのリファールを提供します。これによって、クライアントの応答時間が短縮されます。Mac OSでもDFSはサポートされますが、Mac OSクライアントの動作はWindowsクライアントとまったく同じではありません。

#### 関連コンセプト

[ホーム ディレクトリの管理](#) (327ページ)

#### 関連情報

[clustered Data ONTAP 8.3 ネットワーク管理ガイド](#)

[NetApp Interoperability](#)

### 自動ノード リファールのサポート

自動ノード リファールを有効にする際に、Data ONTAPの一部の機能ではリファールがサポートされない点に注意してください。

- 自動ノード リファールは、次の種類のボリュームではサポートされません。
  - 負荷共有ミラーの読み取り専用のメンバー
  - データ保護ミラーのデスティネーション ボリューム
- LIFが移動してもノード リファールは移動しません。  
クライアントがSMB 2.xまたはSMB 3.0接続を介した参照接続を使用している場合、データLIFが無停止で移動してもクライアントは引き続き同じ参照接続を使用します。LIFがデータに対してローカルでなくなった場合も同様です。
- ボリュームが移動してもノード リファールは移動しません。  
クライアントがいずれかのSMB接続による参照接続を使用している場合、ボリュームが無停止で移動してもクライアントは引き続き同じ参照接続を使用します。ボリュームがデータLIFと異なるノードに移動した場合も同様です。
- ノード リファールは、Hyper-V over SMB構成を含むStorage Virtual Machine (SVM) ではサポートされていません。  
無停止のフェイルオーバーにかかる時間を短縮するためにHyper-V over SMBソリューションで監視プロトコルを使用する場合は、自動ノード リファールを有効にしないでください。



## SMB自動ノード リファールルの有効化と無効化

SMB自動ノード リファールルを有効にして、SMBクライアント アクセスのパフォーマンスを向上させることができます。Data ONTAPでSMBクライアントを参照しないようにするには、自動ノード リファールルを無効にします。

### 開始する前に

FlexVolを備えたStorage Virtual Machine (SVM) でCIFSサーバが設定されて実行されている必要があります。

### タスク概要

自動ノード リファールルの有効と無効はSVMベースで切り替えます。この機能はデフォルトでは無効になっています。自動ノード リファールルは、Hyper-V over SMB構成を含むSVMではサポートされません。SVMでHyper-V over SMB構成がホストされている場合は、このオプションをfalseに設定する必要があります。

このオプションは、advanced権限レベルで使用できます。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| SMB自動ノード リファールルの設定 | 入力するコマンド                                                                                  |
|--------------------|-------------------------------------------------------------------------------------------|
| 有効                 | <code>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</code>  |
| 無効                 | <code>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</code> |

このオプション設定は、新しいSMBセッションで有効になります。既存の接続を使用しているクライアントは、その既存のキャッシュがタイムアウトになったときにのみノード リファールルを利用できます。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

### 関連参照情報

[使用できるCIFSサーバオプション](#) (71ページ)

## 統計を使用した自動ノード リファールル アクティビティの監視

参照されるSMB接続の数を確認するには、statisticsコマンドを使用して自動ノード リファールルのアクティビティを監視します。リファールルを監視することで、自動リファールルによって共有をホストするノードに対して接続が割り当てられている範囲を把握し、データLIFを再配分してCIFSサーバの共有へのローカル アクセスを向上させるべきかどうかを判断することができます。

### タスク概要

cifsオブジェクトに、SMB自動ノード リファールルの監視に役立つadvanced権限レベルのカウンタがいくつか用意されています。

- **node\_referral\_issued**  
共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントのうち、共有のルートのノードへのリファerralが発行されたクライアントの数。
- **node\_referral\_local**  
共有のルートと同じノードでホストされるLIFを使用して接続したクライアントの数。一般に、ローカル アクセスを使用するとパフォーマンスが最適化されます。
- **node\_referral\_not\_possible**  
共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントのうち、共有のルートホストするノードへのリファerralが発行されていないクライアントの数。この状況は、共有のルートのノードに対するアクティブなデータLIFが見つからない場合に発生します。
- **node\_referral\_remote**  
共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントの数。リモートアクセスを使用するとパフォーマンスが低下することがあります。

一定期間内のデータ(サンプル)を収集して表示することにより、Storage Virtual Machine (SVM) の自動ノード リファerral統計を監視できます。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しなければ、以前のクエリとの比較に使用できる更新されたデータを入手できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

**注:** `statistics` コマンドで収集した情報を評価および使用するには、環境でクライアントがどのように分散しているかを把握しておく必要があります。

`statistics` コマンドの詳細については、『*clustered Data ONTAP システム アドミニストレーションガイド(クラスタ管理)*』を参照してください。

#### 手順

1. 権限レベルを `advanced` に設定します。  
**set -privilege advanced**
2. `statistics` コマンドを使用して、自動ノード リファerralの統計を表示します。

#### 例

次に、一定のサンプリング時間におけるデータを収集して表示することにより、自動ノード リファerralの統計を表示する例を示します。

- a. 収集を開始します。

```
statistics start -object cifs -instance vs1 -sample-id sample1
```

```
Statistics collection is being started for Sample-id: sample1
```

- b. 目的の収集時間が経過するまで待ちます。
- c. 収集を停止します。

```
statistics stop -sample-id sample1
```

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. 自動ノード リファerralの統計を表示します。

```
statistics show -sample-id sample1 -counter *node*
```

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

| Counter                    | Value |
|----------------------------|-------|
| node_name                  | node1 |
| node_referral_issued       | 0     |
| node_referral_local        | 1     |
| node_referral_not_possible | 2     |
| node_referral_remote       | 2     |
| ...                        |       |
| node_name                  | node2 |
| node_referral_issued       | 2     |
| node_referral_local        | 1     |
| node_referral_not_possible | 0     |
| node_referral_remote       | 2     |
| ...                        |       |

出力には、SVM vs1に含まれるすべてのノードのカウンタが表示されます。この例では、わかりやすいように、自動ノード リファール統計に関連する出力フィールドだけを示してあります。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

#### 関連タスク

[統計情報の表示](#)(313ページ)

## Windowsクライアントを使用してクライアント側のSMB自動ノード リファール情報を監視する方法

クライアント側から発行されているリファールを確認するには、Windowsのdfsutil.exeユーティリティが使用できます。

dfsutil.exeユーティリティは、Windows 7以降のクライアントで使用できるRemote Server Administration Tools (RSAT; リモート サーバ管理ツール) キットに含まれています。このユーティリティを使用すると、リファール キャッシュの内容に関する情報を表示できるほか、クライアントで現在使用されている各リファールに関する情報を表示できます。また、このユーティリティを使用して、クライアントのリファール キャッシュを消去することもできます。詳細については、Microsoft TechNetライブラリを参照してください。

#### 関連情報

[Microsoft TechNetライブラリ: technet.microsoft.com/ja-jp/library/](http://technet.microsoft.com/ja-jp/library/)

## アクセスベースの列挙を使用した共有のフォルダのセキュリティ確保

アクセスベースの列挙 (ABE) がSMB共有で有効になっていると、共有内のフォルダまたはファイルに (個人またはグループの権限制限により) アクセスする権限がないユーザの環境には、その共有リソースは表示されません。

従来の共有プロパティでは、共有内のファイルまたはフォルダの表示や変更権限を保有するユーザ (個人またはグループ) を指定できます。ただし、権限のないユーザに対して共有内のフォルダやファイルを表示可能とするかどうかを制御することはできません。この状態だと、共有内のこれらのフォルダ名またはファイル名に、顧客名や開発中の製品などの重要な情報が記述されている場合に問題になることがあります。

ABEでは、共有プロパティが強化され、共有内のファイルやフォルダの列挙表示も対象になりました。このため、ABEを使用して、ユーザの権限に基づいて共有内のファイルやフォルダの表示をフィルタリングすることができます。職場の重要な情報を保護することに加え、ABEを使用すると大きなディレクトリ構造の表示を簡略化できるので、ディレクトリ全体にアクセスする必要のないユーザにはメリットです。

## SMB共有でのアクセスベースの列挙の有効化と無効化

SMB共有でAccess-Based Enumeration (ABE;アクセスベースの列挙)を有効または無効にすると、ユーザがアクセス権のない共有リソースを表示することを許可または禁止できます。

### タスク概要

デフォルトでは、ABEは無効です。

### 手順

1. 次のいずれかを実行します。

| 状況              | 入力するコマンド                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しい共有でABEを有効にする | <pre><b>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</b></pre> <p><i>path</i>には、共有のパスを指定します。パスの区切り文字には、スラッシュまたはバックスラッシュを使用できますが、Data ONTAPでは、どちらもスラッシュとして表示されます。</p> <p>SMB共有の作成時に、追加のオプション共有設定や追加の共有プロパティを指定できます。詳細については、<code>vserver cifs share create</code>コマンドのマニュアル ページを参照してください。</p> |
| 既存の共有でABEを有効にする | <pre><b>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</b></pre> <p>既存の共有プロパティは維持されます。ABE共有プロパティは既存の共有プロパティリストに追加されます。</p>                                                                                                                                                                        |
| 既存の共有でABEを無効にする | <pre><b>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</b></pre> <p>その他の共有プロパティは維持されます。ABE共有プロパティのみが共有プロパティリストから削除されます。</p>                                                                                                                                                                    |

2. `vserver cifs share show`コマンドを使用して、共有設定が正しいことを確認します。

### 例

次の例では、Storage Virtual Machine (SVM、旧Vserver) `vs1`上でパス`/sales`を使用して「sales」という名前のABE SMB共有を作成します。この共有は、共有プロパティとして **access-based-enumeration**を使用して作成されます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path /
sales -share-properties access-based-enumeration,oplocks,browsable,change_notify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

Vserver: vs1
Share: sales
CIFS Server NetBIOS Name: VS1
```

```

Path: /sales
Share Properties: access-based-enumeration
                  oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

次の例では、**access-based-enumeration**共有プロパティを「data2」という名前のSMB共有に追加します。

```

cluster1::> vserver cifs share properties add -vserver vs1 -share-name data2
-share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration

```

#### 関連タスク

[CIFSサーバでのSMB共有の作成](#) (180ページ)

[既存のSMB共有に対する共有プロパティの追加または削除](#) (187ページ)

## Windowsクライアントからのアクセスベースの列挙の有効化と無効化

SMB共有でのAccess-Based Enumerationの有効化と無効化はWindowsクライアントから実行できるため、この共有設定はCIFSサーバに接続することなく編集できます。

#### 手順

1. ABEをサポートしているWindowsクライアントで次のコマンドを入力します。

```
abecmd [/enable | /disable] [/server CIFS_server_name] [/all |
share_name]
```

abecmdコマンドの詳細については、Windowsクライアントのマニュアルを参照してください。

## Microsoft Hyper-VおよびSQL Server over SMBソリューション用のData ONTAPの設定

Data ONTAP 8.2以降では、新たにSMB 3.0のファイル共有の継続的な可用性が確保されるようになったため、FlexVolを備えたStorage Virtual Machine(SVM)にあるボリュームにHyper-V仮想マシン ファイルまたはSQL Serverシステム データベースおよびユーザ データベースを格納すると同時に、計画的イベントと計画外イベントの間のノンストップ オペレーション(NDO)を実現できます。

### Microsoft Hyper-V over SMB

Hyper-V over SMBソリューションを作成するには、まず、Microsoft Hyper-Vサーバにストレージ サービスを提供するようにData ONTAPを設定する必要があります。また、Microsoftクラスタ(クラスタ構成を使用する場合)、Hyper-Vサーバ、CIFSサーバによってホストされている共有へのSMB 3.0の継続的な可用性が確保された接続、および必要に応じてSVMボリュームに格納されている仮想マシン ファイルを保護するためのバックアップ サービスも設定する必要があります。

**注:** Hyper-Vサーバは、Windows Server 2012以降で設定する必要があります。Hyper-Vサーバの構成については、スタンドアロンの構成とクラスタ化された構成の両方がサポートされます。

- MicrosoftクラスタおよびHyper-Vサーバの作成については、MicrosoftのWebサイトを参照してください。
- SnapManager for Hyper-Vは、Snapshotコピーベースの高速バックアップ サービスを容易に実現できるホストベースのアプリケーションで、Hyper-V over SMB構成と統合できるように設計されています。

Hyper-V over SMB構成でのSnapManagerの使用については、『*SnapManager for Hyper-V Installation and Administration Guide*』を参照してください。

### Microsoft SQL Server over SMB

SQL Server over SMBソリューションを作成するには、まず、Microsoft SQLサーバアプリケーションにストレージ サービスを提供するようにData ONTAPを設定する必要があります。さらに、Microsoftクラスタも設定する必要があります(クラスタ構成を使用する場合)。その後、WindowsサーバにSQL Server 2012をインストールして設定し、CIFSサーバにホストされている共有への継続的な可用性を備えたSMB 3.0接続を作成します。SVMボリュームに格納されているデータベース ファイルを保護するオプションで、バックアップ サービスを設定することもできます。

**注:** SQL Serverは、Windows Server 2012以降にインストールし、設定する必要があります。構成については、スタンドアロンの構成とクラスタ化された構成の両方がサポートされます。

- Microsoftクラスタの作成およびSQL Server 2012のインストールと設定については、MicrosoftのWebサイトを参照してください。
- SnapManager for Microsoft SQL Serverは、Snapshotコピーベースの高速バックアップ サービスを容易に実現できるホストベースのアプリケーションで、SQL Server over SMB構成と統合できるように設計されています。

SnapManager for Microsoft SQL Serverの使用については、『*SnapManager for Microsoft SQL Serverインストール アドミニストレーション ガイド*』を参照してください。

## Hyper-VおよびSQL Server over SMBのノンストップ オペレーションとは

Hyper-VおよびSQL Server over SMBのノンストップ オペレーションとは、さまざまな管理作業の間も、アプリケーション サーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま

ま維持して、継続的な可用性を実現できる機能の組み合わせのことです。これには、ストレージインフラの計画的停止と計画外停止の両方が含まれます。

SMBを介したアプリケーション サーバのノンストップ オペレーションでは、次のような操作がサポートされます。

- 計画的なテイクオーバーとギブバック
- 計画外のテイクオーバー
- アップグレード
  - 無停止アップグレード(NDU)を実行するには、クラスタ内のすべてのノードで、この機能がサポートされるバージョンのclustered Data ONTAPが実行されている必要があります。
    - Hyper-V over SMBソリューションのNDUが最初にサポートされたのはData ONTAP 8.2です。そのため、無停止アップグレードは、クラスタ内のすべてのノードでData ONTAP 8.2リリース ファミリーでのアップグレードを含むData ONTAP 8.2以降が実行されている場合にサポートされます。
    - SQL Server over SMBソリューションのNDUが最初にサポートされたのはData ONTAP 8.2.1です。そのため、無停止アップグレードは、クラスタ内のすべてのノードでData ONTAP 8.2.1リリース ファミリーでのアップグレードを含むData ONTAP 8.2.1以降が実行されている場合にサポートされます。
- 計画的なアグリゲートの再配置 (ARL)
- LIFの移行とフェイルオーバー
- 計画的なボリュームの移動

#### 関連コンセプト

[Hyper-VおよびSQL Server over SMBでのノンストップ オペレーションの主要な概念](#)(383ページ)

[リモートVSSの概念](#)(387ページ)

## SMB経由のノンストップ オペレーションを実現するプロトコル

SMB 3.0のリリースに伴い、Microsoftから、Hyper-VおよびSQL Server over SMBのノンストップ オペレーションのサポートに必要な機能を備えた新しいプロトコルがリリースされました。

Data ONTAPでは、SMBを介したアプリケーション サーバのノンストップ オペレーションを実現するために、それらのプロトコルを使用しています。

- SMB 3.0
- 監視

#### 関連コンセプト

[SMB 3.0の機能がSMB共有を介したノンストップ オペレーションをサポートする仕組み](#)(385ページ)

[透過的なフェイルオーバーを強化するための監視プロトコルの機能](#)(385ページ)

## Hyper-VおよびSQL Server over SMBでのノンストップ オペレーションの主要な概念

Hyper-V over SMBおよびSQL Server over SMBソリューションを設定する前に理解しておくべきノンストップ オペレーション (NDO) の概念があります。

#### 共有の継続的な可用性

継続的に使用可能な共有プロパティが適切に設定されているSMB3.0共有。継続的に利用可能な共有を介して接続しているクライアントは、テイクオーバー、ギブバック、お

よびアグリゲート移転などの破壊的なイベントが発生しても、運用が中断されることはありません。

## ノード

クラスタのメンバーである単一のコントローラ。SFOペアの2つのノードを区別するために、1つのノードをローカル ノードと呼び、もう1つのノードをパートナー ノードまたはリモート ノードと呼ぶことがあります。ストレージのプライマリ所有者はローカル ノードです。セカンダリ所有者は、プライマリ所有者に障害が発生したストレージを制御するパートナー ノードです。各ノードは、そのストレージのプライマリ所有者と、そのパートナー ストレージのセカンダリ所有者で構成されます。

## 無停止でのアグリゲートの再配置

クライアント アプリケーションを中断することなく、クラスタのSFOペア内のパートナー ノード間でアグリゲートを移動できること。

## 運用停止不要のフェイルオーバー

テイクオーバーを参照。

## 運用停止不要のLIFの移行

LIFを介してクラスタに接続されたクライアント アプリケーションを中断することなく、LIFを移行できること。SMB接続の場合は、SMB 2.0以降を使用して接続するクライアントに対してのみ可能です。

## ノンストップ オペレーション

クライアント アプリケーションを中断することなく、clustered Data ONTAPの主な管理およびアップグレード操作を行え、ノード障害に堪えられること。全体として、この用語は運用停止不要のテイクオーバー、運用停止不要のアップグレード、および運用停止不要の移行などが可能であることを指します。

## 運用停止不要のアップグレード

アプリケーションを中断することなく、ノードのハードウェアまたはソフトウェアをアップグレードできること。

## 運用停止不要のボリューム移動

ボリュームを使用しているすべてのアプリケーションを中断することなく、クラスタ内で自由にボリュームを移動できること。SMB接続の場合、SMBのすべてのバージョンで運用停止不要のボリューム移動がサポートされます。

## 永続的ハンドル

接続が切断した場合に、継続的に使用可能な接続が透過的にCIFSサーバに再接続できるように設定するSMB 3.0のプロパティ。永続性ハンドルと同様に、接続中のクライアントとの通信が失われた後の期間、CIFSサーバによって永続的ハンドルが維持されます。ただし、永続的ハンドルは、永続性ハンドルよりも弾力性があります。CIFSサーバは、再接続後のクライアントにハンドルを60秒間使用する猶予を与え、その60秒間は、ファイルへのアクセスを要求する他のクライアントからのアクセスを拒否します。

永続的ハンドルに関する情報はSFOパートナーの永続的ストレージにミラー化されます。これにより、永続的ハンドルを切断したクライアントが、SFOパートナーによってノードのストレージの所有権が引き継がれた後に、永続性ハンドルを再利用することができるようになります。永続的ハンドルは、LIFの移動(永続性ハンドルによってサポートされる)が発生した場合だけでなく、テイクオーバー、ギブバック、およびアグリゲートの再配置の場合も運用を中断しません。

## SFOギブバック

テイクオーバー イベントから戻るときにホーム位置にアグリゲートを戻します。

## SFOペア

2つのノードのどちらかが機能を停止した場合に相互にデータを処理するようにコントローラが設定されたノードのペアを指します。システム モデルに応じて、両方のコントローラ



ラを1つのシャーンに配置することも、別々のシャーンに配置することもできます。2ノード クラスタでのHAペアを指します。

### テイクオーバー

ストレージのプライマリ所有者が失敗したときに、パートナーがストレージの制御を引き継ぐプロセスです。SFOの文脈では、フェイルオーバーとテイクオーバーは同義です。

### 関連コンセプト

[リモートVSSの概念](#) (387ページ)

[透過的なフェイルオーバーを強化するための監視プロトコルの機能](#) (385ページ)

## SMB 3.0の機能がSMB共有を介したノンストップ オペレーションをサポートする仕組み

SMB 3.0には、Hyper-V over SMBおよびSQL Server over SMB共有のノンストップ オペレーションをサポートするためのきわめて重要な機能があります。これには、新しいcontinuously-available共有プロパティや、永続的ハンドルと呼ばれる新しいタイプのファイルハンドルがあり、これらを使用すると、SMBクライアントは、ファイル オープン状態を再要求してSMB接続を透過的に再確立することができます。

永続的ハンドルは、継続的な可用性が設定された共有に接続するSMB 3.0対応のクライアントに付与できます。SMBセッションが切断された場合、CIFSサーバは永続的ハンドルの状態に関する情報を保持します。CIFSサーバは、クライアントが再接続できる60秒間は他のクライアント要求をブロックするため、永続的ハンドルを持つクライアントは、ネットワークの切断後にハンドルを再要求できます。永続的ハンドルを持つクライアントは、Storage Virtual Machine (SVM) のデータLIFのいずれかを使用して、同じLIFまたは別のLIFを介して再接続できます。

アグリゲートの再配置、テイクオーバー、およびギブバックはすべて、SFOペア間で行われます。永続的ハンドルを持つファイルを使用したセッションの切断と再接続をシームレスに管理するために、パートナー ノードでは、すべての永続的ハンドルのロック情報のコピーが保持されます。イベントが計画的か計画外かに関係なく、SFOパートナーは、永続的ハンドルの再接続を無停止で管理できます。この新機能を使用すると、従来では業務が停止する状況となるイベントでも、CIFSサーバへのSMB 3.0接続を、SVMに割り当てられた別のデータLIFに透過的に無停止でフェイルオーバーできます。

永続的ハンドルを使用すると、CIFSサーバでSMB 3.0接続を透過的にフェイルオーバーできるようになりますが、障害が発生したためにHyper-VアプリケーションがWindows Server 2012クラスタ内の別のノードにフェイルオーバーされる場合、クライアントは切断されたハンドルのファイルハンドルを再要求できません。このシナリオでは、切断された状態のファイルハンドルによって、別のノードで再起動したHyper-Vアプリケーションのアクセスがブロックされる可能性があります。SMB 3.0には、古い競合するハンドルを無効にするメカニズムを提供してこのシナリオに対処する「フェイルオーバー クラスタリング」が用意されています。このメカニズムを使用すると、Hyper-Vクラスタノードに障害が発生した場合に、Hyper-Vクラスタを迅速にリカバリできるようになります。

### 関連コンセプト

[サポートされるSMB 3.0の機能](#) (107ページ)

### 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#) (403ページ)

[SMB 3.0の有効化と無効化](#) (109ページ)

[継続的な可用性を確保するための既存の共有の設定](#) (414ページ)

## 透過的なフェイルオーバーを強化するための監視プロトコルの機能

監視プロトコルにより、SMB 3.0の継続的な可用性が確保された共有 (CA共有) に対するクライアントフェイルオーバー機能が強化されます。監視を使用すると、LIFのフェイルオーバーのリカバリ

がバイパスされるため、フェイルオーバーにかかる時間が短縮されます。ノードを使用できなくなると、SMB 3.0接続のタイムアウトを待たずにアプリケーション サーバに通知されます。

フェイルオーバーはシームレスです。実行中のアプリケーションは、フェイルオーバーが発生したことを認識しません。監視プロトコルを使用できなくてもフェイルオーバー処理に影響はありませんが、監視プロトコルを使用しないフェイルオーバーは効率が落ちます。

監視プロトコルを使用する高度なフェイルオーバーは、以下の要件が満たされた場合に実行できます。

- SMB 3.0が有効になっているSMB 3.0対応のCIFSサーバでのみ使用できる。
- 共有で、共有の継続的な可用性プロパティが設定されているSMB 3.0を使用している。
- アプリケーション サーバの接続先のノードのSFOパートナーに、少なくとも1つ以上、アプリケーション サーバのデータをホスティングするStorage Virtual Machine (SVM)に割り当てられた運用中のデータLIFがある。

注: 監視プロトコルは、SFOペアの間に実行されます。LIFはクラスタ内の任意のノードに移行できるため、すべてのノードがそのSFOパートナーの監視プロトコルであることが必要になる場合があります。

アプリケーション サーバのデータをホスティングしているSVMがパートナー ノード上にアクティブなデータLIFを持っていない場合、監視プロトコルは、指定されたノード上でSMB接続の迅速なフェイルオーバーを提供することはできません。したがって、そのような構成の1つをホスティングしているSVMには、クラスタ内のすべてのノードに少なくとも1つ以上のデータLIFが必要です。

- アプリケーション サーバは、個々のLIFのIPアドレスではなく、DNSに格納されているCIFSサーバ名を使用してCIFSサーバに接続している必要があります。

#### 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#) (403ページ)

[LIFステータスの確認](#) (424ページ)

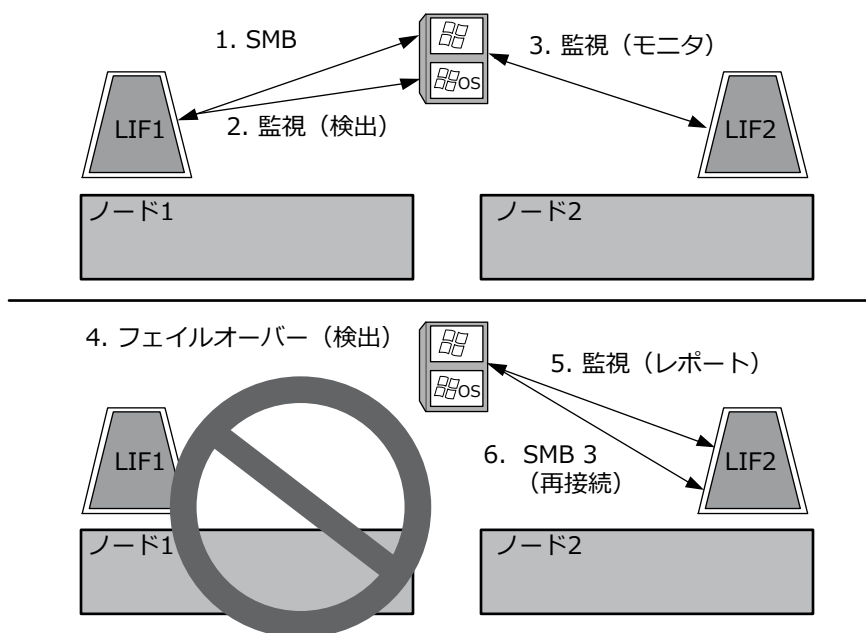
#### 監視プロトコルの仕組み

Data ONTAPでは、ノードのSFOパートナーを監視役として使用して、監視プロトコルを実装します。障害発生時には、パートナーが障害を迅速に検出し、SMBクライアントに通知します。

監視プロトコルでは、次のプロセスを使用してフェイルオーバーが強化されます。

1. アプリケーション サーバがノード1への継続的な可用性が確保されたSMB接続を確立すると、CIFSサーバからアプリケーション サーバに監視が利用可能であることが通知されます。
2. アプリケーション サーバは、ノード1に監視サーバのIPアドレスを要求し、Storage Virtual Machine (SVM)に割り当てられたノード2 (SFOパートナー) のデータLIFのIPアドレス リストを受け取ります。
3. アプリケーション サーバは、いずれかのIPアドレスを選択し、ノード2への監視接続を作成して、ノード1の継続的な可用性が確保された接続を移行する必要がある場合に通知されるように登録します。
4. ノード1でフェイルオーバーが発生した場合、監視によってフェイルオーバーが容易になりますが、ギブバックには影響しません。
5. 監視によってフェイルオーバー イベントが検出され、監視接続を介してアプリケーション サーバに、SMB接続をノード2に移行する必要があることが通知されます。

6. アプリケーション サーバは、SMBセッションをノード2に移行し、クライアント アクセスを中断することなく接続をリカバリします。



## リモートVSSによる共有ベースのバックアップ

リモートVSSを使用して、CIFSサーバに格納されたHyper-V仮想マシン ファイルの共有ベースのバックアップを実行できます。

MicrosoftのリモートVSS(ボリューム シャドウ コピー サービス)は、既存のMicrosoft VSSインフラを拡張したものです。これまでのVSSを使用したバックアップ サービスはローカル ディスクに格納されたデータだけに対応しており、ローカル ディスクまたはSANベースのストレージのいずれかにデータを格納するアプリケーションへのVSSの使用に制限がありました。リモートVSSでは、SMB共有のシャドウ コピーにも対応するようにVSSインフラが拡張され、Hyper-Vなどのサーバ アプリケーションでSMBファイル共有にVHDファイルを格納できるようになりました。これらの新しい拡張機能により、データと構成ファイルを共有に格納する仮想マシンについて、アプリケーションと整合性のあるシャドウ コピーを作成できます。

### 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#)(403ページ)

[Hyper-V over SMBバックアップでのVSSシャドウ コピーの有効化と無効化](#)(416ページ)

## リモートVSSの概念

ここでは、リモートVSS(ボリューム シャドウ コピー サービス)の概念について説明します。リモートVSSがHyper-V over SMB構成でバックアップ サービスによってどのように使用されるかを理解するには、これらの概念を理解しておく必要があります。

### VSS(ボリューム シャドウ コピー サービス)

特定のボリューム上のデータの特定の時点におけるバックアップ コピー(スナップショット)を作成するMicrosoftのテクノロジーです。データ サーバ、バックアップ アプリケーション、およびストレージ管理ソフトウェアを調整して、整合性のあるバックアップの作成と管理をサポートします。

### リモートVSS(リモート ボリューム シャドウ コピー サービス)

SMB 3.0共有を介してデータにアクセスした特定の時点における整合性が取れた共有ベースのバックアップ コピーを作成するMicrosoftのテクノロジーです。単にボリューム シャドウ コピー サービスと呼ぶこともあります。

### シャドウ コピー

共有に含まれるデータセットの明確に定義された特定の時点における複製です。シャドウ コピーを使用すると、システムやアプリケーションによる元のボリュームのデータ更新を継続したまま、整合性が取れたポイントインタイム バックアップを作成できます。

### シャドウ コピー セット

1つ以上のシャドウ コピーの集合です。各シャドウ コピーが1つの共有に対応します。シャドウ コピー セット内のシャドウ コピーに対応する共有は、すべて同じ処理でバックアップする必要があります。セットに含めるシャドウ コピーは、VSSに対応したアプリケーションのVSSクライアントで識別されます。

### シャドウ コピー セットの自動リカバリ

リモートVSSに対応したバックアップ アプリケーションのバックアップ プロセスの一部で、シャドウ コピーを格納するレプリカ ディレクトリのある時点での整合性が確保されます。バックアップの開始時に、アプリケーションのVSSクライアントで、バックアップ対象としてスケジュールされたデータ(Hyper-Vの場合は仮想マシン ファイル)にソフトウェア チェックポイントを設定する処理が開始されます。そのあと、VSSクライアントでアプリケーションの実行を継続できます。シャドウ コピー セットが作成されると、リモートVSSによってシャドウ コピー セットが書き込み可能にされ、書き込み可能なコピーがアプリケーションに公開されます。アプリケーションでは、シャドウ コピー セットをバックアップする準備として、前の処理で作成されたソフトウェア チェックポイントを使用して自動リカバリを実行します。自動リカバリでは、チェックポイントの作成後にファイルやフォルダに対して行われた変更を元に戻すことで、シャドウ コピーを整合性が取れた状態にします。自動リカバリは、VSSに対応したバックアップ向けのオプションの手順です。

### シャドウ コピーID

シャドウ コピーを一意に識別するGUIDです。

### シャドウ コピー セットID

同じサーバに対する一連のシャドウ コピーIDを一意に識別するGUIDです。

### SnapManager for Hyper-V

Microsoft Windows Server 2012 Hyper-Vのバックアップとリストアの処理を自動化して簡単に実行できるようにするソフトウェアです。SnapManager for Hyper-Vでは、リモートVSSと自動リカバリを使用して、SMB共有を介してHyper-Vファイルをバックアップします。

### 関連コンセプト

[Hyper-VおよびSQL Server over SMBでのノンストップ オペレーションの主要な概念](#)(383ページ)  
[リモートVSSによる共有ベースのバックアップ](#)(387ページ)

## リモートVSSで使用されるディレクトリ構造の例

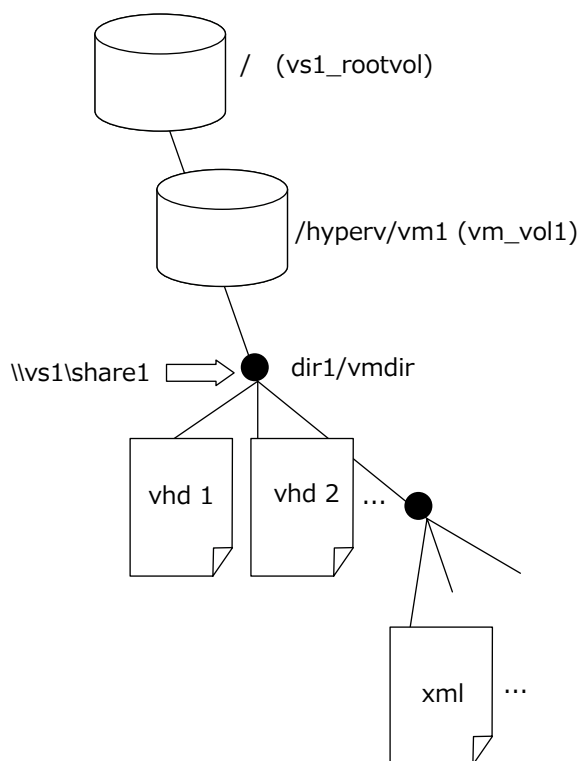
リモートVSSは、シャドウ コピーの作成時に、Hyper-V仮想マシン ファイルが格納されているディレクトリ構造をトラバースします。仮想マシン ファイルが正常にバックアップされるようにするため、適切なディレクトリ構造について理解しておくことが重要です。

シャドウ コピーを正常に作成するためにサポートされるディレクトリ構造は、次の要件を満たしています。

- 仮想マシン ファイルの格納に使用されるディレクトリ構造内に存在するのは、ディレクトリと通常のファイルだけです。  
ディレクトリ構造にはジャンクション、リンク、通常以外のファイルは含まれません。

- 仮想マシンのファイルはすべて単一の共有内に存在します。
- 仮想マシン ファイルの格納に使用されるディレクトリ構造は、設定されたシャドウ コピーのディレクトリ階層より深くなりません。
- 共有のルート ディレクトリには、仮想マシン ファイルまたはディレクトリのみが格納されます。

次の例では、Storage Virtual Machine (SVM) vs1上で/hyperv/vm1をジャンクション ポイントとしてvm\_vol1という名前のボリュームが作成されています。ジャンクション ポイントの下には仮想マシン ファイルを格納するサブディレクトリが作成されています。Hyper-Vサーバの仮想マシン ファイルには、パスが/hyperv/vm1/dir1/vmdirのshare1を経由してアクセスします。シャドウ コピー サービスによって、share1の下ディレクトリ構造内(設定されたシャドウ コピーのディレクトリ階層まで)に格納されたすべての仮想マシン ファイルのシャドウ コピーが作成されます。



## SnapManager for Hyper-VによるHyper-V over SMBのリモートVSSベースのバックアップの管理方法

SnapManager for Hyper-Vを使用して、リモートVSSベースのバックアップ サービスを管理できます。スペース効率に優れたバックアップ セットを作成するには、SnapManager for Hyper-Vで管理されているバックアップ サービスを使用すると役立ちます。

SnapManager for Hyper-Vで管理されているバックアップの最適化には、次のようなものがあります。

- SnapDriveとData ONTAPの統合により、SMB共有の場所を検出する際のパフォーマンスが最適化されます。  
Data ONTAPは、共有が存在するボリュームの名前をSnapDriveに提供します。
- SnapManager for Hyper-Vは、シャドウ コピー サービスでコピーする必要があるSMB共有内の仮想マシン ファイルのリストを指定します。  
仮想マシン ファイルの対象リストを指定することにより、シャドウ コピー サービスで、共有内のすべてのファイルのシャドウ コピーを作成する必要がなくなります。

- Storage Virtual Machine(SVM)に、SnapManager for Hyper-Vがリストアに使用するための Snapshotコピーが保持されます。  
バックアップ フェーズはありません。バックアップは、スペース効率に優れたSnapshotコピーです。

SnapManager for Hyper-Vは、次のプロセスを使用して、Hyper-V over SMBのバックアップとリストアの機能を提供します。

1. シャドウ コピー処理の準備  
SnapManager for Hyper-VアプリケーションのVSSクライアントが、シャドウ コピー セットを設定します。VSSクライアントは、どの共有をシャドウ コピー セットに含めるかに関する情報を収集し、この情報をData ONTAPに提供します。セットには1つ以上のシャドウ コピーが含まれる場合があり、1つのシャドウ コピーが1つの共有に対応します。
2. シャドウ コピー セットの作成(自動リカバリが使用される場合)  
シャドウ コピー セットに含まれている共有ごとに、Data ONTAPがシャドウ コピーを作成し、シャドウ コピーを書き込み可能にします。
3. シャドウ コピー セットの公開  
Data ONTAPによって作成されたシャドウ コピーがSnapManager for Hyper-Vに公開され、アプリケーションのVSSライターが自動リカバリを実行できるようになります。
4. シャドウ コピー セットの自動リカバリ  
シャドウ コピー セットの作成中に、バックアップ セットに含まれているファイルにアクティブな変更が発生する時間帯があります。アプリケーションのVSSライターは、シャドウ コピーを更新して、バックアップ前に完全な整合性が確保された状態にする必要があります。  
  
注: 自動リカバリの実行方法はアプリケーションに固有です。リモートVSSはこのフェーズには関連しません。
5. シャドウ コピー セットの完了とクリーンアップ  
自動リカバリの完了後に、VSSクライアントがData ONTAPに通知します。シャドウ コピー セットが読み取り専用になり、バックアップできる状態になります。バックアップにSnapManager for Hyper-Vを使用する場合は、Snapshotコピー内のファイルがバックアップになるため、バックアップフェーズでは、バックアップ セット内の共有を含むボリュームごとにSnapshotコピーが作成されます。バックアップが完了したら、シャドウ コピー セットがCIFSサーバから削除されます。

## Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピー オフロードの使用方法

Offloaded Data Transfer(ODX;オフロード データ転送)はコピー オフロードとも呼ばれ、この機能を使用すると、互換性があるストレージ デバイス内やストレージ デバイス間で、ホストコンピュータを介さずにデータを直接転送できます。Data ONTAP ODXコピー オフロードを使用すると、アプリケーション サーバでSMB環境経由のコピー処理を実行する際のパフォーマンスが向上します。

ODX以外のファイル転送では、ソースCIFSサーバからデータが読み取られ、ネットワーク経由でクライアント コンピュータに転送されます。クライアント コンピュータは、データをネットワーク経由でデスティネーションCIFSサーバに転送します。つまり、クライアント コンピュータがソースからデータを読み取り、デスティネーションに書き込みます。ODXファイル転送では、データはソースからデスティネーションに直接コピーされます。

ODXオフロード コピーはソース ストレージとデスティネーション ストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量(CPU、メモリ)の削減、ネットワークI/O帯域幅の使用量の削減などが挙げられます。

この機能は、Windows Server 2012サーバで利用できます。Data ONTAP ODXコピー オフロードは、SAN LUNとSMB 3.0の継続的な可用性が確保された接続の両方でサポートされます。



ODXコピーおよび移動の使用は、以下の事例でサポートされます。

- ボリューム内  
ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。
- ボリュームが異なり、ノードとStorage Virtual Machine (SVM) は同じ  
ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。
- ボリュームとノードが異なり、SVMは同じ  
ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。
- SVMが異なり、ノードは同じ  
ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは異なるSVMに所有されます。
- SVMとノードが異なる  
ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは異なるSVMに所有されます。

Hyper-VソリューションでのODXコピー オフロードの具体的な用途には、次のようなものがあります。

- Hyper-VでODXコピー オフロードのパススルーを使用して、Virtual Hard Disk (VHD; 仮想ハード ディスク) ファイル内およびVHDファイル間でのデータのコピー、または同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でのデータのコピーを実行できます。これにより、ゲスト オペレーティング システムからのコピーを基盤となるストレージに渡すことができます。
- 容量固定VHDを作成する際に、ODXを使用して、既知の初期化済みトークンによってディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、ODXコピー オフロードを使用して、仮想マシンのストレージを移行します。

**注:** Hyper-VでのODXコピー オフロードのパススルーの用途を活用するには、ゲスト オペレーティング システムでODXがサポートされている必要があります。また、ゲスト オペレーティング システムのディスクが、ODXをサポートするストレージ (SMBまたはSAN) から作成されたSCSIディスクである必要があります。ゲスト オペレーティング システムのディスクがIDEディスクの場合、ODXのパススルーはサポートされません。

SQL ServerソリューションでのODXコピー オフロードの具体的な用途には、次のようなものがあります。

- ODXコピー オフロードを使用して、マッピングされたSMB共有間、または同じクラスタ内のSMB共有と接続されたiSCSI LUNの間でSQL Serverデータベースのエクスポートとインポートを行うことができます。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、ODXコピー オフロードを使用して、データベースのエクスポートとインポートを行います。

## 関連コンセプト

[Microsoftリモート コピーのパフォーマンスの向上](#) (368ページ)

## 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#) (403ページ)

## 設定要件と考慮事項

NDO over SMB共有用のSQL ServerおよびHyper-Vアプリケーション サーバを計画して設定する際は、いくつかの要件と考慮事項について検討する必要があります。

### 関連コンセプト

[Hyper-VまたはSQL Server over SMB構成の計画](#)(400ページ)

[Hyper-V over SMB構成をリポートする際の考慮事項](#)(417ページ)

### 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#)(403ページ)

## Data ONTAPとライセンスの要件

FlexVolを備えたSVMでノンストップ オペレーションを実現するSQL Server over SMBまたはHyper-V over SMBソリューションを作成するときは、Data ONTAPとライセンスの特定の要件について理解しておく必要があります。

Infinite Volumeを備えたSVMでは、Hyper-V over SMBおよびSQL Server over SMBソリューションはサポートされません。

### Data ONTAPのバージョン要件

- Hyper-V over SMB  
clustered Data ONTAP 8.2以降のリリースでは、Windows Server 2012以降で実行されるHyper-VでSMB共有を介したノンストップ オペレーションがサポートされます。
- SQL Server over SMB  
8.2リリース ファミリーのclustered Data ONTAP 8.2.1以降のリリースでは、Windows Server 2012以降で実行されるSQL Server 2012以降でSMB共有を介したノンストップ オペレーションがサポートされます。

SMB共有を介したノンストップ オペレーションがサポートされるData ONTAP、Windows Server、およびSQL Serverのバージョンの最新情報については、Interoperability Matrix ([mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix))を参照してください。

### ライセンス要件

次のライセンスが必要です。

- CIFS
- FlexClone(Hyper-V over SMBのみ)  
このライセンスは、バックアップにリモートVSSを使用する場合に必要になります。シャドウ コピー サービスでは、バックアップの作成時に使用されるファイルのポイントインタイム コピーを作成するためにFlexCloneが使用されます。  
リモートVSSを使用しないバックアップ方式を使用する場合、FlexCloneライセンスはオプションです。



## ネットワークとデータLIFの要件

ノンストップ オペレーション用にSQL ServerまたはHyper-V over SMB構成を作成する場合、一定のネットワークとデータLIF要件について理解しておく必要があります。

### ネットワーク プロトコルの要件

- IPv4およびIPv6のネットワークがサポートされています。
- SMB 3.0以降が必要です。  
SMB 3.0には、ノンストップ オペレーションを実現するために必要となる継続的な可用性が確保されたSMB接続の確立に欠かせない機能が備わっています。
- DNSサーバには、CIFSサーバ名をStorage Virtual Machine (SVM) 上のデータLIFに割り当てられたIPアドレスにマッピングするエントリが格納されている必要があります。  
通常、Hyper-VまたはSQL Serverアプリケーション サーバは、仮想マシンまたはデータベース ファイルへのアクセス時に複数のデータLIFを介して複数の接続を確立します。正常に機能するには、アプリケーション サーバは、複数の一意のIPアドレスへの複数の接続を確立するのではなく、CIFSサーバ名を使用してこのような複数のSMB接続を確立する必要があります。監視でも、個々のLIF IPアドレスではなくCIFSサーバのDNS名を使用する必要があります。

### データLIFの要件

- SMB経由のアプリケーション サーバソリューションをホストするSVMには、クラスタ内のすべてのノードに稼働しているデータLIFが少なくとも1つが必要です。  
SVMデータLIFは、アプリケーション サーバがアクセスするデータを現在ホストしていないノードを含む、クラスタ内の他のデータ ポートにフェイルオーバーできます。さらに、監視ノードは常に、アプリケーション サーバが接続されているノードのSFOパートナーであるため、クラスタ内のどのノードも監視ノードになる可能性があります。
- データLIFは、自動的にリバートされるように設定されていない必要があります。  
テイクオーバーまたはギブバックの発生後は、データLIFをホーム ポートに手動でリバートする必要があります。
- データLIFのすべてのIPアドレスがDNS内にエントリを保持する必要があります。すべてのエントリがCIFSサーバ名に解決される必要があります。  
アプリケーション サーバは、CIFSサーバ名を使用してSMB共有に接続する必要があります。LIF IPアドレスを使用して接続を確立するようにアプリケーション サーバを設定しないでください。
- CIFSサーバ名がSVM名と異なる場合は、DNSエントリがCIFSサーバ名に解決される必要があります。

## Hyper-V over SMB用のCIFSサーバとボリュームの要件

ノンストップ オペレーション用にHyper-V over SMB構成を作成する場合、一定のCIFSサーバとボリュームの要件について理解しておく必要があります。

### CIFSサーバの要件

- SMB 3.0が有効になっている必要があります。  
この機能は、デフォルトで有効に設定されています。
- デフォルトのUNIXユーザのCIFSサーバ オプションが、有効なUNIXユーザ アカウントを使用して設定されている必要があります。  
アプリケーション サーバでは、SMB接続を確立する際にマシン アカウントが使用されます。すべてのSMBアクセスで、Windowsユーザが任意のUNIXユーザ アカウントまたはデフォルトのUNIXユーザ アカウントに正常にマッピングされる必要があるため、Data ONTAPは、アプリケ

ーション サーバのマシン アカウントをデフォルトのUNIXユーザ アカウントにマッピングできる必要があります。

- 自動ノードリファールが無効になっている必要があります。  
自動ノードリファールは、デフォルトでは無効になっています。Hyper-Vマシン ファイル以外のデータにアクセスするために自動ノードリファールを使用する場合は、そのデータ用に別のSVMを作成する必要があります。
- CIFSサーバが属しているドメインで、KerberosとNTLMの両方の認証が許可されている必要があります。  
Data ONTAPではリモートVSSに対してKerberosサービスがアダプタイズされないため、ドメインはNTLMを許可するように設定されている必要があります。
- シャドウ コピー機能が有効になっている必要があります。  
この機能は、デフォルトで有効に設定されています。
- シャドウ コピー サービスでシャドウ コピーの作成時に使用されるWindowsドメイン アカウントが、CIFSサーバのローカルのBUILTIN\AdministratorsグループまたはBUILTIN\Backup Operatorsグループに属している必要があります。

### ボリュームの要件

- 仮想マシン ファイルを格納するためのボリュームは、NTFSセキュリティ形式のボリュームとして作成されている必要があります。  
継続的な可用性が確保されたSMB接続を使用してアプリケーション サーバのNDOを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、そのボリュームが以前から一貫してNTFSボリュームであることも必要です。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをNDOs over SMB共有で直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、NDOs over SMB共有に使用する場合、ボリュームの一番上にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ソース ボリュームまたはデスティネーション ボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベース ファイルのエクスポートとインポートに失敗する可能性があります。
- シャドウ コピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です。  
利用可能なスペースは、シャドウ コピー バックアップ セットに含まれている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される総スペースと同サイズ以上である必要があります。この要件は、自動リカバリを使用するシャドウ コピーにのみ適用されます。

### 関連情報

[Microsoft TechNetライブラリ: technet.microsoft.com/ja-jp/library/](https://technet.microsoft.com/ja-jp/library/)

## SQL Server over SMB用のCIFSサーバとボリュームの要件

ノンストップ オペレーション用にSQL Server over SMB構成を作成する場合、CIFSサーバとボリュームの要件について理解しておく必要があります。

### CIFSサーバの要件

- SMB 3.0が有効になっている必要があります。  
この機能は、デフォルトで有効に設定されています。

- デフォルトのUNIXユーザのCIFSサーバ オプションが、有効なUNIXユーザ アカウントを使用し  
て設定されている必要があります。  
アプリケーション サーバでは、SMB接続を確立する際にマシン アカウントが使用されます。す  
べてのSMBアクセスで、Windowsユーザが任意のUNIXユーザ アカウントまたはデフォルトの  
UNIXユーザ アカウントに正常にマッピングされる必要があるため、Data ONTAPは、アプリケ  
ーション サーバのマシン アカウントをデフォルトのUNIXユーザ アカウントにマッピングできる  
必要があります。  
さらに、SQL Serverはドメイン ユーザをSQL Serverサービス アカウントとして使用します。サー  
ビス アカウントは、デフォルトUNIXユーザにもマッピングする必要があります。
- 自動ノード リファールが無効になっている必要があります。  
自動ノード リファールは、デフォルトでは無効になっています。SQL Serverデータベース ファ  
イル以外のデータへのアクセスに自動ノード リファールを使用する場合、そのデータ用の  
SVMを個別に作成する必要があります。
- Data ONTAP上のSQL Serverのインストールに使用するWindowsユーザ アカウントには、  
SeSecurityPrivilege権限を割り当てる必要があります。  
この権限は、CIFSサーバのローカルBUILTIN\Administratorsグループに割り当てられます。

### ボリュームの要件

- 仮想マシン ファイルを格納するためのボリュームは、NTFSセキュリティ形式のボリュームとし  
て作成されている必要があります。  
継続的な可用性が確保されたSMB接続を使用してアプリケーション サーバのNDOを実現する  
には、共有を含むボリュームがNTFSボリュームである必要があります。さらに、そのボリュー  
ムが以前から一貫してNTFSボリュームであることも必要です。mixedセキュリティ形式のボリュー  
ムまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更  
し、そのボリュームをNDOs over SMB共有で直接使用することはできません。mixedセキュリテ  
ィ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、NDOs over SMB共有に  
使用する場合、ボリュームの一番上にACLを手動で配置し、格納されているすべてのファイ  
ルおよびフォルダにそのACLを適用する必要があります。そうしないと、ソース ボリュームまた  
はデスティネーション ボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式  
のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合は、ファイルを別  
のボリュームに移動する仮想マシンの移行またはデータベース ファイルのエクスポートとイン  
ポートに失敗する可能性があります。
- データベース ファイルが格納されたボリュームにジャンクションを含めることはできますが、  
SQL Serverはデータベース ディレクトリ構造の作成時にジャンクションを横断しません。
- SnapManager for Microsoft SQL Serverのバックアップ処理を正常に実行するには、ボリューム  
に十分な利用可能スペースが必要です。  
SQL Serverデータベース ファイルを配置するボリュームには、共有内にあるデータベース ディ  
レクトリ構造と、格納されているすべてのファイルを保持できる十分な容量が必要です。

### 関連情報

*Microsoft TechNetライブラリ: [technet.microsoft.com/ja-jp/library/](http://technet.microsoft.com/ja-jp/library/)*

## Hyper-V over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップ オペレーションをサポートするHyper-V over SMB構成で継続的可用性を備えた共有を  
設定する場合は、いくつかの要件と考慮事項に注意する必要があります。

### 共有の要件

- アプリケーション サーバが使用する共有には、継続的可用性が設定されている必要がありま  
す。

継続的可用性を備えた共有に接続するアプリケーション サーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイル ロックを再取得することができます。

- リモートVSSに対応したバックアップ サービスを使用する場合は、ジャンクションを含む共有にHyper-Vファイルを配置することはできません。  
自動リカバリの場合、共有のトラバース時にジャンクションが見つかり、シャドウ コピーの作成は失敗します。自動リカバリではない場合、シャドウ コピーの作成は失敗しませんが、ジャンクションは何も参照しません。
- リモートVSSに対応したバックアップ サービスと自動リカバリを使用する場合は、以下を含む共有にHyper-Vファイルを配置することはできません。
  - シンボリック リンク、ハードリンク、またはワイドリンク
  - 通常以外のファイル  
シャドウ コピーを実行する共有にリンクまたは通常以外のファイルが含まれている場合は、シャドウ コピーの作成に失敗します。この要件は、自動リカバリを使用するシャドウ コピーにのみ適用されます。
  - シャドウ コピー処理を実行するには、ボリュームに十分な利用可能スペースが必要です (Hyper-V over SMBの場合のみ)。  
利用可能なスペースは、シャドウ コピー バックアップ セットに含まれている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される総スペースと同サイズ以上である必要があります。この要件は、自動リカバリを使用するシャドウ コピーにのみ適用されます。
- アプリケーション サーバが使用する継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホーム ディレクトリ
  - 変更通知
  - 属性のキャッシュ
  - BranchCache
  - アクセスベースの列挙

**注:** 変更通知が無効になっていると、Windows Server 2012ではエクスプローラ ウィンドウが更新されないため、ディレクトリ内容の表示に整合性がなくなります。

## 考慮事項

- 継続的可用性を備えた共有では、クォータはサポートされません。  
クォータを指定した場合でも、継続的可用性を備えた共有ではクォータ ポリシーは無視されません。
- Hyper-V over SMB構成では、次の機能はサポートされません。
  - 監査
  - FPolicy
- continuously-availabilityパラメータがYesに設定されているSMB共有ではウィルススキャンが実行されません。

## SQL Server over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップ オペレーションをサポートするSQL Server over SMB構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項に注意する必要があります。

### 共有の要件

- 仮想マシン ファイルを格納するためのボリュームは、NTFSセキュリティ形式のボリュームとして作成されている必要があります。  
 継続的可用性を備えたSMB接続を使用してアプリケーション サーバのノンストップ オペレーションを実現するには、共有が含まれるボリュームがNTFSボリュームである必要があります。さらに、そのボリュームが以前から一貫してNTFSボリュームであることも必要です。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップ オペレーションに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップ オペレーションに使用する場合は、ボリュームの一番上にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ソース ボリュームまたはデスティネーション ボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベース ファイルのエクスポートとインポートに失敗する可能性があります。
- アプリケーション サーバが使用する共有には、継続的可用性が設定されている必要があります。  
 継続的可用性を備えた共有に接続するアプリケーション サーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイル ロックを再取得することができます。
- データベース ファイルが格納されたボリュームにジャンクションを含めることはできますが、SQL Serverはデータベース ディレクトリ構造の作成時にジャンクションを横断しません。
- SnapManager for Microsoft SQL Serverのバックアップ処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です。  
 SQL Serverデータベース ファイルを配置するボリュームには、共有内にあるデータベース ディレクトリ構造と、格納されているすべてのファイルを保持できる十分な容量が必要です。
- アプリケーション サーバが使用する継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホーム ディレクトリ
  - 変更通知
  - 属性のキャッシュ
  - BranchCache
  - アクセススペースの列挙

**注:** 変更通知が無効になっていると、Windows Server 2012ではエクスプローラ ウィンドウが更新されないため、ディレクトリ内容の表示に整合性がなくなります。

### 共有の考慮事項

- 継続的可用性を備えた共有では、クォータはサポートされません。  
 クォータを指定した場合でも、継続的可用性を備えた共有ではクォータ ポリシーは無視されません。

- SQL Server over SMB構成では、次の機能はサポートされません。
  - 監査
  - FPolicy
- continuously-availability共有プロパティが設定されているSMB共有ではウィルススキャンが実行されません。

## Hyper-V over SMB構成用のリモートVSSの考慮事項

Hyper-V over SMB構成用のリモートVSSに対応したバックアップ ソリューションを使用する場合は、一定の考慮事項について理解しておく必要があります。

### 一般的なりモートVSSの考慮事項

- Microsoftのアプリケーション サーバ1つにつき、最大64の共有を設定できます。1つのシャドウ コピー セットに64個を超える共有がある場合、シャドウ コピー処理は失敗します。これはMicrosoftの要件です。
- アクティブなシャドウ コピー セットは、1台のCIFSサーバで1つしか許可されません。シャドウ コピー処理は、同じCIFSサーバ上で別の シャドウ コピー処理が進行中である場合には失敗します。これはMicrosoftの要件です。
- リモートVSSによってシャドウ コピーが作成されるディレクトリ構造内では、ジャンクションは許可されません。
  - 自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、シャドウ コピーの作成は失敗します。
  - 自動リカバリではない場合、シャドウ コピーの作成は失敗しませんが、ジャンクションは何も参照しません。

### 自動リカバリを行うシャドウ コピーのみに適用されるリモートVSSの考慮事項

一部の制限は、自動リカバリを行うシャドウ コピーのみに適用されます。

- シャドウ コピーの作成で許可される最大サブディレクトリ階層は5層です。これは、シャドウ コピー サービスによってシャドウ コピー バックアップ セットが作成されるディレクトリ階層です。仮想マシン ファイルを格納するディレクトリのネストレベルが5よりも深い場合、シャドウ コピーの作成は失敗します。この目的は、共有のクローニング時におけるディレクトリのトラバースを制限することです。最大ディレクトリ階層はCIFSサーバ オプションを使用して変更できます。
- ボリューム上に利用可能なスペースが十分ある必要があります。利用可能なスペースは、シャドウ コピー バックアップ セットに含まれている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される総スペースと同サイズ以上である必要があります。
- リモートVSSによってシャドウ コピーが作成されるディレクトリ構造内では、リンクおよび通常以外のファイルは許可されません。シャドウ コピーの作成は、そのシャドウ コピーに対応する共有内にリンクまたは通常以外のファイルがある場合には失敗します。これらのリンクおよびファイルは、クローニング プロセスでサポートされていません。
- ディレクトリに対するNFSv4 ACLは許可されません。シャドウ コピーの作成では、ファイルのNFSv4 ACLは維持されますが、ディレクトリのNFSv4 ACLは失われます。
- シャドウ コピー セットの作成に許可される時間は最大60秒です。

Microsoftの仕様により、シャドウ コピー セットの作成に許可される時間は最大60秒です。この時間内にVSSクライアントでシャドウ コピー セットを作成できなかった場合、シャドウ コピー 処理は失敗します。したがって、シャドウ コピー セット内のファイル数には制限があります。バックアップ セットに含めることができる実際のファイル数または仮想マシン数は、一定ではなく、多くの要因に依存するので、お客様の環境ごとに判断する必要があります。

## SQL ServerおよびHyper-V over SMB用のODXコピー オフロード要件

アプリケーション サーバ経由で送信せずに、直接ソース ストレージからデスティネーション ストレージに仮想マシン ファイルを移行する場合やデータベース ファイルをエクスポートしてインポートするには、ODXコピー オフロードが有効になっている必要があります。ODXコピー オフロードとSQL ServerおよびHyper-V over SMBソリューションを使用する場合は、理解しておくべきいくつかの要件があります。

ODXコピー オフロードを使用すると、パフォーマンスが大幅に向上します。このCIFSサーバ オプションは、デフォルトで有効に設定されています。

- ODXコピー オフロードを使用するには、SMB 3.0が有効になっている必要があります。
- ソース ボリュームは1.25GB以上でなければなりません。
- コピー オフロードに使用するボリュームで重複排除を有効にする必要があります。
- コピー オフロードに使用するボリュームで圧縮を有効にしてはなりません。
- ODXコピー オフロードを使用してHyper-Vゲストをディスク内やディスク間で移行するには、Hyper-VサーバがSCSIディスクを使用するように設定されている必要があります。  
デフォルトではIDEディスクが設定されますが、ディスクがIDEディスクを使用して作成されている場合は、ゲストの移行時にODXコピー オフロードは機能しません。

## SQL ServerおよびHyper-V over SMB構成に関する推奨事項

SQL Server over SMBおよびHyper-V over SMB環境が安定して機能するようにするには、ソリューションの設定に関するベスト プラクティスについて理解しておく必要があります。

### 一般的な推奨事項

- アプリケーション サーバのファイルは一般的なユーザ データとは別に格納します。  
可能な場合は、Storage Virtual Machine (SVM) とそのストレージ全体をアプリケーション サーバのデータ専用にしします。
- パフォーマンスを最大限に高めるには、アプリケーション サーバのデータを格納するSVMでSMB署名を無効にします。
- Hyper-VまたはSQL Server over SMB構成で使用する共有以外では、継続的な可用性が確保された共有を作成しないようにします。
- 継続的な可用性を確保するための共有では変更通知を無効にします。
- ARLには一部の処理が一時的に停止するフェーズがあるため、ARLと同時にボリュームの移動を実行しないようにします。
- Hyper-V over SMBソリューションでは、仮想マシンを作成するときや既存の仮想マシンにディスクを追加するときは、iSCSIドライブを使用します。

## Hyper-VまたはSQL Server over SMB構成の計画

ノンストップ オペレーション用にHyper-VまたはSQL Server over SMBを設定する前に、設定を作成する際に必要となる選択肢について理解しておく必要があります。この作業は、ベストプラクティスと推奨事項に従った構成を行うのに役立ちます。

### 関連コンセプト

[設定要件と考慮事項](#)(392ページ)

### 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#)(403ページ)

## ボリューム設定ワークシートの完了

このワークシートを使うと、SQL ServerおよびHyper-V over SMB構成用のボリュームを作成する際に必要となる値を簡単に記録できます。

ボリュームごとに、次の情報を指定する必要があります。

- Storage Virtual Machine(SVM)名  
SVM名はすべてのボリュームで同じです。
- ボリューム名
- アグリゲート名  
ボリュームは、クラスタ内のノード上のアグリゲートに作成できます。
- サイズ
- ジャンクション パス

アプリケーション サーバのデータを格納するボリュームの作成時には、次の事項を考慮してください。

- ルート ボリュームのセキュリティ形式がNTFSでない場合は、ボリュームの作成時にセキュリティ形式をNTFSとして指定する必要があります。  
デフォルトで、ボリュームはSVMルート ボリュームのセキュリティ形式を継承します。
- ボリュームは、デフォルトのボリューム スペース ギャランティを使用して設定する必要があります。
- 必要に応じて、スペースのオートサイズ管理を設定できます。
- Snapshotコピーのスペース リザーベーションを決めるオプションは0に設定する必要があります。
- ボリュームに適用されるSnapshotポリシーを無効にする必要があります。  
SVMのSnapshotポリシーが無効になっている場合は、ボリュームのSnapshotポリシーを指定する必要はありません。ボリュームはSVMのSnapshotポリシーを継承します。SVMのSnapshotポリシーが無効になっておらず、Snapshotコピーを作成するように設定されている場合は、Snapshotポリシーをボリューム レベルで指定し、そのポリシーを無効にする必要があります。  
Snapshotコピーの作成と削除は、シャドウ コピー サービス対応のバックアップとSQL Serverバックアップによって管理されます。
- ボリュームの負荷共有ミラーを設定することはできません。



アプリケーション サーバで使用される共有を作成するジャンクション パスを選択する際は、共有エントリ ポイントの下に結合されたボリュームが含まれないようにする必要があります。

たとえば、「vol1」、「vol2」、「vol3」、および「vol4」という名前の4つのボリュームに仮想マシン ファイルを格納する場合は、例に示すネームスペースを作成できます。その後、アプリケーション サーバの共有をパス/data1/vol1、/data1/vol2、/data1/vol3、および/data1/vol4に作成できます。

| Vserver | Volume | Junction Active | Junction Path | Junction Path Source |
|---------|--------|-----------------|---------------|----------------------|
| vs1     | data1  | true            | /data1        | RW_volume            |
| vs1     | vol1   | true            | /data1/vol1   | RW_volume            |
| vs1     | vol2   | true            | /data1/vol2   | RW_volume            |
| vs1     | data2  | true            | /data2        | RW_volume            |
| vs1     | vol3   | true            | /data2/vol3   | RW_volume            |
| vs1     | vol4   | true            | /data2/vol4   | RW_volume            |

| 情報の種類                                 | 値 |
|---------------------------------------|---|
| ボリューム1: ボリューム名、アグリゲート、サイズ、ジャンクション パス  |   |
| ボリューム2: ボリューム名、アグリゲート、サイズ、ジャンクション パス  |   |
| ボリューム3: ボリューム名、アグリゲート、サイズ、ジャンクション パス  |   |
| ボリューム4: ボリューム名、アグリゲート、サイズ、ジャンクション パス  |   |
| ボリューム5: ボリューム名、アグリゲート、サイズ、ジャンクション パス  |   |
| ボリューム6: ボリューム名、アグリゲート、サイズ、ジャンクション パス  |   |
| 追加ボリューム: ボリューム名、アグリゲート、サイズ、ジャンクション パス |   |

## SMB共有設定ワークシートの完了

このワークシートを使用して、SQL ServerおよびHyper-V over SMB構成用に継続的な可用性を実装したSMB共有を作成する際に必要となる値を記録してください。

### SMB共有のプロパティおよび設定に関する情報

共有ごとに、次の情報を指定する必要があります。

- Storage Virtual Machine (SVM) 名  
SVM名はすべての共有で同じです。
- 共有名
- パス
- 共有プロパティ  
次の2つの共有プロパティを設定する必要があります。
  - oplocks
  - continuously-available

次の共有プロパティは設定しないでください。

- **homedirectory**
- **changenotify**
- **attributecache**
- **branchcache**
- **access-based-enumeration**

注: 変更通知が無効になっていると、Windows Server 2012ではエクスプローラ ウィンドウが更新されないため、ディレクトリ内容の表示に整合性がなくなります。

- シンボリック リnkは無効にする必要があります(-symlink-propertiesパラメータの値を null[""])にする必要があります)。

共有パスに関する情報

リモートVSSを使用してHyper-Vファイルをバックアップする場合は、Hyper-Vサーバから仮想マシン ファイルの格納場所へのSMB接続を確立する際に使用する共有パスの選択が重要になります。共有はネームスペース内の任意のポイントに作成できますが、Hyper-Vサーバで使用される共有のパスに結合されたボリュームを含めることはできません。ジャンクション ポイントを含む共有パスでシャドウ コピー処理を実行することはできません。

データベース ディレクトリ構造を作成する場合、SQL Serverはジャンクションを横断できません。ジャンクション ポイントを含むSQL Serverの共有パスは作成しないでください。

たとえば、次に示すネームスペースを例にとると、仮想マシン ファイルまたはデータベース ファイルをボリューム「vol1」、「vol2」、「vol3」、および「vol4」に格納する場合は、アプリケーション サーバの共有をパス/data1/vol1、/data1/vol2、/data2/vol3、および/data2/vol4に作成する必要があります。

| Vserver | Volume | Junction Active | Junction Path | Junction Path Source |
|---------|--------|-----------------|---------------|----------------------|
| vs1     | data1  | true            | /data1        | RW_volume            |
| vs1     | vol1   | true            | /data1/vol1   | RW_volume            |
| vs1     | vol2   | true            | /data1/vol2   | RW_volume            |
| vs1     | data2  | true            | /data2        | RW_volume            |
| vs1     | vol3   | true            | /data2/vol3   | RW_volume            |
| vs1     | vol4   | true            | /data2/vol4   | RW_volume            |

注: 管理用に/data1と/data2のパスに共有を作成することはできますが、データの格納にこれらの共有を使用するようにアプリケーション サーバを設定してはいけません。

計画ワークシート

| 情報の種類              | 値 |
|--------------------|---|
| ボリューム1:SMB共有名およびパス |   |
| ボリューム2:SMB共有名およびパス |   |
| ボリューム3:SMB共有名およびパス |   |
| ボリューム4:SMB共有名およびパス |   |
| ボリューム5:SMB共有名およびパス |   |

| 情報の種類               | 値 |
|---------------------|---|
| ボリューム6:SMB共有名およびパス  |   |
| ボリューム7:SMB共有名およびパス  |   |
| 追加ボリューム:SMB共有名およびパス |   |

## Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成

SMBを介したノンストップ オペレーションを実現するHyper-VおよびSQL Server環境を使用するためには、Data ONTAPのさまざまな設定手順を実行する必要があります。

### 開始する前に

Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成を作成する前に、次のタスクを完了する必要があります。

- クラスタでタイム サービスをセットアップします。
- SVM用のネットワークをセットアップします。
- SVMを作成します。
- SVMでデータLIFインターフェイスを設定します。
- SVMでDNSを設定します。
- SVMに必要なネーム サービスをセットアップします。
- CIFSサーバを作成します。

### 手順

1. [Kerberos認証およびNTLMv2認証の許可の確認\(Hyper-V over SMB共有\)](#) (404ページ)  
Hyper-V over SMBのノンストップ オペレーションを実行する場合、データSVMのCIFSサーバおよびHyper-VサーバでKerberos認証とNTLMv2認証の両方が許可されていなければなりません。CIFSサーバとHyper-Vサーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。
2. [ドメイン アカウントがデフォルトのUNIXユーザにマッピングされていることの確認](#) (405ページ)  
Hyper-VおよびSQL Serverでは、継続的な可用性が確保された共有へのSMB接続を作成する際にドメイン アカウントを使用します。接続を作成するには、そのコンピュータ アカウントがUNIXユーザに正しくマッピングされている必要があります。そのための最も便利な方法が、コンピュータ アカウントをデフォルトのUNIXユーザにマッピングする方法です。
3. [SVMルート ボリュームのセキュリティ形式がNTFSに設定されていることの確認](#) (407ページ)  
Hyper-VおよびSQL Server over SMBのノンストップ オペレーションを実行する場合は、ボリュームをNTFSセキュリティ形式で作成する必要があります。ルート ボリュームのセキュリティ形式には、Storage Virtual Machine (SVM) で作成されたボリュームのデフォルトが適用されるため、ルート ボリュームのセキュリティ形式はNTFSに設定する必要があります。
4. [必要なCIFSサーバ オプションの設定の確認](#) (408ページ)  
Hyper-VおよびSQL Server over SMBのノンストップ オペレーションを実行する場合、必要なCIFSサーバ オプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。
5. [自動ノード リファラルの無効化の確認](#) (409ページ)  
自動ノード リファラルは、Hyper-VおよびSQL Server over SMB構成のノンストップ オペレーションではサポートされません。SMBを介したアプリケーション サーバのノンストップ オペレーション

ンを行うCIFSサーバでは、自動ノードリファールが無効になっていることを確認する必要があります。

#### 6. NTFSデータボリュームの作成 (410ページ)

Hyper-V over SMBまたはSQL Server over SMBアプリケーション サーバで使用する継続的可用性を備えた共有を設定する前に、Storage Virtual Machine (SVM) 上にNTFSデータ ボリュームを作成する必要があります。ボリューム設定ワークシートを使用して、データ ボリュームを作成します。

#### 7. 継続的可用性を備えたSMB共有の作成 (411ページ)

データ ボリュームを作成したら、アプリケーション サーバがHyper-V仮想マシンおよび構成ファイルとSQL Serverデータベース ファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

#### 8. ユーザ アカウント (SMB共有のSQL Server用) へのSeSecurityPrivilege権限の追加 (412ページ)

SQL Serverのインストールに使用するドメイン ユーザ アカウントには、デフォルトではドメイン ユーザに割り当てられない権限を必要とする特定の操作をCIFSサーバで実行するために、「SeSecurityPrivilege」権限を割り当てる必要があります。

#### 9. VSSシャドウ コピーのディレクトリ階層の設定 (Hyper-V over SMB要求用) (413ページ)

必要に応じて、シャドウ コピーを作成するSMB共有のディレクトリの最大階層を設定できます。このパラメータは、Data ONTAPによってシャドウ コピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

### 関連コンセプト

[Hyper-VまたはSQL Server over SMB構成の計画](#) (400ページ)

[設定要件と考慮事項](#) (392ページ)

### 関連タスク

[CIFSサーバの最低限の認証セキュリティレベルの設定](#) (84ページ)

## Kerberos認証およびNTLMv2認証の許可の確認 (Hyper-V over SMB共有)

Hyper-V over SMBのノンストップ オペレーションを実行する場合、データSVMのCIFSサーバおよびHyper-VサーバでKerberos認証とNTLMv2認証の両方が許可されていなければなりません。CIFSサーバとHyper-Vサーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。

### タスク概要

Kerberos認証は、継続的な可用性が確保された共有への接続を確立する際に必要になります。また、リモートVSSのプロセスでNTLMv2認証が使用されます。そのため、Hyper-V over SMB構成に対しては、両方の認証方法を使用した接続がサポートされている必要があります。

Kerberos認証とNTLMv2認証の両方が許可されるように、次の設定について確認する必要があります。

- Storage Virtual Machine (SVM) でSMBのエクスポート ポリシーが無効になっている必要があります。  
SVMでは、Kerberos認証とNTLMv2認証がどちらも常に有効になりますが、エクスポート ポリシーを使用することで認証方法に基づいてアクセスを制限することが可能です。  
Data ONTAP 8.2よりも前のリリースでは、SMBアクセスのエクスポート ポリシーの設定は必須であり、NASプロトコルを使用してデータにアクセスする際に使用できる認証の種類をエクスポート ポリシーで制御していました。

Data ONTAP 8.2以降のリリースでは、SMBのエクスポート ポリシーは省略可能になり、デフォルトで無効になっています。エクスポート ポリシーが無効になっていれば、CIFSサーバでKerberos認証とNTLMv2認証の両方がデフォルトで許可されます。

- CIFSサーバとHyper-Vサーバが属するドメインで、Kerberos認証とNTLMv2認証の両方を許可する必要があります。  
Kerberos認証は、Active Directoryドメインに対してデフォルトで有効になります。ただし、NTLMv2認証は、セキュリティ ポリシーの設定またはグループ ポリシーで禁止されている場合があります。

#### 手順

1. 次の手順に従って、SVMでエクスポート ポリシーが無効になっていることを確認します。
  - a. 権限レベルをadvancedに設定します。  
**set -privilege advanced**
  - b. `-is-exportpolicy-enabled` CIFSサーバ オプションがfalseに設定されていることを確認します。  
**vserver cifs options show -vserver vserver\_name -fields vserver,is-exportpolicy-enabled**
  - c. admin権限レベルに戻ります。  
**set -privilege admin**
2. SMBのエクスポート ポリシーが無効になっていない場合は無効にします。  
**vserver cifs options modify -vserver vserver\_name -is-exportpolicy-enabled false**
3. ドメインでNTLMv2認証とKerberos認証の両方が許可されていることを確認します。  
ドメインで許可されている認証方法を確認する方法については、Microsoft TechNetライブラリを参照してください。
4. ドメインでNTMLv2認証が許可されていない場合は、Microsoftのドキュメントに記載されたいずれかの方法でNTLMv2認証を有効にします。

#### 例

次に、SVM vs1でSMBのエクスポート ポリシーが無効になっていることを確認するコマンドの例を示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-----
vs1      false

cluster1::> set -privilege admin
```

### ドメイン アカウントがデフォルトのUNIXユーザにマッピングされていることの確認

Hyper-VおよびSQL Serverでは、継続的な可用性が確保された共有へのSMB接続を作成する際にドメイン アカウントを使用します。接続を作成するには、そのコンピュータ アカウントがUNIXユ

ーザに正しくマッピングされている必要があります。そのための最も便利な方法が、コンピュータアカウントをデフォルトのUNIXユーザにマッピングする方法です。

### タスク概要

Hyper-VおよびSQL Serverは、ドメイン コンピュータ アカウントを使用してSMB接続を作成します。さらに、SQL Serverはドメイン ユーザ アカウントをSMB接続を作成するサービス アカウントとして使用します。

Data ONTAP 8.2以降のリリースでは、Storage Virtual Machine (SVM)を作成する際にデフォルト ユーザ「pcuser」(UID **65534**)が自動的に作成され、そのユーザ「pcuser」が「pcuser」グループ (GID **65534**)に追加されます。クラスタをData ONTAP 8.2にアップグレードする前に使用していたSVMでHyper-V over SMBソリューションを設定する場合は、デフォルトのユーザとグループが存在していない可能性があります。その場合は、CIFSサーバのデフォルトのUNIXユーザを設定する前に、デフォルトのユーザとグループを作成する必要があります。

### 手順

1. デフォルトのUNIXユーザが存在するかどうかを確認します。  

```
vserver cifs options show -vserver vserver_name
```
2. デフォルト ユーザ オプションが設定されていない場合は、デフォルトのUNIXユーザとして指定できるUNIXユーザが存在するかどうかを確認します。  

```
vserver services unix-user show -vserver vserver_name
```
3. デフォルト ユーザ オプションが設定されておらず、デフォルトのUNIXユーザとして指定できるUNIXユーザも存在しない場合は、デフォルトのUNIXユーザとデフォルトのグループを作成し、デフォルトのユーザをそのグループに追加します。  

デフォルトのユーザの名前は通常は「pcuser」で、UID **65534**を割り当てる必要があります。デフォルトのグループの名前は通常は「pcuser」で、GIDは**65534**にする必要があります。

  - a. デフォルトのグループを作成します。  

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```
  - b. デフォルトのユーザを作成し、デフォルトのグループに追加します。  

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```
  - c. デフォルトのユーザとデフォルトのグループが正しく設定されていることを確認します。  

```
vserver services unix-user show -vserver vserver_name  
vserver services unix-group show -vserver vserver_name -members
```
4. CIFSサーバのデフォルトのユーザが設定されていない場合は、次の手順を実行します。
  - a. デフォルトのユーザを設定します。  

```
vserver cifs options modify -vserver vserver_name -default-unix-user pcuser
```
  - b. デフォルトのUNIXユーザが正しく設定されていることを確認します。  

```
vserver cifs options show -vserver vserver_name
```
5. アプリケーション サーバのコンピュータ アカウントがデフォルトのユーザに正しくマッピングされていることを確認するには、SVMの共有にドライブをマッピングし、`vserver cifs sessions show`コマンドを使用してWindowsユーザとUNIXユーザのマッピングを確認します。  

このコマンドを使用する方法については、マニュアル ページを参照してください。

**例**

次の例では、CIFSサーバのデフォルトのユーザが設定されていませんが、「pcuser」ユーザと「pcuser」グループは存在しています。SVM vs1で、CIFSサーバのデフォルトのユーザとして「pcuser」ユーザを割り当てています。

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group      : -
  Default Unix User       : -
  Guest Unix User         : -
  Read Grants Exec        : disabled
  Read Only Delete        : disabled
  WINS Servers            : -

cluster1::> vserver services unix-user show
Vserver  User      User   Group  Full
         Name      ID      ID      Name
-----
vs1      nobody    65535  65535  -
vs1      pcuser     65534  65534  -
vs1      root       0       1       -

cluster1::> vserver services unix-group show -members
Vserver  Name      ID
vs1      daemon    1
vs1      Users: -
vs1      nobody    65535
vs1      Users: -
vs1      pcuser     65534
vs1      Users: -
vs1      root       0
vs1      Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group      : -
  Default Unix User       : pcuser
  Guest Unix User         : -
  Read Grants Exec        : disabled
  Read Only Delete        : disabled
  WINS Servers            : -
```

## SVMルート ボリュームのセキュリティ形式がNTFSに設定されていることの確認

Hyper-VおよびSQL Server over SMBのノンストップ オペレーションを実行する場合は、ボリュームをNTFSセキュリティ形式で作成する必要があります。ルート ボリュームのセキュリティ形式には、Storage Virtual Machine (SVM) で作成されたボリュームのデフォルトが適用されるため、ルート ボリュームのセキュリティ形式はNTFSに設定する必要があります。

### タスク概要

- ルート ボリュームのセキュリティ形式はSVMの作成時に指定できます。
- SVMの作成時にルート ボリュームのセキュリティ形式をNTFS以外に設定した場合は、あとで volume modify コマンドを使用してセキュリティ形式を変更することができます。

**手順**

1. SVMのルート ボリュームの現在のセキュリティ形式を確認します。  
**volume show -vserver vs1 -fields vs1,volume,security-style**
2. ルート ボリュームのセキュリティ形式がNTFS以外になっている場合は、セキュリティ形式をNTFSに変更します。  
**volume modify -vserver vs1 -volume vs1\_root -security-style ntfs**
3. SVMのルート ボリュームのセキュリティ形式がNTFSに設定されていることを確認します。  
**volume show -vserver vs1 -fields vs1,volume,security-style**

**例**

次に、SVM vs1のルート ボリュームのセキュリティ形式がNTFSになっていることを確認するコマンドの例を示します。

```
cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vserver  volume      security-style
-----
vs1      vs1_root    unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style ntfs

cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vserver  volume      security-style
-----
vs1      vs1_root    ntfs
```

**必要なCIFSサーバ オプションの設定の確認**

Hyper-VおよびSQL Server over SMBのノンストップ オペレーションを実行する場合、必要なCIFSサーバ オプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。

**タスク概要**

- SMB 2.xとSMB 3.0が有効になっている必要があります。
- パフォーマンスが向上したコピー オフロードを使用するには、ODXコピー オフロードが有効になっている必要があります。
- Hyper-V over SMBソリューションでリモートVSSに対応したバックアップ サービスを使用する場合は、VSSシャドウ コピー サービスが有効になっている必要があります (Hyper-Vのみ)。

**手順**

1. Storage Virtual Machine (SVM) で必要なCIFSサーバ オプションが有効になっていることを確認します。
  - a. 権限レベルをadvancedに設定します。  
**set -privilege advanced**
  - b. 次のコマンドを入力します。  
**vserver cifs options show -vserver vs1**  
 次のオプションがtrueに設定されていることを確認します。
    - -smb2-enabled



- -smb3-enabled
- -copy-offload-enabled
- -shadowcopy-enabled (Hyper-Vのみ)

2. **true**に設定されていないオプションがある場合は、次の手順を実行します。
  - a. `vserver cifs options modify`コマンドを使用して、オプションを**true**に設定します。
  - b. `vserver cifs options show`コマンドを使用して、オプションが**true**に設定されていることを確認します。
3. admin権限レベルに戻ります。  
**set -privilege admin**

### 例

次に、SVM vs1について、Hyper-V over SMB構成の必要なオプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、ODXコピー オフロードのオプションを有効にする必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver  smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true         true         false         true

cluster-1::> vserver cifs options modify -vserver vs1 -copy-offload-enabled
true

cluster-1::> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

cluster1::> set -privilege admin
```

## 自動ノード リファールルの無効化の確認

自動ノード リファールルは、Hyper-VおよびSQL Server over SMB構成のノンストップ オペレーションではサポートされません。SMBを介したアプリケーション サーバのノンストップ オペレーションを行うCIFSサーバでは、自動ノード リファールルが無効になっていることを確認する必要があります。

### タスク概要

自動ノード リファールルは、デフォルトでは無効になっています。SMB共有を介したノンストップ サービスを提供するCIFSサーバで有効にした場合は、無効にする必要があります。

### 手順

1. 次の手順に従って、CIFSサーバで自動ノード リファールルが無効になっていることを確認します。
  - a. 権限レベルをadvancedに設定します。  
**set -privilege advanced**

- b. `-is-referral-enabled` CIFSサーバ オプションが`false`に設定されていることを確認します。

```
vserver cifs options show -vserver vserver_name -fields is-referral-enabled
```

2. 自動ノード リファールが無効になっていない場合は、次の手順を実行します。

- a. 自動ノード リファールを無効にします。

```
vserver cifs options modify -vserver vserver_name -is-referral-enabled false
```

- b. 新しい設定が正しいことを確認します。

```
vserver cifs options show -vserver vserver_name -fields is-referral-enabled
```

3. `admin`権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次のコマンドで、Storage Virtual Machine (SVM、旧Vserver) `vs1`の自動ノード リファールが無効になっていることを確認します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields is-referral-enabled

vserver  is-referral-enabled
-----
vs1      false

cluster1::*> set -privilege admin
```

## NTFSデータ ボリュームの作成

Hyper-V over SMBまたはSQL Server over SMBアプリケーション サーバで使用する継続的可用性を備えた共有を設定する前に、Storage Virtual Machine (SVM) 上にNTFSデータ ボリュームを作成する必要があります。ボリューム設定ワークシートを使用して、データ ボリュームを作成します。

### タスク概要

データ ボリュームのカスタマイズに使用できるオプションのパラメータが用意されています。ボリュームのカスタマイズの詳細については、『*clustered Data ONTAP 論理ストレージ管理ガイド*』を参照してください。

データ ボリュームの作成時に、次のファイルが格納されたボリューム内にはジャンクション ポイントを作成しないでください。

- Data ONTAPによってシャドウ コピーが生成されるHyper-Vファイル
- SQL Serverを使用してバックアップされるSQL Serverデータベース ファイル

**注:** mixedセキュリティ形式またはUNIXセキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームをNTFSセキュリティ形式のボリュームに変更して、ノンストップ オペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMBおよびSQL Server over SMBのノンストップ オペレーションは、この構成で使用するボリュームをNTFSセキュリティ形式のボリュームとして作成しないかぎり、適切に機能しません。

ボリュームを削除するか、NTFSセキュリティ形式を使用してボリュームを再作成する必要があります。または、Windowsホストにボリュームをマッピングし、ボリューム上にACLを適用して、ボリューム内のすべてのファイルとフォルダにACLを反映することができます。

#### 手順

1. 適切なコマンドを入力して、データ ボリュームを作成します。

| ボリュームを作成するSVM<br>のルート ボリュームのセキュ<br>リティ形式 | 入力するコマンド                                                                                                                                                                            |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NTFS                                     | <code>volume create -vserver vservers_name -volume<br/>volume_name -aggregate aggregate_name -size<br/>integer[KB MB GB TB PB] -junction-path path</code>                           |
| NTFS以外                                   | <code>volume create -vserver vservers_name -volume<br/>volume_name -aggregate aggregate_name -size<br/>integer[KB MB GB TB PB] -security-style ntfs -<br/>junction-path path</code> |

2. ボリューム設定が正しいことを確認します。

```
volume show -vserver vservers_name -volume volume_name
```

### 継続的可用性を備えたSMB共有の作成

データ ボリュームを作成したら、アプリケーション サーバがHyper-V仮想マシンおよび構成ファイルとSQL Serverデータベース ファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

#### 手順

1. 既存のデータ ボリュームとそのジャンクション パスに関する情報を表示します。

```
volume show -vserver vservers_name -junction
```

2. 次のコマンドを入力して、継続的可用性を備えたSMB共有を作成します。

```
vserver cifs share create -vserver vservers_name -share-name share_name -  
path path -share-properties oplocks,continuously-available -symlink ""  
[-comment text]
```

- 必要に応じて、コメントを共有設定に追加することもできます。
  - デフォルトでは、共有にはオフライン ファイル共有プロパティが設定され、`manual`に設定されます。
  - Windowsのデフォルトの共有権限である**Everyone / Full Control**が設定された共有が作成されます。
3. 共有設定ワークシートのすべての共有について前の手順を繰り返します。
  4. `vserver cifs share show`コマンドを使用して、設定が正しいことを確認します。
  5. ドライブを各共有にマッピングし、Windowsの[プロパティ]ウィンドウを使用してファイル権限を指定することで、継続的可用性を備えた共有のNTFSファイル権限を設定します。

**例**

次のコマンドを実行すると、「data2」という名前の継続的可用性を備えた共有がStorage Virtual Machine (SVM、旧Vserver) vs1に作成されます。シンボリックリンクを無効にするには、-symlinkパラメータを""に設定します。

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Junction Active | Junction Path | Junction Path Source |
|---------|----------|-----------------|---------------|----------------------|
| vs1     | data     | true            | /data         | RW_volume            |
| vs1     | data1    | true            | /data/data1   | RW_volume            |
| vs1     | data2    | true            | /data/data2   | RW_volume            |
| vs1     | vs1_root | -               | /             | -                    |

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path /
data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

## ユーザ アカウント(SMB共有のSQL Server用)へのSeSecurityPrivilege権限の追加

SQL Serverのインストールに使用するドメイン ユーザ アカウントには、デフォルトではドメイン ユーザに割り当てられない権限を必要とする特定の操作をCIFSサーバで実行するために、「SeSecurityPrivilege」権限を割り当てる必要があります。

### 開始する前に

SQL Serverのインストールに使用するドメイン アカウントがすでに存在している必要があります。

### タスク概要

SQL Serverインストーラのアカウントに権限を追加するときに、Data ONTAPがドメイン コントローラに照会してアカウントを検証することがあります。Data ONTAPからドメイン コントローラに照会できない場合、コマンドが失敗することがあります。

### 手順

1. 「SeSecurityPrivilege」権限を追加します。

```
vserver cifs users-and-groups privilege add-privilege -vserver
vserver_name -user-or-group-name account_name -privileges
SeSecurityPrivilege
```

-user-or-group-name/パラメータの値は、SQL Serverのインストールに使用するドメイン ユーザ アカウントの名前です。

2. 権限がアカウントに適用されていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name account_name
```

#### 例

次のコマンドを実行すると、Storage Virtual Machine (SVM) vs1のEXAMPLEドメインにあるSQL Serverインストーラのアカウントに「SeSecurityPrivilege」権限が追加されます。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver vs1 -user-or-group-name EXAMPLE\SQLInstaller -privileges SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name      Privileges
-----
vs1       EXAMPLE\SQLInstaller    SeSecurityPrivilege
```

## VSSシャドウ コピーのディレクトリ階層の設定(Hyper-V over SMB要求用)

必要に応じて、シャドウ コピーを作成するSMB共有のディレクトリの最大階層を設定できます。このパラメータは、Data ONTAPによってシャドウ コピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

#### 開始する前に

VSSシャドウ コピー機能を有効にする必要があります。

#### タスク概要

デフォルトでは、最大5個のサブディレクトリにシャドウ コピーが作成されます。値を0に設定した場合、すべてのサブディレクトリにシャドウ コピーが作成されます。

**注:** シャドウ コピー セットのディレクトリ階層は6個以上のサブディレクトリまたはすべてのサブディレクトリを含むことができますが、シャドウ コピー セットの作成は60秒以内に完了しなければならないというMicrosoftの要件があります。この時間内に完了できない場合、シャドウ コピー セットの作成は失敗します。作成時間がこの時間制限を超えないようにシャドウ コピーのディレクトリ階層を選択する必要があります。

#### 手順

1. 権限レベルをadvancedに設定します。  
**set -privilege advanced**
2. VSSシャドウ コピーのディレクトリ階層を目的のレベルに設定します。  
**vserver cifs options modify -vserver vserver\_name -shadowcopy-dir-depth integer**

#### 例

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. admin権限レベルに戻ります。  
**set -privilege admin**

## Hyper-VおよびSQL Server over SMB構成の管理

Hyper-V over SMBおよびSQL Server over SMBを管理するためのData ONTAPタスクがいくつかあります。

## 関連タスク

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#) (403ページ)

## 継続的な可用性を確保するための既存の共有の設定

既存の共有を変更して、継続的な可用性が確保された共有にすることができます。この共有は、Hyper-VおよびSQL Serverアプリケーション サーバがHyper-V仮想マシンおよび構成ファイルやSQL Serverデータベース ファイルに無停止でアクセスするために使用します。

### タスク概要

既存の共有に次のような特徴がある場合、SMBを介したアプリケーション サーバでその共有をノンストップ オペレーション用の継続的可用性を備えた共有として使用することはできません。

- その共有に**homedirectory**共有プロパティが設定されている場合
- 共有に有効なシンボリックリンクまたはワイドリンクが含まれている場合
- 共有のルート配下にジャンクション ボリュームが含まれている場合

共有の次の2つのパラメータについて、正しく設定されていることを確認する必要があります。

- **-offline-files**パラメータが**manual**(デフォルト)または**none**に設定されている必要があります。
- シンボリック リンクが無効になっている必要があります。

次の共有プロパティを設定する必要があります。

- **continuously-available**
- **oplocks**

次の共有プロパティは設定しないでください。現在の共有プロパティのリストに含まれている場合は、継続的な可用性が確保された共有から削除する必要があります。

- **changenotify**
- **attributecache**
- **branchcache**
- **access-based-enumeration**

### 手順

1. 現在の共有パラメータの設定と、設定済みの共有プロパティの現在のリストを表示します。  
`vserver cifs share show -vserver vserver_name -share-name share_name`
2. 必要に応じて、`vserver cifs share properties modify`コマンドを使用して共有パラメータを変更し、シンボリックリンクを無効にし、オフライン ファイルを**manual**に設定します。  
 -`symlink`パラメータの値を"**"**に設定すると、シンボリックリンクを無効にできます。
  - `symlink`パラメータの値を"**"**に設定すると、シンボリックリンクを無効にできます。
  - `offline-files`パラメータに**manual**を指定して正しい設定を行うことができます。
3. **continuously-available**共有プロパティを追加し、必要に応じて**oplocks**共有プロパティを追加します。

```
vserver cifs share properties add -vserver vserver_name -share-name
share_name -share-properties continuously-available[,oplock]
```

**oplocks共有プロパティ**がまだ設定されていない場合は、このプロパティを**continuously-available共有プロパティ**と一緒に追加する必要があります。

4. 継続的な可用性が確保された共有でサポートされていない共有プロパティを削除します。

```
vserver cifs share properties remove -vserver vserver_name -share-name
share_name -share-properties properties[,...]
```

共有プロパティをカンマで区切って指定して、1つ以上の共有プロパティを削除することができます。

5. -symlinkパラメータと-offline-filesパラメータが正しく設定されていることを確認します。

```
vserver cifs share show -vserver vserver_name -share-name share_name -
fields symlink-properties,offline-files
```

6. 設定済みの共有プロパティのリストが正しいことを確認します。

```
vserver cifs shares properties show -vserver vserver_name -share-name
share_name
```

### 例

次の例は、Storage Virtual Machine (SVM) vs1の「share1」という名前の既存の共有をSMBを介したアプリケーション サーバでのNDO用に設定する方法を示しています。

- -symlinkパラメータを""に設定して、共有でシンボリックリンクを無効にします。
- -offline-fileパラメータを変更して**manual**に設定します。
- **continuously-available共有プロパティ**を共有に追加します。
- **oplocks共有プロパティ**は共有プロパティのリストにすでに含まれているため、追加する必要はありません。
- **attributecache共有プロパティ**と**changenotify共有プロパティ**を共有から削除します。
- **browsable共有プロパティ**は、SMBを介したアプリケーション サーバでのNDO構成に使用される継続的な可用性が確保された共有では省略可能であり、共有プロパティの1つとして保持されます。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
```

```

      Vserver: vs1
      Share: share1
CIFS Server NetBIOS Name: vs1
      Path: /data
      Share Properties: oplocks
                       browsable
                       changenotify
                       attributecache
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
      Volume Name: data
      Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name share1 -
offline-file manual -symlink ""
```

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name share1 -fields
symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-----
vs1      share1      -                               manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

          Vserver: vs1
          Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

## Hyper-V over SMBバックアップでのVSSシャドウ コピーの有効化と無効化

VSS対応バックアップ アプリケーションを使用して、SMB共有に格納されたHyper-V仮想マシン ファイルをバックアップする場合は、VSSシャドウ コピーを有効にする必要があります。VSS対応バックアップ アプリケーションを使用しない場合は、VSSシャドウ コピーを無効にできます。デフォルトでは、VSSシャドウ コピーは有効になっています。

### タスク概要

VSSシャドウ コピーは随時有効または無効にできます。

### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

| VSSシャドウ コピーの設定 | 入力するコマンド                                                                                 |
|----------------|------------------------------------------------------------------------------------------|
| 有効             | <code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</code>  |
| 無効             | <code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</code> |

3. admin権限レベルに戻ります。

```
set -privilege admin
```

### 例

次のコマンドを実行すると、SVM vs1でVSSシャドウ コピーが有効になります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```



## Hyper-V over SMB構成をリバートする際の考慮事項

Hyper-V over SMBのノンストップ オペレーションをサポートしていないData ONTAPバージョンにリバートする場合は、リバートの準備ができるように一定の考慮事項について理解しておく必要があります。

リバートを行う前に、以下の点について検討し、必要に応じて措置を講じる必要があります。

- SMB 3.0および永続性ハンドルのロックをサポートしていないData ONTAPのバージョンにリバートする場合、Hyper-Vサーバでは切断された永続性ハンドルを再利用できないため、フェイルオーバーやギブバックなどの処理はシステム停止が必要となります。
- リバート時、仮想マシン ファイルへのHyper-Vサーバによるファイル アクセスがあってはなりません。
  - Hyper-Vアプリケーションを使用して、仮想マシン ファイルを別のストレージ デバイスまたはローカル ストレージに移行することができます。
  - すべての仮想マシンを停止し、データLIFへのHyper-Vサーバの接続を手動で終了することができます。

Data ONTAPでは、リバートの前にSMB 3.0が無効化されます。したがって、SMB接続を手動で終了していない場合は、リバート時にData ONTAPによって切断されます。

- Hyper-V over SMBソリューションは、このソリューションをサポートしていないData ONTAPのバージョンにリバートする場合には使用できません。  
接続されたLUNを使用して仮想マシン ファイルの格納およびアクセスを行うようにHyper-Vサーバを設定する必要があります。そのあと、SMB共有から、接続されたLUNに、仮想マシン ファイルをコピーする必要があります。
- リバートするには、リモートVSSで進行中のシャドウ コピー処理がないことを確認する必要があります。  
進行中の処理がある場合は、処理が終了するまで待機するか、リバートを開始する前に手動で中止する必要があります。シャドウ コピー処理を中止する必要がある場合は、テクニカル サポートにお問い合わせください。リバート時、Data ONTAPでは、既存のSnapshotコピーは削除されません。

## SQL Server over SMB構成をリバートする際の考慮事項

SQL Server over SMB共有のノンストップ オペレーションをサポートしていないData ONTAPバージョンにリバートする場合は、リバートの準備ができるように一定の考慮事項について理解しておく必要があります。

リバートを行う前に、以下の点について検討し、必要に応じて措置を講じる必要があります。

- SMB 3.0および永続性ハンドルのロックをサポートしていないData ONTAPのバージョンにリバートする場合、SQL Serverサーバでは切断された永続性ハンドルを再利用できないため、フェイルオーバーやギブバックなどの処理はシステム停止が必要となります。
- リバート時、データベース ファイルへのSQL Serverサーバによるファイル アクセスがあってはなりません。
  - SQL Serverアプリケーションを使用して、データベース ファイルを別のストレージ デバイスまたはローカル ストレージに移行することができます。
  - すべてのSQL Serverデータベースをシャットダウンし、データLIFへのSQL Serverの接続を手動で終了することができます。

Data ONTAPでは、リバートの前にSMB 3.0が無効化されます。したがって、SMB接続を手動で終了していない場合は、リバート時にData ONTAPによって切断されます。

- SQL Server SMB 3.0のノンストップ オペレーション用の継続的可用性を備えた共有は、このソリューションをサポートしていないData ONTAPのバージョンにリバートする場合には使用できません。  
接続されたLUNを使用してデータベース ファイルの格納およびアクセスを行うようにSQL Serverサーバを設定する必要があります。そのあと、SMB共有から、接続されたLUNに、データベース ファイルを移動する必要があります。

## 統計を使用したHyper-VおよびSQL Server over SMBアクティビティの監視

CIFSおよびSMBの各種の統計を表示して、Hyper-VおよびSQL Server over SMBのアクティビティを監視することができます。たとえば、SMBセッションの数、継続的な可用性が確保されたクライアントによるセッションの数、再接続要求の数などに関する情報を確認できます。

### 関連タスク

[SMBセッションの継続的可用性の確認](#) (425ページ)

## 使用可能な統計オブジェクトと統計カウンタの確認

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得し、パフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

### 手順

- 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- 次のいずれかを実行します。

| 確認する項目               | コマンド                                                             |
|----------------------|------------------------------------------------------------------|
| 使用可能なオブジェクト          | <code>statistics catalog object show</code>                      |
| 使用可能な特定のオブジェクトに関する情報 | <code>statistics catalog object show -object object_name</code>  |
| 使用可能なカウンタ            | <code>statistics catalog counter show -object object_name</code> |

使用可能なオブジェクトとカウンタの詳細については、マニュアル ページを参照してください。

- admin権限レベルに戻ります。

```
set -privilege admin
```

### 例

次のコマンドを実行すると、advanced権限レベルで表示したときの、クラスタ内のCIFSおよびSMBアクセスに関連する特定の統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed
to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
audit_ng          CM object for exporting audit_ng performance
counters

cluster1::*> statistics catalog object show -object cifs
cifs              The CIFS object reports activity of the
```

```

Common Internet File System protocol
subsystem. This is the Microsoft file-sharing
protocol that evolved from the Server Message
Block (SMB) application layer network
protocol to connect PCs to Network Attached
Storage devices (NAS). This object reports
activity for both SMB and SMB2 revisions of
the CIFS protocol. For information related
only to SMB, see the 'smb1' object. For
information related only to SMB2, see the
'smb2' object.

cluster1::*> statistics catalog nblade_cifs
nblade_cifs
object show -object nblade_cifs
The Common Internet File System (CIFS)
protocol is an implementation of the Server
Message Block (SMB) protocol. It is a
standard application layer file system
protocol used to share files with Windows(TM)
systems. This object tracks the data transfer
performance at the CIFS protocol layer, in
Ontap's Nblade network component. These
counters are relevant to the entire node,
rather than individual virtual servers.

cluster1::*> statistics catalog smb1
smb1
object show -object smb1
These counters report activity from the SMB
revision of the protocol. For information
specific to SMB2, see the 'smb2' object. To
see an overview across both revisions, see
the 'cifs' object.

cluster1::*> statistics catalog smb2
smb2
object show -object smb2
These counters report activity from the
SMB2/SMB3 revision of the protocol. For
information specific to SMB, see the 'smb1'
object. To see an overview across all
revisions, see the 'cifs' object.

cluster1::*> statistics catalog hashd
hashd
object show -object hashd
The hashd object provides counters to measure
the performance of the BranchCache hash
daemon.

cluster1::*> set -privilege admin

```

次のコマンドを実行すると、advanced権限レベルで表示したときの、cifsオブジェクトの一部のカウンタに関する情報が表示されます。

注: この例で表示されているのは、cifsオブジェクトに使用できるカウンタの一部であり、出力は省略されています。

```

cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed
to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
Counter          Description
-----
active_searches  Number of active searches over SMB and SMB2
auth_reject_too_many Authentication refused after too many
                        requests were made in rapid succession
avg_directory_depth Average number of directories crossed by SMB
                        and SMB2 path-based commands
avg_junction_depth Average number of junctions crossed by SMB
                        and SMB2 path-based commands
branchcache_hash_fetch_fail Total number of times a request to fetch hash
                        data failed. These are failures when
                        attempting to read existing hash data. It
                        does not include attempts to fetch hash data
                        that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch hash
                        data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
                        requesting hashes.
branchcache_missing_hash_bytes Total number of bytes of data that had to be
                        read by the client because the hash for that
                        content was not available on the server.
change_notifications_outstanding Number of active change notifications over
                        SMB and SMB2
cifs_latency      Average latency for CIFS operations
cifs_latency_base Total observed CIFS operations to be used as
                        a base counter for CIFS average latency

```

```

cifs_ops          calculation
cifs_read_ops     Total number of CIFS operations
cifs_write_ops    Total number of CIFS read operations
                  Total number of CIFS write operations
[...]

```

## 関連タスク

[統計情報の表示](#) (313ページ)

## 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: statistics catalog object show - Display the list of objects](#)

[clustered Data ONTAP 8.3.1 マニュアル ページ: statistics catalog counter show - Display the list of counters in an object](#)

## SMB統計の表示

パフォーマンスの監視と問題の診断用に、さまざまなSMB統計を表示することができます。

### 手順

1. `statistics start` コマンドとオプションの `statistics stop` コマンドを使用して、データ サンプルを収集します。

これらのコマンドの詳細については、[clustered Data ONTAP システム アドミニストレーション ガイド \(クラスタ管理\)](#) を参照してください。

2. 次のいずれかを実行します。

| 統計を表示する対象       | 入力するコマンド                                         |
|-----------------|--------------------------------------------------|
| SMBのすべてのバージョン   | <code>statistics show -object cifs</code>        |
| SMB 1.0         | <code>statistics show -object smb1</code>        |
| SMB 2.xとSMB 3.0 | <code>statistics show -object smb2</code>        |
| ノードのCIFSサブシステム  | <code>statistics show -object nblade_cifs</code> |

詳細については、[マニュアル ページ](#) を参照してください。

## 非破壊的な操作が可能であることの確認

Hyper-VまたはSQL Server over SMB構成に問題がなく、処理を無停止で実行できることを確認するには、ヘルスマニタの情報を表示し、SMB共有が永続的に共有されることを確認し、LIFの構成のステータスを確認します。

## ヘルス監視を使用してノンストップ オペレーションのステータスが正常かどうかを確認する方法

ヘルス監視を使用すると、クラスタ全体のシステム ヘルス ステータスに関する情報が得られます。ヘルスマニタはHyper-V over SMBおよびSQL Server over SMB構成を監視して、アプリケーション サーバのNondisruptive Operation (NDO; ノンストップ オペレーション) を実現します。ステータ

スが[degraded]になっている場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を表示できます。

ヘルスマニタはいくつかあります。Data ONTAPでは、システム全体のヘルスと個々のヘルスマニタのヘルスの両方が監視されます。ノード接続ヘルスマニタには、CIFS-NDOサブシステムが含まれています。モニタには一連のヘルスポリシーがあり、特定の物理的条件によりシステム停止が発生する可能性がある場合にアラートをトリガーするポリシーと、システム停止が発生している場合にアラートが生成し、対処方法に関する情報を提供するポリシーがあります。SMBを介したNDO構成では、アラートは次の2通りの状態で生成されます。

| アラートID                    | 重大度  | 条件                                                                                                                                   |
|---------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------|
| HaNotReadyCifsNdo_Alert   | メジャー | ノード上のアグリゲート内のボリュームでホストされている1つ以上のファイルが、継続的可用性を備えたSMB共有を介して開かれており、障害が発生した場合でも継続性が保証されるはずだが、パートナーとのHA関係が設定されていないか正常でない。                 |
| NoStandbyLifCifsNdo_Alert | マイナー | Storage Virtual Machine (SVM) はノードからSMBを介してアクティブにデータを提供しており、SMBファイルは継続的可用性を備えた共有を介して継続的に開かれているが、そのパートナーノードがSVMのアクティブなデータLIFを公開していない。 |

## システムヘルスの監視を使用したノンストップオペレーションのステータスの表示

system healthコマンドを使用して、クラスタのシステムヘルス全体およびCIFS-NDOサブシステムのヘルスに関する情報の表示、アラートへの対応、以後のアラートの設定、ヘルスマニタの設定に関する情報の表示を行うことができます。

### タスク概要

システムヘルスの監視の使用の詳細については、『*clustered Data ONTAP システム アドミニストレーションガイド(クラスタ管理)*』を参照してください。

### 手順

- 適切な操作を実行して、ヘルスステータスを監視します。

| 表示する項目                                | 入力するコマンド                                                                |
|---------------------------------------|-------------------------------------------------------------------------|
| 個々のヘルスマニタのステータス全体が反映された、システムのヘルスステータス | <code>system health status show</code>                                  |
| CIFS-NDOサブシステムのヘルスステータスに関する情報         | <code>system health subsystem show -subsystem CIFS-NDO -instance</code> |

- 適切な操作を実行して、CIFS-NDOアラートの監視がどのように設定されているかに関する情報を表示します。

| 表示する情報                                                | 入力するコマンド                                                   |
|-------------------------------------------------------|------------------------------------------------------------|
| 監視対象のノード、初期化状態、ステータスなど、CIFS-NDOサブシステムのヘルスマニタの設定とステータス | <code>system health config show -subsystem CIFS-NDO</code> |

| 表示する情報                                   | 入力するコマンド                                                          |
|------------------------------------------|-------------------------------------------------------------------|
| ヘルスマニタで生成される可能性があるCIFS-NDOアラート           | <b>system health alert definition show -subsystem CIFS-NDO</b>    |
| アラートが発行されるタイミングを決定する、CIFS-NDOヘルスマニタのポリシー | <b>system health policy definition show -monitor node-connect</b> |

注: 詳細な情報を表示するには、-instanceパラメータを使用します。

### 例

次の出力は、クラスタおよびCIFS-NDOサブシステムのヘルス ステータス全体に関する情報を示しています。

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

Subsystem: CIFS-NDO
Health: ok
Initialization State: initialized
Number of Outstanding Alerts: 0
Number of Suppressed Alerts: 0
```

次の出力は、CIFS-NDOサブシステムのヘルスマニタの設定とステータスに関する詳細な情報を示しています。

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf, HaNodePair,
HaICMailbox, CifsNdoNode, CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0, 1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf, HaNodePair,
HaICMailbox, CifsNdoNode, CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0, 1.0
```

## SMB共有の継続的な可用性の設定の確認

ノンストップ オペレーションをサポートするには、Hyper-VおよびSQL Server SMB共有が継続的な可用性を確保するように設定されている必要があります。また、それ以外にも、いくつかの共有の設定について確認が必要になります。計画的または計画外の停止が発生する状況でアプリケー

ション サーバのノンストップ オペレーションをシームレスに実行できるように、共有が適切に設定されていることを確認してください。

### タスク概要

共有の次の2つのパラメータについて、正しく設定されていることを確認する必要があります。

- `-offline-files`パラメータが`manual`(デフォルト)または`none`に設定されている必要があります。
- シンボリック リnkが無効になっている必要があります。

ノンストップ オペレーションが適切に実行されるようにするには、次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。

- `homedirectory`
- `changenotify`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

### 手順

1. オフライン ファイルが`manual`または`disabled`に設定されていること、およびシンボリック リnkが無効になっていることを確認します。

```
vserver cifs shares show -vserver vserver_name
```

2. SMB共有が継続的な可用性を確保するように設定されていることを確認します。

```
vserver cifs shares properties show -vserver vserver_name
```

### 例

次の例では、Storage Virtual Machine (SVM、旧Vserver) vs1で「share1」という名前の共有の共有設定を表示します。オフライン ファイルは`manual`に設定されており、シンボリック リnkは無効になっています (*[SymLink Properties]*フィールドの出力がハイフンになっています)。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
Vserver: vs1
Share: share1
CIFS Server NetBIOS Name: VS1
Path: /data/share1
Share Properties: oplocks
continuously-available
SymLink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例では、SVM vs1の「share1」という名前の共有の共有プロパティを表示します。

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1     oplocks
              continuously-available
```

## LIFステータスの確認

Hyper-VおよびSQL Server over SMB構成のStorage Virtual Machine(SVM)がクラスタ内の各ノードにLIFを配置するように設定しても、日々の業務を行っているうちに、一部のLIFが他のノードのポートに移動してしまうことがあります。LIFのステータスを確認して、必要な措置を講じる必要があります。

### タスク概要

シームレスなノンストップ オペレーションの運用支援を提供するには、クラスタ内の各ノードのSVMに少なくとも1つのLIFを配置し、すべてのLIFをホーム ポートに関連付ける必要があります。設定されているLIFの中に現在ホーム ポートに関連付けられていないものがある場合は、ポートの問題を修正してから、対応するホーム ポートにLIFをリポートする必要があります。

### 手順

1. 設定されているSVMのLIFに関する情報を表示します。

```
network interface show -vsriver vsriver_name
```

#### 例

この例では、「lif1」がホーム ポートに配置されていません。

```
network interface show -vsriver vs1
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| vs1     |                   |                   |                      |              |              |         |
|         | lif1              | up/up             | 10.0.0.128/24        | node2        | e0d          | false   |
|         | lif2              | up/up             | 10.0.0.129/24        | node2        | e0d          | true    |

2. 対応するホーム ポートに関連付けられていないLIFがある場合は、次の手順を実行します。

- a. それぞれのLIFについて、LIFのホーム ポートを確認します。

```
network interface show -vsriver vsriver_name -lif lif_name -fields
home-node,home-port
```

#### 例

```
network interface show -vsriver vs1 -lif lif1 -fields home-node,home-
port
```

| vsriver | lif  | home-node | home-port |
|---------|------|-----------|-----------|
| vs1     | lif1 | node1     | e0d       |

- b. それぞれのLIFについて、LIFのホーム ポートがup状態になっているかどうかを確認します。

```
network port show -node node_name -port port -fields port,link
```



**例**

```
network port show -node node1 -port e0d -fields port,link
```

| node  | port | link |
|-------|------|------|
| node1 | e0d  | up   |

この例では、「lif1」をホーム ポートのnode1:e0dに戻す必要があります。

3. LIFを関連付けるホーム ポートのネットワーク インターフェイスがup状態になっていない場合は、問題を解決してup状態にします。
4. 必要に応じて、ホーム ポートにLIFをリバートします。

```
network interface revert -vserver vs1 -lif lif1
```

**例**

```
network interface revert -vserver vs1 -lif lif1
```

5. クラスタ内の各ノードにアクティブなSVMのLIFがあることを確認します。

```
network interface show -vserver vs1
```

**例**

```
network interface show -vserver vs1
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| vs1     | lif1              | up/up             | 10.0.0.128/24        | node1        | e0d          | true    |
|         | lif2              | up/up             | 10.0.0.129/24        | node2        | e0d          | true    |

**関連タスク**

[Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するData ONTAP構成の作成](#)(403ページ)

**SMBセッションの継続的可用性の確認**

SMBセッションと開いているSMBファイルに関する情報を表示して、その継続的可用性を確認できます。

**関連タスク**

[統計を使用したHyper-VおよびSQL Server over SMBアクティビティの監視](#)(418ページ)

**SMBセッション情報の表示**

SMB接続、SMBセッションID、セッションを使用しているワークステーションのIPアドレスなど、確立されたSMBセッションに関する情報を表示できます。セッションのSMBプロトコル バージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップ オペレーションがサポートされているかどうか確認するのに役立ちます。

**タスク概要**

Storage Virtual Machine (SVM) 上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションの `-fields` パラメータを使用して、選択したフィールドの出力を表示できます。  
`-fields ?`と入力すると、使用できるフィールドを確認できます。
- `-instance` パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます。
- `-fields` パラメータまたは `-instance` パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

## 手順

1. 次のいずれかを実行します。

| 確立されたセッションのSMB<br>セッション情報を表示する対<br>象 | 入力するコマンド                                                                                                                                                                                                                                                                                  |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SVM上のすべてのセッション<br>(要約形式)             | <code>vserver cifs session show -vserver <i>vserver_name</i></code>                                                                                                                                                                                                                       |
| 指定した接続IDのセッション                       | <code>vserver cifs session show -vserver <i>vserver_name</i> -<br/>connection-id <i>integer</i></code>                                                                                                                                                                                    |
| 指定したワークステーション<br>のIPアドレスからのセッション     | <code>vserver cifs session show -vserver <i>vserver_name</i> -<br/>address <i>workstation_IP_address</i></code>                                                                                                                                                                           |
| 指定したLIF IPアドレスのセ<br>ッション             | <code>vserver cifs session show -vserver <i>vserver_name</i> -<br/>lif-address <i>LIF_IP_address</i></code>                                                                                                                                                                               |
| 指定したノード上のファイル                        | <code>vserver cifs session show -vserver <i>vserver_name</i> -<br/>node {<i>node_name</i> local}</code>                                                                                                                                                                                   |
| 指定したWindowsユーザか<br>らのセッション           | <code>vserver cifs session show -vserver <i>vserver_name</i> -<br/>windows-user <i>user_name</i></code><br><br><i>user_name</i> の形式は[domain]\userです。                                                                                                                                      |
| 指定した認証メカニズムを使<br>用しているセッション          | <code>vserver cifs session show -vserver <i>vserver_name</i> -<br/>auth-mechanism <i>authentication_mechanism</i></code><br><br>-auth-mechanism には、次のいずれかの値を指定できます。 <ul style="list-style-type: none"> <li>• NTLMv1</li> <li>• NTLMv2</li> <li>• Kerberos</li> <li>• Anonymous</li> </ul> |

| 確立されたセッションのSMBセッション情報を表示する対象    | 入力するコマンド                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 指定したプロトコルバージョンを使用しているセッション      | <pre><b>vserver cifs session show -vserver <i>vserver_name</i> -protocol-version <i>protocol_version</i></b></pre> <p>-protocol-versionには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li><b>SMB1</b></li> <li><b>SMB2</b></li> <li><b>SMB2_1</b></li> <li><b>SMB3</b></li> </ul> <p><b>注:</b> 継続的可用性を備えた保護は、SMB 3.0セッションでのみ使用できます。該当するすべてのセッションの継続的可用性を備えた保護のステータスを表示するには、このパラメータの値を<b>SMB3</b>に設定します。</p>                                                                                                                  |
| 指定したレベルの継続的可用性を備えた保護を使用しているファイル | <pre><b>vserver cifs session show -vserver <i>vserver_name</i> -continuously-available <i>continuously_available_protection_level</i></b></pre> <p>-continuously-availableには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li><b>No</b></li> <li><b>Yes</b></li> <li><b>Partial</b></li> </ul> <p><b>注:</b> 継続的可用性のステータスが<b>Partial</b>の場合、継続的可用性を使用して開かれたファイルが1つ以上セッションにあるが、継続的可用性を備えた保護を使用せずに開かれたファイルもセッションにあることを意味します。vserver cifs sessions file show コマンドを使用すると、確立されたセッションのファイルのうち、継続的可用性を備えた保護を使用せずに開かれたファイルを確認できます。</p> |
| 指定したSMB署名セッションステータスのセッション       | <pre><b>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed {true false}</b></pre>                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## 例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID         ID         Workstation   Windows User   Open   Idle
-----
3151272279 1         10.1.1.1     DOMAIN\joe     2      23s
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。この接続はドメイン コンピュータ アカウントを使用して行われています。

```
cluster1::> vserver cifs session show -instance -continuously-available Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

次のコマンドを実行すると、SVM vs1上のSMB 3.0を使用しているセッションに関するセッション情報が表示されます。ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するためには、Kerberos認証を使用して接続を行う必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151272607
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

## 開いているSMBファイルに関する情報の表示

SMB接続、SMBセッションID、ホスティング ボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報も表示できます。この情報は、開いているファイルがノンストップ オペレーションをサポートする状態であるかどうか確認するのに役立ちます。

### タスク概要

確立されたSMBセッションで開いているファイルに関する情報を表示できます。これは、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと、継続的可用性を備えた保護を使用せずに開いているファイルがある場合(vserver cifs session showコマンド出力の -continuously-available フィールドの値は**Partial**になります)、このコマンドによって、継続的可用性に対応していないファイルを特定できます。

オプションのパラメータを何も指定せずに `vserver cifs session file show` コマンドを実行することで、Storage Virtual Machine (SVM) 上の確立された SMB セッションのすべての開いているファイルに関する情報を要約形式で表示できます。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションの `-fields` パラメータを使用して、選択したフィールドの出力を表示できます。  
このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。
- `-instance` パラメータを使用して、開いている SMB ファイルに関する詳細情報を表示できます。  
このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。

## 手順

1. 次のいずれかを実行します。

| 表示する開いている SMB ファイル      | 入力するコマンド                                                                                                          |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|
| SVM 上のファイル (要約形式)       | <code>vserver cifs session file show -vserver <i>vserver_name</i></code>                                          |
| 指定したノード上のファイル           | <code>vserver cifs session file show -vserver <i>vserver_name</i> -node {<i>node_name</i> local}</code>           |
| 指定したファイル ID のファイル       | <code>vserver cifs session file show -vserver <i>vserver_name</i> -file-id <i>integer</i></code>                  |
| 指定した SMB 接続 ID のファイル    | <code>vserver cifs session file show -vserver <i>vserver_name</i> -connection-id <i>integer</i></code>            |
| 指定した SMB セッション ID のファイル | <code>vserver cifs session file show -vserver <i>vserver_name</i> -session-id <i>integer</i></code>               |
| 指定したホスティング アグリゲートのファイル  | <code>vserver cifs session file show -vserver <i>vserver_name</i> -hosting-aggregate <i>aggregate_name</i></code> |
| 指定したボリュームのファイル          | <code>vserver cifs session file show -vserver <i>vserver_name</i> -hosting-volume <i>volume_name</i></code>       |
| 指定した SMB 共有のファイル        | <code>vserver cifs session file show -vserver <i>vserver_name</i> -share <i>share_name</i></code>                 |
| 指定した SMB パスのファイル        | <code>vserver cifs session file show -vserver <i>vserver_name</i> -path <i>path</i></code>                        |

| 表示する開いているSMBファイル                | 入力するコマンド                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 指定したレベルの継続的可用性を備えた保護を使用しているファイル | <pre>vserver cifs session file show -vserver vserver_name -continuously-available continuously_available_status</pre> <p>-continuously-availableには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <p><b>注:</b> 継続的可用性のステータスがNoの場合、それらの開いているファイルが、テイクオーバーやギブバックからのシステム停止不要のリカバリに対応していないことを意味します。また、可用性の高い関係のパートナー間における一般的なアグリゲートの再配置からリカバリすることもできません。</p> |
| 指定した再接続の状態のファイル                 | <pre>vserver cifs session file show -vserver vserver_name -reconnected reconnected_state</pre> <p>-reconnectedには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <p><b>注:</b> 再接続の状態がNoの場合、その開いているファイルは、切断の発生後に再接続されていません。つまり、そのファイルは一度も切断されていないか、切断されてから再接続できなかったことを意味します。再接続の状態がYesの場合、その開いているファイルは、切断の発生後に正常に再接続されたことを意味します。</p>                       |

ほかにも、出力結果を詳細に指定するためのオプションのパラメータがあります。詳細については、マニュアル ページを参照してください。

#### 例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node: node1
Vserver: vs1
Connection: 3151274158
Session: 1
File ID      Open Mode  Hosting Volume  Share  Continuously
-----
41      Regular      r      data      data      Yes
Path: \mytest.rtf
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82 -instance
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
```

```
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

## FlexVolを備えたSVMでのNASイベントの監査

NASイベントの監査は、FlexVolを備えたStorage Virtual Machine (SVM) で特定のCIFSおよびNFS イベントを追跡してログに記録できるセキュリティ対策です。これは、潜在的なセキュリティの問題を追跡するのに役立つほか、セキュリティ違反が発生した場合の証拠にもなります。Active Directoryの集約型アクセス ポリシーのステージングおよび監査によってこれらを実施した場合の結果を確認することもできます。

### CIFSイベント

次のイベントを監査できます。

- **SMBファイルおよびフォルダ アクセス イベント**  
監査が有効になっているSVMに属するFlexVol上に格納されているオブジェクトに対するSMBによるファイルおよびフォルダ アクセス イベントを監査できます。
- **CIFSログオンおよびログオフ イベント**  
FlexVolを備えたSVM上にあるCIFSサーバでのCIFSログオンおよびログオフ イベントを監査できます。
- **集約型アクセス ポリシーのステージング イベント**  
提案された集約型アクセス ポリシーによって適用された権限を使用したCIFSサーバ上のオブジェクトへの有効なアクセスを監査できます。集約型アクセス ポリシーのステージングによって監査を行うと、集約型アクセス ポリシーを導入する前に、その影響を確認できます。  
集約型アクセス ポリシーのステージングによる監査は、Active DirectoryのGPOを使用してセットアップされます。ただし、SVMの監査設定は、集約型アクセス ポリシー ステージング イベントを監査するように設定されている必要があります。  
監査設定では、CIFSサーバでDynamic Access Control (DAC; ダイナミック アクセス制御) を有効にしなくても、集約型アクセス ポリシーのステージングを有効にできますが、集約型アクセス ポリシーのステージング イベントはダイナミック制御が有効になっている場合にしか生成されません。ダイナミック アクセス制御は、CIFSサーバ オプションを使用して有効にします。デフォルトでは有効になっていません。

### NFSイベント

FlexVolを備えたSVM上に格納されているオブジェクトに対するファイルおよびディレクトリの NFSv4アクセス イベントを監査できます。

### 関連コンセプト

[ファイル権限を使用したファイル アクセスの保護](#) (193ページ)

[監査できるSMBイベント](#) (438ページ)

[DAC \(ダイナミック アクセス制御\) を使用したファイル アクセスの保護](#) (200ページ)

## 監査の仕組み

監査の設定を計画して設定する前に、監査の仕組みについて理解しておく必要があります。

### 監査の基本概念

Data ONTAPの監査について理解するために、監査の基本概念を確認しておく必要があります。

#### ステージング ファイル



統合および変換の前に監査レコードが格納される、個々のノード上の中間バイナリファイル。ステージングファイルはステージングボリュームに格納されます。

### ステージング ボリューム

ステージングファイルを格納するためにData ONTAPによって作成される専用ボリューム。各アグリゲートに1つのステージングボリュームがあります。ステージングボリュームは、監査が有効なすべてのStorage Virtual Machine (SVM) で共有され、そのアグリゲート内のデータボリュームを対象としたデータアクセスの監査レコードを格納します。各SVMの監査レコードは、ステージングボリューム内の個別のディレクトリに格納されます。

クラスタ管理者はステージングボリュームに関する情報を表示できますが、それ以外のほとんどのボリューム処理は実行できません。clustered Data ONTAPのみがステージングボリュームを作成できます。clustered Data ONTAPはステージングボリュームへの名前の割り当てを自動的に行います。すべてのステージングボリューム名はMDV\_aud\_で始まり、そのあとにステージングボリュームを格納するアグリゲートのUUIDが続きます (例: MDV\_aud\_1d0131843d4811e296fc123478563412)。

### システム ボリューム

ファイル サービスや監査ログのメタデータなど、特別なメタデータを格納するFlexVolです。システムボリュームの所有者は管理SVMであり、システムボリュームはクラスタ全体に表示されます。ステージングボリュームはシステムボリュームの一種です。

### 統合タスク

監査が有効になっている場合に作成されるタスクです。各SVMで長時間にわたって実行され、SVMのメンバー ノード全体のステージングファイルから監査レコードを取得します。監査レコードは時間順にマージされたのち、監査設定で指定されたユーザが読解可能なイベント ログ形式 (EVTXまたはXML形式) に変換されます。変換されたイベントログは、SVMの監査設定で指定された監査イベント ログ ディレクトリに格納されます。

## Data ONTAP監査プロセスの仕組み

Data ONTAPの監査プロセスは、Microsoftの監査プロセスとは異なります。監査を設定する前に、Data ONTAPの監査プロセスの仕組みについて理解しておく必要があります。

監査レコードは、最初に個々のノードのバイナリステージングファイルに格納されます。あるSVMで監査が有効になると、すべてのメンバー ノードでそのSVMのステージングファイルが保持されます。ステージングファイルは定期的に統合され、ユーザが読解可能なイベント ログに変換されて、SVMの監査イベント ログ ディレクトリに格納されます。

### あるSVMで監査が有効になっている場合の処理

監査は、FlexVolを備えたSVMでのみ有効にできます。ストレージ管理者がSVMで監査を有効にすると、監査サブシステムによってステージングボリュームが存在するかどうかを確認されます。ステージングボリュームは、SVMに所有されているデータボリュームを含むアグリゲートごとに必要です。存在しない場合は、監査サブシステムによって必要なステージングボリュームが作成されます。

また、監査が有効になる前に、前提条件となるその他のタスクが実行されます。

- 監査サブシステムによって、ログ ディレクトリのパスが使用可能でシンボリックリンクが含まれていないことが検証されます。

ログ ディレクトリがすでに存在している必要があります。監査サブシステムは、デフォルトのログファイルの場所を割り当てません。監査設定で指定されているログ ディレクトリのパスが有効なパスでない場合は、「

The specified path "/<path>" does not exist in the namespace belonging to Vserver "<Vserver\_name>"

」というエラーが発生し、監査設定の作成に失敗します。

ディレクトリは存在するがシンボリックリンクが含まれている場合も、設定の作成に失敗します。

- 監査によって統合タスクがスケジュールされます。

このタスクがスケジュールされたあと、監査が有効になります。SVMの監査設定とログ ファイルは、リブート後も、NFSサーバまたはCIFSサーバが停止したり再起動したりした場合も維持されます。

### イベント ログの統合

ログの統合は、監査が無効になるまで定期的に実行されるスケジュール済みタスクです。監査が無効になると、統合タスクによって残っているすべてのログが統合されます。

### 監査の保証

デフォルトでは、監査が保証されています。Data ONTAPでは、あるノードが利用できない場合でも、監査可能なファイル アクセス イベント(設定された監査ポリシーのACLで指定されている)がすべて記録されることが保証されます。要求されたファイル処理は、その操作の監査レコードが永続的ストレージのステージング ボリュームに保存されるまで完了できません。監査レコードをスペース不足またはその他の問題が原因でディスクのステージング ファイルにコミットできない場合は、クライアント処理が拒否されています。

### ノードが利用できない場合の統合処理

監査が有効になっているSVMに属するボリュームを含むノードが利用できない場合、監査の統合タスクの動作は、そのノードのSFOパートナー(2ノード クラスタの場合はHAパートナー)が利用可能かどうかによって異なります。

- SFOパートナー経由でステージング ボリュームにアクセスできる場合は、ノードから最後にレポートされたステージング ボリュームがスキャンされ、通常どおりに統合が実行されます。
- SFOパートナーが利用できない場合は、部分的なログ ファイルが作成されます。  
あるノードにアクセスできない場合は、統合タスクによって、そのSVMの利用可能な他のノードの監査レコードが統合されます。部分的に統合されたログであることがわかるように、統合されたファイルの名前にはサフィックス `.partial` が追加されます。
- 利用できないノードが利用可能になった時点で、そのノードの監査レコードが、その時点における他のノードの監査レコードと統合されます。
- 監査レコードはすべて維持されます。

### イベント ログのローテーション

監査イベント ログ ファイルは、設定されたログ サイズしきい値に達した場合に、または設定されたスケジュールに従ってローテーションされます。イベント ログ ファイルがローテーションされると、スケジュールされた統合タスクによって、まず、アクティブな変換済みファイルの名前がタイムスタンプのあるアーカイブ ファイルに変更され、次に新しいアクティブな変換済みイベント ログ ファイルが作成されます。

### SVMで監査が無効になっている場合の処理

SVMで監査が無効になると、統合タスクが最後にもう一度トリガーされます。未処理の記録済みの監査レコードがすべて、ユーザが読解可能な形式でログに記録されます。SVMで監査が無効になっても、イベント ログ ディレクトリに格納されている既存のイベント ログは削除されず、参照が可能です。

そのSVMの既存のステージング ファイルがすべて統合されたら、スケジュールから統合タスクが削除されます。SVMの監査設定を無効にしても、監査設定は削除されません。ストレージ管理者は、監査をいつでも再度有効にできます。

監査が有効になると監査の統合ジョブが作成されます。このジョブは統合タスクを監視して、タスクがエラーによって終了した場合には統合タスクを再作成します。これまでは、`job delete`のようなジョブ マネージャ コマンドを使用して監査の統合ジョブを削除することができましたが、ユーザは監査の統合ジョブを削除できなくなりました。

#### 関連コンセプト

- [監査の基本概念](#) (432ページ)
- [サポートされる監査イベント ログの形式](#) (436ページ)
- [監査できるSMBイベント](#) (438ページ)

#### 関連タスク

- [SVMでのファイルとディレクトリの監査設定の作成](#) (448ページ)

#### 関連参照情報

- [監査できるNFSファイルおよびディレクトリのアクセス イベント](#) (442ページ)

## 監査を有効にする際のアグリゲート スペースに関する考慮事項

監査設定が作成されていてクラスタ内の少なくとも1つのStorage Virtual Machine (SVM) で監査が有効になっている場合、監査サブシステムは、既存のすべてのアグリゲートと、作成されるすべての新しいアグリゲートにステージング ボリュームを作成します。クラスタ上で監査を有効にする際は、アグリゲート スペースに関する考慮事項に注意する必要があります。

アグリゲートに十分な空き容量がない場合、ステージング ボリュームの作成に失敗することがあります。監査を構成しても、既存のアグリゲートにステージング ボリュームの格納に必要な空き容量がない場合に、このエラーが起きることがあります。

あるSVMで監査を有効にする前に、既存のアグリゲート上にステージング ボリューム用の十分な領域があることを確認する必要があります。

#### 関連コンセプト

- [監査およびステージング用のボリュームのスペースに関する問題のトラブルシューティング](#) (463ページ)

## 監査の要件と考慮事項

Storage Virtual Machine (SVM) で監査を設定して有効にする前に、一定の要件と考慮事項について理解しておく必要があります。

- 監査を有効にしたSVMは、クラスタで最大50個までサポートされます。
- 監査はCIFSまたはNFSのライセンスとは関係ありません。  
CIFSとNFSのライセンスがクラスタにインストールされていない場合でも、監査を設定して有効にすることができます。
- NFS監査では、セキュリティACE (タイプU) をサポートしています。
- NFS監査では、モード ビットと監査ACEの間のマッピングはありません。  
ACLをモード ビットに変換する場合、監査ACEはスキップされます。モード ビットをACLに変換する場合、監査ACEは生成されません。
- 監査設定で指定するディレクトリが存在している必要があります。  
存在しない場合、監査設定を作成するコマンドは失敗します。
- 監査設定で指定するディレクトリは、次の要件を満たしている必要があります。

- ディレクトリにシンボリックリンクを含むことはできません。  
監査設定で指定するディレクトリにシンボリックリンクが含まれている場合、監査設定を作成するコマンドは失敗します。
- 絶対パスを使用してディレクトリを指定する必要があります。  
相対パス(例: /vs1/./)は指定しないでください。
- 監査は、ステージング ボリューム内に利用可能なスペースがあるかどうか依存します。  
監査対象のボリュームを含むアグリゲートのステージング ボリュームに十分なスペースを確保できるよう注意する必要があります。
- 監査は、変換されたイベント ログの格納先ディレクトリを含むボリューム内に利用可能なスペースがあるかどうか依存します。  
イベント ログの格納に使用するボリュームに十分なスペースを確保できるよう注意する必要があります。監査ディレクトリ内に保持するイベント ログの数は、監査設定の作成時に `-rotate-limit` パラメータを使用して指定できます。これは、ボリューム内にイベント ログで使用可能な領域を十分に確保するのに役立ちます。
- 監査設定では、CIFSサーバでDynamic Access Control (DAC; ダイナミック アクセス制御)を有効にしなくても、集約型アクセス ポリシーのステージングを有効にできますが、集約型アクセス ポリシーのステージング イベントを生成するには、ダイナミック アクセス制御を有効にしておく必要があります。  
ダイナミック アクセス制御は、デフォルトでは有効になっていません。

#### 関連コンセプト

[監査設定の計画](#)(443ページ)

## サポートされる監査イベント ログの形式

変換された監査イベント ログでサポートされるファイル形式は、EVTXおよび XMLファイル形式です。

監査設定を作成する際には、ファイル形式の種類を指定できます。デフォルトでは、Data ONTAPによってバイナリ ログがEVTXファイル形式に変換されます。

#### 関連コンセプト

[監査イベント ログの表示](#)(436ページ)

[イベントビューアを使用したアクティブな監査ログの表示方法](#)(437ページ)

## 監査イベント ログの表示

監査イベント ログを使用して、ファイル セキュリティが適切であるかどうか、ファイルやフォルダへの不適切なアクセス試行がなかったかどうかを確認できます。EVTXまたはXMLファイル形式で保存された監査イベント ログを表示および処理できます。

- EVTXファイル形式  
EVTXに変換された監査イベント ログは、保存済みファイルとしてMicrosoftイベントビューアを使用して開くことができます。  
イベントビューアでイベント ログを表示する際に使用できる2つのオプションがあります。
  - 全般表示  
イベントレコードに対し、すべてのイベントに共通する情報が表示されます。このバージョンのData ONTAPでは、イベントレコードに関するイベント固有のデータは表示されません。  
詳細表示を使用すると、イベント固有のデータを表示できます。

- 詳細表示  
フレンドリ表示とXML表示が利用できます。フレンドリ表示とXML表示には、すべてのイベントに共通の情報とイベントレコードのイベント固有のデータの両方が表示されます。
- XMLファイル形式  
XML監査イベント ログは、XMLファイル形式をサポートするサードパーティのアプリケーションで表示および処理できます。XML閲覧ツールを使用して監査ログを表示するには、XMLスキーマとXMLフィールドの定義に関する情報が必要です。XMLスキーマおよびXMLの定義に関するドキュメントを入手する方法については、テクニカル サポートまたはアカウント チームにお問い合わせください。

**関連コンセプト**

- [Data ONTAP監査プロセスの仕組み](#)(433ページ)
- [イベントビューアを使用したアクティブな監査ログの表示方法](#)(437ページ)
- [シンボリックリンクおよびハード リンクを監査する際の考慮事項](#)(440ページ)
- [NTFS代替データストリームを監査する際の考慮事項](#)(441ページ)

**関連タスク**

- [監査対象オブジェクトへの完全パスの決定](#)(440ページ)
- [監査イベント ログの手動ローテーション](#)(459ページ)

**イベントビューアを使用したアクティブな監査ログの表示方法**

クラスタで監査の統合プロセスを実行している場合、統合プロセスにより、監査を有効にした Storage Virtual Machine (SVM) のアクティブな監査ログ ファイルに新しいレコードが追加されます。このアクティブな監査ログは、SMB共有でアクセスしてMicrosoftイベントビューアで開くことができます。

イベントビューアには、既存の監査レコードの表示だけでなく、コンソール ウィンドウの内容を更新できる更新オプションもあります。アクティブな監査ログへのアクセスに使用される共有でoplockが有効になっているかどうかに応じて、新たに追加されたレコードをイベントビューアで表示できるかどうかが決まります。

| 共有でのoplockの設定 | 動作                                                                                     |
|---------------|----------------------------------------------------------------------------------------|
| 有効            | その時点までに書き込まれたイベントを含むログがイベントビューアに表示されます。更新操作を実行してもログは更新されず、統合プロセスで追加された新しいイベントは表示されません。 |
| 無効            | その時点までに書き込まれたイベントを含むログがイベントビューアに表示されます。更新操作を実行するとログが更新され、統合プロセスで追加された新しいイベントが表示されます。   |

注: この情報が該当するのはEVTXイベント ログのみです。XMLイベント ログは、SMB経由でブラウザで、または任意のXMLエディタまたはビューアを使用してNFS経由で表示することができます。

## 監査できるSMBイベント

Data ONTAPは、ファイルおよびフォルダのアクセス イベント、ログオンおよびログオフ イベント、集約型アクセス ポリシーのステー징 イベントなどのSMBイベントを監査できます。どのようなアクセス イベントを監査できるか理解しておく、イベント ログの結果を解釈するときに役立ちます。

監査できるSMBイベントは次のとおりです。

| イベントID<br>(EVT /<br>EVTX) | イベント                    | 説明                                                                                                       | カテゴリ        |
|---------------------------|-------------------------|----------------------------------------------------------------------------------------------------------|-------------|
| 540 / 4624                | アカウントがログオンに成功           | ログオン / ログオフ: ネットワーク(CIFS) ログオン。                                                                          | ログオンおよびログオフ |
| 529 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: ユーザ名が不明またはパスワードが無効です。                                                                       | ログオンおよびログオフ |
| 530 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: アカウント ログオンの時間制限です。                                                                          | ログオンおよびログオフ |
| 531 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: アカウントは現在無効に設定されています。                                                                        | ログオンおよびログオフ |
| 532 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: ユーザ アカウントの有効期限が切れています。                                                                      | ログオンおよびログオフ |
| 533 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: ユーザはこのコンピュータにログオンできません。                                                                     | ログオンおよびログオフ |
| 534 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: ユーザはログオンを認められていません。                                                                         | ログオンおよびログオフ |
| 535 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: ユーザのパスワードが期限切れです。                                                                           | ログオンおよびログオフ |
| 537 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: 上記の理由以外でログオンが失敗しました。                                                                        | ログオンおよびログオフ |
| 539 / 4625                | アカウントがログオンに失敗           | ログオン / ログオフ: アカウントのロックアウト。                                                                               | ログオンおよびログオフ |
| 538 / 4634                | アカウントがログオフ              | ログオン / ログオフ: ローカルまたはネットワーク ユーザのログオフ。                                                                     | ログオンおよびログオフ |
| 560 / 4656                | オブジェクトのオープン / オブジェクトの作成 | オブジェクトへのアクセス: オブジェクト(ファイルまたはフォルダ)が開かれた。                                                                  | ファイル アクセス   |
| 563 / 4659                | 削除するためのオブジェクトのオープン      | オブジェクトへのアクセス: 削除するためにオブジェクト(ファイルまたはディレクトリ)へのハンドルが要求されました。                                                | ファイル アクセス   |
| 564 / 4660                | オブジェクトの削除               | オブジェクトへのアクセス: オブジェクト(ファイルまたはフォルダ)の削除。Data ONTAPはWindowsクライアントがオブジェクト(ファイルまたはディレクトリ)の削除を試みるとこのイベントを生成します。 | ファイル アクセス   |

| イベントID<br>(EVT /<br>EVTX)      | イベント                                                    | 説明                                                                                                                                                                                                                                                   | カテゴリ      |
|--------------------------------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 567 / 4663                     | オブジェクトの読み取り / オブジェクトの書き込み / オブジェクトの属性の取得 / オブジェクトの属性の設定 | オブジェクトへのアクセス: オブジェクトへのアクセスの試み(読み取り、書き込み、属性の取得、属性の設定)が行われた。<br><br>注: このイベントが発生した場合、Data ONTAPは、オブジェクトに対する最初のSMB読み取り操作とSMB書き込み操作(の成功または失敗)を監査します。これにより、1つのクライアントが、あるオブジェクトを開き、そのオブジェクトに対して連続的に多数の読み取りまたは書き込みを行っても、Data ONTAPが余計にログエントリを書き込むことがなくなります。 | ファイル アクセス |
| NA / 4664                      | ハードリンク                                                  | オブジェクトへのアクセス: ハードリンクの作成が試みられた。                                                                                                                                                                                                                       | ファイル アクセス |
| NA / 4818                      | 提案された集約型アクセス ポリシーで現在の集約型アクセス ポリシーと同じアクセス権限が許可されない       | オブジェクトへのアクセス: 集約型アクセス ポリシーのステージング。                                                                                                                                                                                                                   | ファイル アクセス |
| NA / NA Data ONTAP イベントID 9999 | オブジェクトの名前変更                                             | オブジェクトへのアクセス: オブジェクトの名前が変更された。これはData ONTAPのイベントです。Windowsでは、現在シングル イベントとしてはサポートされていません。                                                                                                                                                             | ファイル アクセス |
| NA / NA Data ONTAP イベントID 9998 | オブジェクトのリンク解除                                            | オブジェクトへのアクセス: オブジェクトのリンクが解除された。これはData ONTAPのイベントです。Windowsでは、現在シングル イベントとしてはサポートされていません。                                                                                                                                                            | ファイル アクセス |

#### イベント4656に関する補足情報

監査XMLイベント内のHandleIDタグには、アクセスされたオブジェクト(ファイルまたはディレクトリ)のハンドルが格納されています。EVTX 4656イベントのHandleIDタグに格納される情報は、オープン イベントが新規オブジェクトを作成するためのものか、既存のオブジェクトを開くためのものかによって異なります。

- オープン イベントが新規オブジェクト(ファイルまたはディレクトリ)を作成するためのオープン要求の場合、監査XMLイベント内の HandleIDタグは空のHandleIDを表示します(例:  
`<DataName="HandleID">00000000000000;00;00000000;00000000</Data>`)。  
HandleIDが空になっているのは、(新規オブジェクト作成のための)OPEN要求の監査は、実際のオブジェクト作成が行われる前、かつハンドルが存在する前に行われるからです。同じオブジェクトの以降の監査対象イベントでは、HandleIDタグに適切なオブジェクト ハンドルが格納されます。
- オープン イベントが既存のオブジェクトを開くためのオープン要求である場合、監査イベントでは、HandleIDタグにそのオブジェクトの割り当て済みハンドルが格納されます(例:  
`<DataName="HandleID">000000000000401;00;000000ea;00123ed4</Data>`)。

## 関連コンセプト

[NTFSセキュリティ形式のファイルおよびディレクトリの監査ポリシーの設定](#) (451ページ)

## 関連タスク

[監査対象オブジェクトへの完全パスの決定](#) (440ページ)

## 監査対象オブジェクトへの完全パスの決定

監査レコードの<ObjectName>タグに記録されているオブジェクト パスには、ボリュームの名前(カッコ内)と格納先ボリュームのルートを起点とする相対パスが格納されます。ジャンクション パスを含む、監査対象オブジェクトの完全パスを決定する場合には、実行すべき特定の手順があります。

### 手順

1. 監査イベントの<ObjectName>タグを調べて、ボリューム名と監査対象オブジェクトへの相対パスを確認します。

#### 例

この例では、ボリューム名が「data1」、ファイルへの相対パスが/dir1/file.txtになっています。

```
<Data Name="ObjectName">(data1);/dir1/file.txt </Data>
```

2. 前の手順で確認したボリューム名を使用して、監査対象オブジェクトが含まれているボリュームのジャンクション パスを確認します。

#### 例

```
volume show -junction -volume data1
```

| Vserver | Volume | Language    | Junction Active | Junction Path | Junction Path Source |
|---------|--------|-------------|-----------------|---------------|----------------------|
| vs1     | data1  | en_US.UTF-8 | true            | /data/data1   | RW_volume            |

3. <ObjectName>タグにあった相対パスをボリュームのジャンクション パスのあとに追加して、監査対象オブジェクトへの完全パスを決定します。

#### 例

```
/data/data1/dir1/file.txt
```

## シンボリックリンクおよびハード リンクを監査する際の考慮事項

シンボリックリンクおよびハード リンクを監査する際には、注意しなければならない特定の考慮事項があります。

監査レコードには、ObjectNameタグで特定される監査対象オブジェクトのパスなど、監査されるオブジェクトに関する情報が格納されます。シンボリックリンクおよびハード リンクのパスがObjectNameタグにどのように記録されるかを把握しておく必要があります。

### シンボリック リンク

シンボリックリンクは個別のinodeが割り当てられたファイルで、ターゲットと呼ばれるデスティネーション オブジェクトの場所へのポインターが含まれています。シンボリックリンクを介してオブジェク



トにアクセスする際、clustered Data ONTAPはシンボリックリンクを自動的に解釈し、ボリューム内のターゲット オブジェクトへのプロトコルに依存しない実際のパスを使用します。

次の出力例には2つのシンボリックリンクが含まれていますが、どちらもtarget.txtというファイルを指しています。一方のシンボリックリンクは相対シンボリックリンクで、他方は絶対シンボリックリンクです。どちらかのシンボリックリンクが監査された場合、監査イベントのObjectNameタグにはtarget.txtファイルへのパスが格納されます。

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt -> /data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

## ハードリンク

ハードリンクとは、ファイル システム上の既存のファイルに名前を関連付けるディレクトリ エントリです。ハードリンクは、元のファイルのinodeの場所を指しています。clustered Data ONTAPは、シンボリックリンクと同様にハードリンクを解釈し、ボリューム内のターゲット オブジェクトへの実際のパスを使用します。ハードリンク オブジェクトへのアクセスが監査された場合、ObjectNameタグにはハードリンクのパスではなく、この正規の絶対パスが記録されます。

## NTFS代替データ ストリームを監査する際の考慮事項

NTFS代替データ ストリームが設定されたファイルを監査する際には、注意しなければならない特定の考慮事項があります。

監査されるオブジェクトの場所は、2つのタグ、ObjectNameタグ(パス)とHandleIDタグ(ハンドル)を使用してイベントレコードに記録されます。どのストリーム要求がログに記録されるかを正しく把握するには、NTFS代替データ ストリームについてこれらのフィールドに記録される内容を理解する必要があります。

- EVTX ID:4656イベント(オープンおよび作成の監査イベント)
  - 代替データ ストリームのパスがObjectNameタグに記録されます。
  - 代替データ ストリームのハンドルがHandleIDタグに記録されます。
- EVTX ID:4663イベント(読み取り、書き込み、属性の取得など、その他すべての監査イベント)
  - (代替データ ストリームではなく)ベース ファイルのパスがObjectNameタグに記録されます。
  - 代替データ ストリームのハンドルがHandleIDタグに記録されます。

## 例

次の例は、HandleIDタグを使用して代替データ ストリームのEVTX ID:4663イベントを特定する方法を示しています。読み取りの監査イベントで記録されたObjectNameタグ(パス)はベース ファイルへのパスですが、HandleIDタグを使用してイベントを代替データ ストリームの監査レコードとして特定できます。

ストリーム ファイル名の形式はbase\_file\_name:stream\_nameです。この例では、次のパスの代替データ ストリームが設定されたベース ファイルがdir1ディレクトリに含まれています。

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

注: 次のイベント例の出力は省略されており、イベントに対するすべての出力タグが表示されているわけではありません。

EVTX ID 4656(オープンの監査イベント)の場合、代替データストリームの監査レコード出力で、**ObjectName**タグに代替データストリーム名が記録されています。

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  <Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">000000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">(data1);/dir1/file1.txt:stream1</Data>
Data>
  [...]
</EventData>
</Event>
- <Event>
```

EVTX ID 4663(読み取りの監査イベント)の場合、同じ代替データストリームの監査レコード出力で、**ObjectName**タグにベース ファイル名が記録されていますが、**HandleID**タグのハンドルは代替データストリームのハンドルであり、これを使用してこのイベントと代替データストリームを関連付けることができます。

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  <Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">000000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">(data1);/dir1/file1.txt</Data>
  [...]
</EventData>
</Event>
- <Event>
```

## 監査できるNFSファイルおよびディレクトリのアクセス イベント

Data ONTAPでは、特定のNFSファイルおよびディレクトリへのアクセス イベントを監査できます。どのようなアクセス イベントを監査できるか理解しておく、変換された監査イベント ログの結果を解釈するときに役立ちます。

次に、監査できるNFSファイルおよびディレクトリへのアクセス イベントを示します。

- READ
- OPEN
- CLOSE
- REaddir

- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

NFS のRENAMEイベントを確実に監査するには、ファイルではなくディレクトリに監査ACEを設定します。これは、ディレクトリ権限が十分であれば名前RENAME処理でファイルの権限はチェックされないためです。

**関連タスク**

- [UNIXセキュリティ形式のファイルおよびディレクトリの監査設定](#)(455ページ)
- [監査対象オブジェクトへの完全パスの決定](#)(440ページ)

## 監査設定の計画

FlexVolを備えたStorage Virtual Machine(SVM)で監査を設定する前に、使用可能な設定オプションを理解し、各オプションに設定する値を計画する必要があります。この情報は、ビジネス ニーズを満たす監査構成を設定するのに役立ちます。

すべての監査設定に共通する設定パラメータがあります。

また、統合および変換された監査ログをローテーションする際に次の2つのうちどちらの方法を使用するかを指定するパラメータもあります。監査設定を行う際に次の2つの方法のどちらかを指定できます。

- ログ サイズに基づいたログのローテーション  
ログのローテーションに使用されるデフォルトの方法です。
- スケジュールに基づいたログのローテーション

**すべての監査設定に共通するパラメータ**

監査設定の作成時に指定する必要がある必須パラメータが2つと、オプションのパラメータが3つあります。

| 情報の種類                                                     | オプション                    | 必須 | 含める | 値 |
|-----------------------------------------------------------|--------------------------|----|-----|---|
| <i>SVM</i> 名<br>監査設定を作成するSVMの名前。<br>SVMはすでに存在している必要があります。 | -vserver<br>vserver_name | ○  | ○   |   |

| 情報の種類                                                                                                                                                                                                                                                                                                    | オプション                | 必須                    | 含める                   | 値 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------|-----------------------|---|
| <p><b>ログ デスティネーション パス</b></p> <p>変換された監査ログを格納する場所を指定します。パスはSVM上にすでに存在している必要があります。</p> <p>パスには、最大864文字の文字列を指定でき、読み取り / 書き込み権限が必要です。</p> <p>パスが有効でない場合、監査設定コマンドは失敗します。</p> <p>SVMがSVMディザスタリカバリソースである場合、ログのデスティネーション パスをルート ボリューム上に設定することはできません。これは、ルート ボリュームのコンテンツはディザスタリカバリ デスティネーションにレプリケートされないためです。</p> | -destination<br>text | <input type="radio"/> | <input type="radio"/> |   |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | オプション                                                   | 必須 | 含める | 値 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|----|-----|---|
| <p><b>監査するイベントのカテゴリ</b><br/> 監査するイベントのカテゴリを指定します。監査できるイベント カテゴリは次のとおりです。</p> <ul style="list-style-type: none"> <li>ファイル アクセス イベント (SMBと NFSv4の両方)</li> <li>CIFSログオンおよびログオフ イベント</li> <li>集約型アクセス ポリシーのステージング イベント<br/> 集約型アクセス ポリシーのステージング イベントは、Windows 2012 Active Directoryドメイン以降で利用できる新しい高度な監査イベントです。集約型アクセス ポリシーのステージング イベントは、Active Directory で設定されている集約型アクセス ポリシーの変更に関する情報をログに記録します。</li> </ul> <p>デフォルトでは、ファイル アクセス イベントとCIFSログオンおよびログオフイベントが監査されます。</p> <p>注: イベント カテゴリとしてcap-stagingを指定するには、SVM上にCIFSサーバが存在している必要があります。</p> <p>CIFSサーバでダイナミック アクセス制御を有効にしていなくても監査設定では集約型アクセス ポリシーステージングを有効にすることができますが、集約型アクセス ポリシーのステージング イベントはダイナミック アクセス制御が有効になっている場合にしか生成されません。ダイナミック アクセス制御は、CIFSサーバ オプションを使用して有効にします。デフォルトでは有効になっていません。</p> | <p>-events {file-ops cifs-logon-logoff cap-staging}</p> | ×  |     |   |
| <p><b>ログ ファイルの出力形式</b><br/> 監査ログの出力形式を指定します。出力形式には、Data ONTAP固有のXMLまたはMicrosoft WindowsのEVTXログ形式のどちらかを指定できます。デフォルトの出力形式はEVTXです。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>-format {xml evtx}</p>                               | ×  |     |   |

| 情報の種類                                                                                                                                                      | オプション                           | 必須 | 含める | 値 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|----|-----|---|
| <b>ログ ファイルのローテーションの制限</b><br>保持する監査ログ ファイルの数を指定します。指定した値を超えたログ ファイルが古い順から削除されます。たとえば、5を入力すると、最新の5つの監査ログが保持されます。<br>値0を指定すると、すべてのログ ファイルが保持されます。デフォルト値は0です。 | -rotate-limit<br><i>integer</i> | ×  |     |   |

### 監査イベント ログのローテーションのタイミングを決定するパラメータ

#### ログ サイズに基づいたログのローテーション

デフォルトでは、サイズに基づいた監査ログのローテーションが行われます。デフォルトのログ サイズは100MBです。デフォルトのログ ローテーション方法とデフォルトのログ サイズを使用する場合、ログ ローテーションに関するパラメータは設定する必要はありません。デフォルトのログ サイズを使用しない場合は、-rotate-sizeパラメータの設定によってカスタム ログ サイズを指定できます。

| 情報の種類                                          | オプション                                              | 必須 | 含める | 値 |
|------------------------------------------------|----------------------------------------------------|----|-----|---|
| <b>ログ ファイルの最大サイズ</b><br>監査ログ ファイルの最大サイズを指定します。 | -rotate-size<br>{ <i>integer</i> [KB MB GB TB PB]} | ×  |     |   |

#### スケジュールに基づいたログのローテーション

スケジュールに基づく監査ログのローテーションを選択した場合は、任意の組み合わせで時間ベースのローテーション パラメータを使用して、ログのローテーションをスケジュールすることができます。

- 時間ベースのログ ローテーション パラメータを設定した場合は、ログ サイズではなく、設定されたスケジュールに基づいてログのローテーションが行われます。
- 時間ベースのローテーションを使用する場合、-rotate-schedule-minuteパラメータの設定は必須です。
- これ以外の時間ベースのローテーション パラメータは、すべてオプションです。
- ローテーション スケジュールは、時間に関係するすべての値を用いて計算されます。  
たとえば、-rotate-schedule-minuteパラメータのみを指定した場合、監査ログ ファイルのローテーションは、年間の各月のすべての曜日の毎時間、指定された分に行われます。
- 時間ベースのローテーション パラメータを1つか2つ(たとえば、-rotate-schedule-monthと-rotate-schedule-minutes)を指定した場合、ログ ファイルのローテーションは、指定した月のすべての曜日の毎時間、指定された分に行われます。  
たとえば、監査ログのローテーションを、1月、3月、8月の間、月曜日、水曜日、土曜日の10時30分に実行するように指定できます。
- rotate-schedule-dayofweekと-rotate-schedule-dayで指定された値は、それぞれ個別に判断されます。  
たとえば、-rotate-schedule-dayofweekに金曜日を指定し、-rotate-schedule-dayに13を指定した場合、監査ログのローテーションは、単に13日の金曜日ごとに行われるのではなく、指定した月の各13日の金曜日に実行されます。

次に示す使用可能な監査パラメータのリストを使用すると、監査イベント ログのローテーションのスケジュール設定に使用する値を決定できます。

| 情報の種類                                                                                                                                                                                                          | オプション                                                        | 必須                                 | 含める | 値 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|------------------------------------|-----|---|
| <p><b>ログ ローテーション スケジュール: 月</b><br/>監査ログのローテーションを実行する月を指定します。<br/>指定できる値は、<b>January</b>～<b>December</b>と、<b>all</b>です。たとえば、監査ログのローテーションが1月、3月、8月に行われるように指定できます。</p>                                            | <p>-rotate-schedule-month<br/><i>chron_month</i></p>         | ×                                  |     |   |
| <p><b>ログ ローテーション スケジュール: 曜日</b><br/>監査ログのローテーションを実行する日(曜日)を指定します。<br/>指定できる値は、<b>January</b>～<b>December</b>と、<b>all</b>です。たとえば、監査ログのローテーションが木曜日と金曜日、またはすべての曜日に行われるように指定できます。</p>                              | <p>-rotate-schedule-dayofweek<br/><i>chron_dayofweek</i></p> | ×                                  |     |   |
| <p><b>ログ ローテーション スケジュール: 日</b><br/>監査ログのローテーションを実行する日(月の日)を指定します。<br/>指定できる値は、<b>1</b>～<b>31</b>です。たとえば、監査ログのローテーションが毎月10日と20日、または毎日行われるように指定できます。</p>                                                         | <p>-rotate-schedule-day<br/><i>chron_dayofmonth</i></p>      | ×                                  |     |   |
| <p><b>ログ ローテーション スケジュール: 時間</b><br/>監査ログのローテーションを実行する時間を決めます。<br/>指定できる値の範囲は、<b>0</b>(午前零時)～<b>23</b>(午後11時)です。<b>all</b>を指定すると、監査ログのローテーションが1時間に1回行われます。たとえば、監査ログのローテーションが6(午前6時)と18(午後6時)に行われるように指定できます。</p> | <p>-rotate-schedule-hour<br/><i>chron_hour</i></p>           | ×                                  |     |   |
| <p><b>ログ ローテーション スケジュール: 分</b><br/>監査ログのローテーションを実行する分を決めます。<br/>指定できる値の範囲は、<b>0</b>～<b>59</b>です。たとえば、監査ログのローテーションが30分に行われるように指定できます。</p>                                                                       | <p>-rotate-schedule-minute<br/><i>chron_minute</i></p>       | ○(スケジュールベースのログ ローテーションを設定している場合のみ) |     |   |

#### 関連コンセプト

[ファイルおよびフォルダの監査ポリシーの設定](#)(450ページ)

[監査の要件と考慮事項](#)(435ページ)

[サポートされる監査イベント ログの形式](#)(436ページ)

**関連タスク**

[SVMでのファイルとディレクトリの監査設定の作成](#)(448ページ)

**SVMでのファイルとディレクトリの監査設定の作成**

Storage Virtual Machine (SVM) 上でファイルとディレクトリの監査設定を作成するには、使用可能な設定オプションを理解し、設定の計画を立てたうえで、設定を行って有効にします。作成後、監査設定に関する情報を表示して、設定した内容が適切であることを確認できます。

**手順**

1. [監査設定の作成](#) (448ページ)  
ファイルおよびディレクトリ イベントの監査を開始する前に、監査設定をStorage Virtual Machine (SVM) で作成する必要があります。
2. [SVMでの監査の有効化](#) (450ページ)  
監査設定のセットアップが完了したら、Storage Virtual Machine (SVM) で監査を有効にする必要があります。
3. [監査設定の確認](#) (450ページ)  
監査設定が完了したら、監査が適切に設定されて有効になっていることを確認します。

**関連コンセプト**

[監査設定の計画](#) (443ページ)

[Data ONTAP CLIを使用したNTFS監査ポリシーの設定方法](#) (454ページ)

[監査設定の管理](#) (459ページ)

[DAC\(ダイナミック アクセス制御\)を使用したファイル アクセスの保護](#) (200ページ)

**関連タスク**

[Windowsの\[セキュリティ\]タブを使用したNTFS監査ポリシーの設定](#) (451ページ)

[UNIXセキュリティ形式のファイルおよびディレクトリの監査設定](#) (455ページ)

[SVMでの監査の有効化と無効化](#) (459ページ)

[監査設定の削除](#) (462ページ)

[監査イベント ログの手動ローテーション](#) (459ページ)

**監査設定の作成**

ファイルおよびディレクトリ イベントの監査を開始する前に、監査設定をStorage Virtual Machine (SVM) で作成する必要があります。

**開始する前に**

集約型アクセス ポリシー ステージングの監査設定を作成する予定がある場合は、SVMにCIFSサーバが存在している必要があります。

**注:** CIFSサーバでダイナミック アクセス制御を有効にしていなくても監査設定では集約型アクセス ポリシー ステージングを有効にすることができますが、集約型アクセス ポリシーのステージング イベントはダイナミック アクセス制御が有効になっている場合にしか生成されません。ダイナミック アクセス制御は、CIFSサーバ オプションを使用して有効にします。デフォルトでは有効になっていません。



タスク概要

SVMがSVMディザスタリカバリソースである場合、デスティネーションパスをルートボリューム上に設定することはできません。

手順

- 1. 計画ワークシートの情報を使用して、ログサイズまたはスケジュールに基づいて監査ログのローテーションを行うための監査設定を作成します。

| 監査ログのローテーションの 基準 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログサイズ            | <code>vserver audit create -vserver <i>vserver_name</i> -destination <i>path</i> -events [{<i>file-ops</i> <i>cifs-logon-logoff</i> <i>cap-staging</i>}] [-format {<i>xml</i> <i>evtx</i>}] [-rotate-limit <i>integer</i>] [-rotate-size {<i>integer</i>[KB MB GB TB PB]]]</code>                                                                                                                                                                                                                                                              |
| スケジュール           | <code>vserver audit create -vserver <i>vserver_name</i> -destination <i>path</i> -events [{<i>file-ops</i> <i>cifs-logon-logoff</i> <i>cap-staging</i>}] [-format {<i>xml</i> <i>evtx</i>}] [-rotate-limit <i>integer</i>] [-rotate-schedule-month <i>chron_month</i>] [-rotate-schedule-dayofweek <i>chron_dayofweek</i>] [-rotate-schedule-day <i>chron_dayofmonth</i>] [-rotate-schedule-hour <i>chron_hour</i>] -rotate-schedule-minute <i>chron_minute</i></code><br><br>注: 時間に基づく監査ログのローテーションを設定する場合、-rotate-schedule-minute/パラメータは必須です。 |

例

次の例は、サイズに基づくローテーションを使用してファイル処理とCIFSログオンおよびログオフイベント(デフォルト)を監査する監査設定を作成します。ログ形式はEVTX(デフォルト)です。ログは/audit\_logディレクトリに格納されます。ログファイルサイズの上限は200MBです。ログのサイズが200MB以上になると、ログのローテーションが実行されます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-size 200MB
```

次の例は、サイズに基づくローテーションを使用してファイル処理とCIFSログオンおよびログオフイベント(デフォルト)を監査する監査設定を作成します。ログ形式はEVTX(デフォルト)です。ログファイルサイズの上限は100MB(デフォルト)、ログのローテーション回数の上限は5回です。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-limit 5
```

次の例は、時間に基づくローテーションを使用してファイル処理、CIFSログオンおよびログオフイベント、集約型アクセスポリシーのステージングイベントを監査する監査設定を作成します。ログ形式はEVTX(デフォルト)です。監査ログのローテーションが毎月、そして毎日、午後12:30に実行されます。ログのローテーション回数の上限は5回です。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events file-ops,cifs-logon-logoff,cap-staging -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

## SVMでの監査の有効化

監査設定のセットアップが完了したら、Storage Virtual Machine (SVM) で監査を有効にする必要があります。

### 開始する前に

SVMの監査設定がすでに存在している必要があります。

### タスク概要

SVMディザスタリカバリのID破棄設定が (SnapMirror初期化完了後に) 先に開始され、SVMに監査設定がある場合、監査設定は自動的に無効化されます。読み取り専用SVMでは、ステージング ボリュームがいっぱいにならないように監査が無効になっています。監査を有効にできるのは、SnapMirror関係が解除されてSVMが読み書き可能になったあとです。

### 手順

1. SVMで監査を有効にします。

```
vserver audit enable -vserver vserver_name
```

### 例

```
vserver audit enable -vserver vs1
```

## 監査設定の確認

監査設定が完了したら、監査が適切に設定されて有効になっていることを確認します。

### 手順

1. 監査設定を確認します。

```
vserver audit show -instance -vserver vserver_name
```

### 例

次のコマンドは、Storage Virtual Machine (SVM) vs1のすべての監査設定の情報をリスト形式で表示します。

```
vserver audit show -instance -vserver vs1
```

```

Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtX
Log File Size Limit: 200MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0

```

## ファイルおよびフォルダの監査ポリシーの設定

ファイルやフォルダに対するアクセス イベントの監査は、2つのステップで実装します。まず、FlexVolを備えたStorage Virtual Machine (SVM) で監査設定を作成し、有効にする必要がありま

す。次に、監視するファイルおよびフォルダに対して監査ポリシーを設定する必要があります。成功したアクセス試行と失敗したアクセス試行の両方を監視するように監査ポリシーを設定できます。

SMBとNFSの両方の監査ポリシーを設定できます。SMBとNFSの監査ポリシーでは、設定の要件や監査の機能が異なります。

適切な監査ポリシーが設定されている場合、Data ONTAPは、SMBまたはNFSサーバの稼働中に限り、監査ポリシーでの指定に従ってSMBおよびNFSアクセス イベントを監視します。

## 関連コンセプト

[Data ONTAP監査プロセスの仕組み](#) (433ページ)

[監査できるSMBイベント](#) (438ページ)

[ファイルおよびディレクトリに適用されている監査ポリシーに関する情報の表示](#) (455ページ)

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#) (154ページ)

## NTFSセキュリティ形式のファイルおよびディレクトリの監査ポリシーの設定

ファイルおよびディレクトリ操作を監査する前に、監査情報を収集するファイルおよびディレクトリに対して監査ポリシーを設定する必要があります。これは、監査の設定と有効化に加えて行います。NTFS監査ポリシーを設定するには、Windowsの[セキュリティ]タブを使用するか、Data ONTAP CLIを使用します。

### Windowsの[セキュリティ]タブを使用したNTFS監査ポリシーの設定

Windowsの[プロパティ]ウィンドウにあるWindowsの[セキュリティ]タブを使用して、ファイルやディレクトリに対する監査ポリシーを設定できます。これはWindowsクライアント上に存在するデータの監査ポリシーを設定する場合と同じ方法であり、ユーザは使い慣れたものと同じGUIインターフェイスを使用できます。

#### 開始する前に

監査は、SACLを適用するデータが格納されているStorage Virtual Machine (SVM) で設定する必要があります。

#### タスク概要

NTFS監査ポリシーの設定は、NTFSセキュリティ記述子に関連付けられているNTFSのシステムアクセス制御リスト(SACL)にエントリを追加することによって行います。その後、セキュリティ記述子をNTFSファイルおよびディレクトリに適用します。これらのタスクはWindows GUIによって自動的に処理されます。セキュリティ記述子には、ファイルやフォルダのアクセス権を適用するための随意アクセス制御リスト(DACL)、ファイルやフォルダを監査するためのシステム アクセス制御リスト(SACL)、またはSACLとDACLの両方を含めることができます。

Windowsの[プロパティ]ウィンドウにあるWindowsの[セキュリティ]タブを使用して、Windowsホストで次の手順を実行することで、個々のファイルやフォルダに対するアクセスを監査するためのNTFS監査ポリシーを設定できます。

#### 手順

1. Windowsエクスプローラの[ツール]メニューで、[ネットワークドライブの割り当て]を選択します。
2. [ネットワークドライブの割り当て]ボックスのすべての項目に入力します。
  - a. [ドライブ]文字を選択します。
  - b. [フォルダ]ボックスに、監査するデータが格納されている共有を含むCIFSサーバ名と、共有の名前を入力します。

**例**

CIFSサーバ名が「CIFS\_SERVER」で、共有の名前が「share1」である場合は、「\\CIFS\_SERVER\share1」と入力します。

**注:** CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

c. **[完了]**をクリックします。

選択したドライブがマウントされて使用可能な状態となり、共有内に格納されているファイルやフォルダがWindowsエクスプローラ ウィンドウに表示されます。

3. アクセスの監査を有効にするファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリで右クリックし、**[プロパティ]**を選択します。
5. **[セキュリティ]**タブを選択します。
6. **[詳細]**をクリックします。
7. **[監査]**タブを選択します。
8. 次のうち必要な操作を実行します。

| 目的                    | 操作                                                                                                                                                                                                      |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しいユーザまたはグループの監査を設定する | <ol style="list-style-type: none"> <li>a. <b>[追加]</b>をクリックします。</li> <li>b. <b>[選択するオブジェクト名を入力してください]</b>ボックスに、追加するユーザまたはグループの名前を入力します。</li> <li>c. <b>[OK]</b>をクリックします。</li> </ol>                      |
| ユーザまたはグループから監査を削除する   | <ol style="list-style-type: none"> <li>a. <b>[選択するオブジェクト名を入力してください]</b>ボックスで、削除するユーザまたはグループを選択します。</li> <li>b. <b>[削除]</b>をクリックします。</li> <li>c. <b>[OK]</b>をクリックします。</li> <li>d. 残りの手順は不要です。</li> </ol> |
| ユーザまたはグループの監査を変更する    | <ol style="list-style-type: none"> <li>a. <b>[選択するオブジェクト名を入力してください]</b>ボックスで、変更するユーザまたはグループを選択します。</li> <li>b. <b>[編集]</b>をクリックします。</li> <li>c. <b>[OK]</b>をクリックします。</li> </ol>                         |

ユーザまたはグループの監査を設定する場合、および既存のユーザまたはグループの監査を変更する場合は、[<object> の監査エントリ]ボックスが開きます。

9. **[適用先]**ボックスで、この監査エントリを適用する方法を選択します。

次のいずれかを選択できます。

- このフォルダ、サブフォルダおよびファイル
- このフォルダとサブフォルダ
- このフォルダのみ
- このフォルダとファイル

- サブフォルダとファイルのみ
- サブフォルダのみ
- ファイルのみ

単一ファイルの監査を設定している場合は、**[適用先]**ボックスを使用できません。**[適用先]**はデフォルトの**[このオブジェクトのみ]**になります。

注: 監査ではSVMリソースが使用されるので、セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。

10. **[アクセス]**ボックスで、成功したイベント、失敗したイベント、またはその両方のいずれを監査対象にするかを選択します。

- 成功したイベントを監査するには、**[成功]**ボックスを選択します。
- 失敗したイベントを監査するには、**[失敗]**ボックスを選択します。

次のイベントを監査できます。

- フル コントロール
- フォルダのスキャン / ファイルの実行
- フォルダの一覧 / データの読み取り
- 属性の読み取り
- 拡張属性の読み取り
- ファイルの作成 / データの書き込み
- フォルダの作成 / データの追加
- 属性の書き込み
- 拡張属性の書き込み
- サブフォルダとファイルの削除
- 削除
- アクセス許可の読み取り
- アクセス許可の変更
- 所有権の取得

注: セキュリティ要件を満たすために監視する必要がある操作のみを選択してください。これらの監査可能なイベントの詳細については、Windowsのマニュアルを参照してください。

11. 元のコンテナにあるファイルとフォルダのみに監査設定を適用する場合は、**[これらの監査エントリを、このコンテナの中にあるオブジェクトやコンテナにのみ適用する]**ボックスを選択します。
12. **[適用]**をクリックします。
13. 監査エントリの追加、削除、または編集が完了したら、**[OK]**をクリックします。  
[<object> の監査エントリ]ボックスが閉じます。
14. **[監査]**ボックスで、このフォルダの継承設定を選択します。  
次のいずれかを選択できます。
  - **[このオブジェクトの親からの継承可能な監査エントリを含める]**ボックスを選択する。

- [すべての子孫の既存の継承可能な監査エントリすべてを、このオブジェクトからの継承可能な監査エントリで置き換える]ボックスを選択する。
- 両方のボックスを選択する。
- どちらのボックスも選択しない。

単一ファイルのSACLを設定している場合は、[監査]ダイアログ ボックスに[すべての子孫の既存の継承可能な監査エントリすべてを、このオブジェクトからの継承可能な監査エントリで置き換える]ボックスは表示されません。

注: セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。

#### 15. [OK]をクリックします。

[監査]ボックスが閉じます。

#### 関連コンセプト

[監査できるSMBイベント](#) (438ページ)

#### 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用](#) (275ページ)

[CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示](#) (457ページ)

[Windowsの\[セキュリティ\]タブを使用した監査ポリシーに関する情報の表示](#) (455ページ)

### Data ONTAP CLIを使用したNTFS監査ポリシーの設定方法

Data ONTAP CLIを使用して、ファイルおよびフォルダに対して監査ポリシーを設定できます。これにより、WindowsクライアントでSMB共有を使用してデータに接続することなくNTFS監査ポリシーを設定できます。

NTFS監査ポリシーを設定するには、`vserver security file-directory` コマンド ファミリーを使用します。

CLIで設定できるのはNTFS SACLだけです。NFSv4 SACLの設定は、このData ONTAPコマンドファミリーではサポートされていません。このコマンドを使用してNTFS SACLを設定し、ファイルおよびフォルダに追加する方法については、マニュアル ページを参照してください。

#### 関連コンセプト

[ストレージレベルのアクセス保護を使用したファイル アクセスの保護](#) (154ページ)

[監査できるSMBイベント](#) (438ページ)

#### 関連タスク

[CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用](#) (275ページ)

[CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示](#) (457ページ)

#### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: `vserver security file-directory show - Display file/folder security information`](#)

## UNIXセキュリティ形式のファイルおよびディレクトリの監査設定

UNIXセキュリティ形式のファイルおよびディレクトリの監査を設定するには、NFSv4.x ACLに監査ACEを追加します。これにより、セキュリティの目的で特定のNFSファイルおよびディレクトリのアクセス イベントを監視できます。

### タスク概要

NFSv4.xでは、随意ACEとシステムACEの両方が同じACLに格納されます。個別のDACLとSACLには格納されません。したがって、既存のACLに監査ACEを追加する際は、既存のACLを上書きして失われることがないように、細心の注意を払う必要があります。既存のACLに監査ACEを追加する順序は重要ではありません。

### 手順

1. `nfs4_getfacl`または同等のコマンドを使用して、ファイルまたはディレクトリの既存のACLを取得します。  
ACLの操作の詳細については、NFSクライアントのマニュアル ページを参照してください。
2. 目的の監査ACEを追加します。
3. `nfs4_setfacl`または同等のコマンドを使用して、ファイルまたはディレクトリに更新したACLを適用します。

### 関連タスク

[CLIを使用したFlexVolのNFSv4監査ポリシーに関する情報の表示](#) (255ページ)

### 関連参照情報

[監査できるNFSファイルおよびディレクトリのアクセス イベント](#) (442ページ)

### 関連情報

[clustered Data ONTAP 8.3.1 マニュアル ページ: vserver security file-directory show - Display file/folder security information](#)

## ファイルおよびディレクトリに適用されている監査ポリシーに関する情報の表示

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステム アクセス制御リスト(SACL)が設定されていることを確認できます。

### 関連コンセプト

[ファイルおよびフォルダの監査ポリシーの設定](#) (450ページ)

## Windowsの[セキュリティ]タブを使用した監査ポリシーに関する情報の表示

Windowsの[プロパティ]ウィンドウにある[セキュリティ]タブを使用して、ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示できます。これはWindowsサーバ上に存在するデ

ータを利用する場合と同じ方法であり、ユーザは使い慣れたものと同じGUIインターフェイスを使用できます。

### タスク概要

NTFSファイルおよびフォルダに適用されているSACLに関する情報を表示するには、Windowsホストで以下の手順を実行します。

### 手順

1. Windowsエクスプローラの[ツール]メニューで、[ネットワークドライブの割り当て]を選択します。
2. [ネットワークドライブの割り当て]ダイアログ ボックスのすべての項目に入力します。
  - a. [ドライブ]文字を選択します。
  - b. [フォルダ]ボックスに、監査するデータが格納されている共有を含むStorage Virtual Machine (SVM) のIPアドレスまたはCIFSサーバ名と、共有の名前を入力します。

### 例

CIFSサーバ名が「CIFS\_SERVER」で、共有の名前が「share1」である場合は、「\CIFS\_SERVER\share1」と入力します。

注: CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

- c. [完了]をクリックします。
- 選択したドライブがマウントされて使用可能な状態となり、共有内に格納されているファイルやフォルダがWindowsエクスプローラ ウィンドウに表示されます。
3. 監査情報を表示するファイルまたはディレクトリを選択します。
  4. ファイルまたはディレクトリで右クリックし、[プロパティ]を選択します。
  5. [セキュリティ]タブを選択します。
  6. [詳細]をクリックします。
  7. [監査]タブを選択します。
  8. [続行]をクリックします。
- [監査]ボックスが開きます。[監査エントリ]ボックスに、SACLが適用されているユーザとグループの概要が表示されます。
9. [監査エントリ]ボックスで、表示するSACLエントリを保持するユーザまたはグループを選択します。
  10. [編集]をクリックします。
- [<object> の監査エントリ]ボックスが開きます。
11. [アクセス]ボックスで、選択したオブジェクトに適用されている現在のSACLを確認します。
  12. [キャンセル]をクリックして、[<object> の監査エントリ]ボックスを閉じます。
  13. [キャンセル]をクリックして、[監査]ボックスを閉じます。



## CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システム アクセス制御リストに関する情報など、FlexVolのNTFS監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

### タスク概要

Storage Virtual Machine (SVM) の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力は、要約形式または詳細なリストで表示できます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、NTFSのSystem Access Control List (SACL; システム アクセス制御リスト) のみが監査ポリシーに使用されます。
- NTFS対応のセキュリティが有効なmixedセキュリティ形式のボリューム内のファイルおよびフォルダには、NTFS監査ポリシーを適用できます。  
mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル アクセス権 (モード ビットまたはNFSv4 ACL) を使用するファイルおよびディレクトリと、NTFSファイル アクセス権を使用するファイルおよびディレクトリを格納できます。
- mixedセキュリティ形式のボリュームの最上位では、UNIXまたはNTFS対応のセキュリティを有効にすることができ、そこにはNTFS SACLが格納されている場合も、格納されていない場合もあります。
- mixedセキュリティ形式のボリュームまたはqtreeでは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、ストレージレベルのアクセス保護セキュリティを設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeの出力には、標準ファイルおよびフォルダのNFSv4 SACLとストレージレベルのアクセス保護のNTFS SACLの両方が表示される場合があります。
- NTFS対応のセキュリティが有効なデータへのパスをコマンドに入力した場合、所定のファイルまたはディレクトリ パスでダイナミック アクセス制御が設定されていれば、出力にダイナミック アクセス制御のACEに関する情報も表示されます。
- NTFS対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報の表示時には、UNIX関連の出力フィールドに表示専用のUNIXファイル アクセス権情報が格納されます。  
ファイル アクセス権の決定時には、NTFSセキュリティ形式のファイルおよびフォルダで、NTFSファイル アクセス権とWindowsユーザおよびグループのみが使用されます。
- ACL出力は、NTFSまたはNFSv4セキュリティ形式によるファイルおよびフォルダでのみ表示されます。  
このフィールドは、モード ビットのアクセス権のみ (NFSv4 ACLはなし) が適用されているUNIXセキュリティ形式のファイルおよびフォルダでは空になります。
- ACL出力の所有者およびグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。

### 手順

1. ファイルおよびディレクトリ監査ポリシー設定を適切な詳細レベルで表示します。

| 情報の表示方法 | 入力するコマンド                                                                           |
|---------|------------------------------------------------------------------------------------|
| 要約形式    | <code>vserver security file-directory show -vserver vserver_name -path path</code> |

| 情報の表示方法 | 入力するコマンド                                                                                           |
|---------|----------------------------------------------------------------------------------------------------|
| 詳細情報を展開 | <b>vserver security file-directory show -vserver<br/>vserver_name -path path -expand-mask true</b> |

## 例

次の例は、SVM vs1のパス/corpに関する監査ポリシーの情報を表示します。このパスではNTFS対応のセキュリティが有効になっています。NTFSセキュリティ記述子には、SUCCESSおよびSUCCESS / FAIL SACLエントリの両方が格納されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
Vserver: vs1
File Path: /corp
File Inode Number: 357
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACES
        ALL-DOMAIN\Administrator-0x100081-0I|CI|SA|FA
        SUCCESSFUL-DOMAIN\user1-0x100116-0I|CI|SA
      DACL - ACES
        ALLOW-BUILTIN\Administrators-0x1f01ff-0I|CI
        ALLOW-BUILTIN\Users-0x1f01ff-0I|CI
        ALLOW-CREATOR OWNER-0x1f01ff-0I|CI
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-0I|CI
```

次の例は、SVM vs1のパスSVMに関する監査ポリシーの情報を表示します。このパスには、標準ファイルおよびフォルダのSACLとストレージレベルのアクセス保護のSACLの両方が格納されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
      Control:0xaa14
      Owner:BUILTIN\Administrators
      Group:BUILTIN\Administrators
      SACL - ACES
        AUDIT-EXAMPLE\marketing-0xf01ff-0I|CI|FA
      DACL - ACES
        ALLOW-EXAMPLE\Domain Admins-0x1f01ff-0I|CI
        ALLOW-EXAMPLE\marketing-0x1200a9-0I|CI

Storage-Level Access Guard security
SACL (Applies to Directories):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
```

```

DACL (Applies to Files):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## 監査設定の管理

Storage Virtual Machine (SVM) の監査設定は、手動での監査ログのローテーション、監査の有効化または無効化、監査設定に関する情報の表示、監査設定の変更、監査設定の削除を行うことで、管理できます。また、監査をサポートしていないリリースへ切り替えた場合の問題について、理解しておく必要があります。

### 関連コンセプト

[監査およびステージング用のボリュームのスペースに関する問題のトラブルシューティング](#)  
(463ページ)

## 監査イベント ログの手動ローテーション

監査イベント ログは、表示する前に、ユーザが読解可能な形式に変換する必要があります。Data ONTAPで自動ローテーションされる前に特定のStorage Virtual Machine (SVM) のイベント ログを表示する場合は、そのSVMで監査イベント ログの手動ローテーションを実行します。

### 手順

1. `vserver audit rotate-log` コマンドを使用して監査イベント ログをローテーションします。

### 例

```
vserver audit rotate-log -vserver vs1
```

監査イベント ログは監査設定で指定されている形式 (XML または EVTX) で、SVM の監査イベント ログ ディレクトリに保存され、適切なアプリケーションを使用して表示できます。

### 関連コンセプト

[監査イベント ログの表示](#) (436ページ)

### 関連タスク

[SVMでのファイルとディレクトリの監査設定の作成](#) (448ページ)

## SVMでの監査の有効化と無効化

Storage Virtual Machine (SVM) での監査を有効または無効にすることができます。必要に応じて、監査を無効にすることで、ファイルおよびディレクトリの監査を一時的に停止できます。監査は、いつでも有効にすることができます (監査設定が存在する場合)。

### 開始する前に

SVMで監査を有効にするには、SVMの監査設定がすでに存在している必要があります。

### タスク概要

監査を無効にしても、監査設定は削除されません。

**手順**

1. 適切なコマンドを実行します。

| 監査設定 | 入力するコマンド                                                 |
|------|----------------------------------------------------------|
| 有効   | <code>vserver audit enable -vserver vserver_name</code>  |
| 無効   | <code>vserver audit disable -vserver vserver_name</code> |

2. 監査が目的の状態になっていることを確認します。

`vserver audit show -vserver vserver_name`

**例**

次の例では、SVM vs1で監査を有効にします。

```
cluster1::> vserver audit enable -vserver vs1
cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
            Auditing state: true
      Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
        Log File Size Limit: 100MB
      Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                Rotation Schedules: -
        Log Files Rotation Limit: 10
```

次の例では、SVM vs1で監査を無効にします。

```
cluster1::> vserver audit disable -vserver vs1

                Vserver: vs1
            Auditing state: false
      Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
        Log File Size Limit: 100MB
      Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                Rotation Schedules: -
        Log Files Rotation Limit: 10
```

**関連タスク**

[監査設定の削除](#) (462ページ)

## 監査設定に関する情報の表示

監査設定に関する情報を表示できます。この情報は、各SVMで適切な設定が使用されているかどうか確認するのに役立ちます。また、表示される情報から、監査設定が有効であるかどうかを確認することもできます。

### タスク概要

すべてのSVMの監査設定に関する詳細情報を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- 監査設定が適用されるSVMの名前
- 監査の状態(**true**または**false**)  
監査の状態が**true**の場合、監査は有効です。監査の状態が**false**の場合、監査は無効です。
- 監査するイベントのカテゴリ
- 監査ログ形式
- 統合および変換された監査ログが監査サブシステムによって格納されるターゲット ディレクトリ

### 手順

1. `vserver audit show`コマンドを使用して、監査設定に関する情報を表示します。

このコマンドの使用の詳細については、マニュアル ページを参照してください。

#### 例

次の例は、すべてのSVMの監査設定の概要を表示したものです。

```
cluster1::> vserver audit show
```

| Vserver | State | Event Types | Log Format | Target Directory |
|---------|-------|-------------|------------|------------------|
| vs1     | false | file-ops    | evtx       | /audit_log       |

次の例は、すべてのSVMの監査設定情報をリスト形式で表示したものです。

```
cluster1::> vserver audit show -instance
```

```

Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtx
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0

```

### 関連タスク

[SVMでのファイルとディレクトリの監査設定の作成](#) (448ページ)

## 監査設定を変更するコマンド

監査設定はいつでも変更できます。ログのデスティネーションパスと形式、監査するイベントのカテゴリ、ログファイルの自動保存方法、および保存するログファイルの最大数を変更できます。

| 状況                           | 使用するコマンド                                                                                                                                                                                                                                   |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログのデスティネーションパスの変更            | <code>vserver audit modify</code> と <code>-destination</code> パラメータ                                                                                                                                                                        |
| 監査するイベントのカテゴリの変更             | <code>vserver audit modify</code> と <code>-events</code> パラメータ<br><br>注: 集約型アクセスポリシーのステージングイベントを監査するには、Dynamic Access Control (DAC; ダイナミックアクセス制御) のCIFSサーバオプションがStorage Virtual Machine (SVM) で有効になっている必要があります。                            |
| ログ形式の変更                      | <code>vserver audit modify</code> と <code>-format</code> パラメータ                                                                                                                                                                             |
| 内部的な一時ログファイルサイズに基づいた自動保存の有効化 | <code>vserver audit modify</code> と <code>-rotate-size</code> パラメータ                                                                                                                                                                        |
| 時間間隔に基づいた自動保存の有効化            | <code>vserver audit modify</code> と <code>-rotate-schedule-month</code> 、 <code>-rotate-schedule-dayofweek</code> 、 <code>-rotate-schedule-day</code> 、 <code>-rotate-schedule-hour</code> 、および <code>-rotate-schedule-minute</code> パラメータ |
| 保存されるログファイルの最大数の指定           | <code>vserver audit modify</code> と <code>-rotate-limit</code> パラメータ                                                                                                                                                                       |

## 監査設定の削除

Storage Virtual Machine (SVM) でのファイルおよびディレクトリイベントの監査が必要なくなり、SVMで監査設定を維持する必要がなくなった場合は、監査設定を削除できます。

### 手順

1. 監査設定を無効にします。

```
vserver audit disable -vserver vserver_name
```

#### 例

```
vserver audit disable -vserver vs1
```

2. 監査設定を削除します。

```
vserver audit delete -vserver vserver_name
```

#### 例

```
vserver audit delete -vserver vs1
```

### 関連タスク

[SVMでの監査の有効化と無効化](#) (459ページ)

## リバート時のプロセス

クラスタのリバートを予定している場合は、クラスタ内に監査が有効になっているStorage Virtual Machine (SVM) が存在するときにData ONTAPで実行されるリバート プロセスを理解しておく必要があります。リバートする前に特定の操作を実行する必要があります。

### CIFSのログオンおよびログオフ イベントや集約型アクセス ポリシーのステージング イベントの監査をサポートしていないバージョンのclustered Data ONTAPへのリバート

CIFSのログオンおよびログオフ イベントや集約型アクセス ポリシーのステージング イベントは、clustered Data ONTAP 8.3以降でサポートされます。これらのイベント タイプをサポートしていないバージョンのclustered Data ONTAPへのリバートを予定していて、これらのイベント タイプを監視する監査が設定されている場合は、リバート前に監査が有効になっているSVMの監査設定を変更する必要があります。設定は、ファイル処理イベントのみが監査されるように変更する必要があります。

#### 関連タスク

[SVMでの監査の有効化と無効化](#) (459ページ)

[監査設定の削除](#) (462ページ)

## 監査およびステージング用のボリュームのスペースに関する問題のトラブルシューティング

ステージング ボリュームや監査イベント ログを格納するボリュームに十分なスペースがない場合、問題が発生することがあります。十分なスペースがないと新しい監査レコードを作成できないため、クライアントからデータにアクセスできず、アクセス要求が失敗します。ボリュームのスペースに関するこれらの問題について、トラブルシューティングを行って問題を解決する方法を確認しておく必要があります。

#### 関連コンセプト

[監査を有効にする際のアグリゲート スペースに関する考慮事項](#) (435ページ)

## イベント ログ ボリュームに関するスペースの問題のトラブルシューティング方法

イベント ログ ファイルを含むボリュームでスペースが不足すると、監査でログ レコードをログ ファイルに変換できなくなります。その結果、クライアント アクセスが失敗します。イベント ログ ボリュームのスペースに関する問題のトラブルシューティング方法を把握しておく必要があります。

- Storage Virtual Machine (SVM) 管理者およびクラスタ管理者は、ボリュームとアグリゲートの使用量と設定に関する情報を表示して、ボリュームでスペースが不足していないかを確認できます。
- イベント ログを含むボリュームでスペースが不足している場合、SVM管理者およびクラスタ管理者は、いくつかのイベント ログ ファイルを削除するかボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。

**注:** イベント ログ ボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを大きくする前に、アグリゲートのサイズを大きくする必要があります。アグリゲートのサイズを大きくすることができるのは、クラスタ管理者だけです。

- 監査設定を変更して、イベント ログ ファイルのデスティネーション パスを別のボリューム上のディレクトリに変更できます。

ボリュームに関する情報の表示とボリューム サイズの拡張の詳細については、『*clustered Data ONTAP 論理ストレージ管理ガイド*』を参照してください。

アグリゲートに関する情報の表示とアグリゲートの管理の詳細については、『*clustered Data ONTAP 物理ストレージ管理ガイド*』を参照してください。

#### 関連情報

[clustered Data ONTAP 8.3 論理ストレージ管理ガイド](#)

[clustered Data ONTAP 8.3 物理ストレージ管理ガイド](#)

## ステージング ボリュームに関するスペースの問題のトラブルシューティング方法(クラスタ管理者のみ)

Storage Virtual Machine (SVM) のステージング ファイルを含むボリュームのいずれかでスペースが不足すると、監査でログ レコードをステージング ファイルに書き込むことができなくなります。その結果、クライアント アクセスが失敗します。この問題のトラブルシューティングを行うには、ボリュームの使用量に関する情報を表示して、SVMで使用されているステージング ボリュームのいずれかがいっぱいになっていないかを確認する必要があります。

統合イベント ログ ファイルを含むボリュームに十分なスペースがあるにもかかわらず、スペース不足が原因でクライアント アクセスに失敗する場合は、ステージング ボリュームでスペースが不足している可能性があります。SVM管理者は、クラスタ管理者に問い合わせ、SVMのステージング ファイルを格納しているステージング ボリュームでスペースが不足していないかを確認する必要があります。ステージング ボリュームのスペース不足が原因で監査イベントを生成できない場合は、監査サブシステムによってEMSイベントが生成されます。「No space left on device」というメッセージが表示されます。ステージング ボリュームに関する情報を表示できるのは、クラスタ管理者だけです。SVM管理者はこの操作を行うことができません。

すべてのステージング ボリューム名はMDV\_aud\_で始まり、そのあとにステージング ボリュームが含まれているアグリゲートのUUIDが続きます。次に、管理SVM上にある4個のシステム ボリュームの例を示します。これらのボリュームは、クラスタ内のデータSVMに対してファイル サービスの監査設定が作成されたときに自動的に作成されたものです。

```
cluster1::> volume show -vserver cluster1
```

| Vserver  | Volume                                   | Aggregate | State  | Type | Size | Available | Used% |
|----------|------------------------------------------|-----------|--------|------|------|-----------|-------|
| cluster1 | MDV_aud_1d0131843d4811e296fc123478563412 | aggr0     | online | RW   | 2GB  | 1.90GB    | 5%    |
| cluster1 | MDV_aud_8be27f813d7311e296fc123478563412 | root_vs0  | online | RW   | 2GB  | 1.90GB    | 5%    |
| cluster1 | MDV_aud_9dc4ad503d7311e296fc123478563412 | aggr1     | online | RW   | 2GB  | 1.90GB    | 5%    |
| cluster1 | MDV_aud_a4b887ac3d7311e296fc123478563412 | aggr2     | online | RW   | 2GB  | 1.90GB    | 5%    |

4 entries were displayed.

ステージング ボリュームでスペースが不足している場合は、ボリュームのサイズを拡張することで、スペースに関する問題を解決できます。

**注:** ステージング ボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを拡張する前に、アグリゲートのサイズを拡張する必要があります。アグリゲートのサイズを拡張できるのは、クラスタ管理者だけです。SVM管理者はこの操作を行うことができません。

#### 関連情報

[clustered Data ONTAP 8.3 論理ストレージ管理ガイド](#)

[clustered Data ONTAP 8.3 物理ストレージ管理ガイド](#)



## FlexVolを備えたSVMでのFPolicyによるファイルの監視と管理

---

FPolicyは、FlexVolを備えたStorage Virtual Machine (SVM) でファイル アクセス イベントの監視と管理に使用されるファイル アクセス通知フレームワークです。

このフレームワークで生成される通知は、外部FPolicyサーバまたはData ONTAPに送信されます。FPolicyは、NFSおよびSMBを使用してアクセスされるファイルとディレクトリのイベント通知に対応しています。

注: Infinite Volumeを備えたSVMではFPolicyはサポートされません。

### FPolicyの仕組み

FPolicyの設定を計画して作成する前に、FPolicyの仕組みの基本について理解しておく必要があります。

### FPolicyソリューションの2つの要素とは

FPolicyソリューションは2つの要素で構成されます。Data ONTAP FPolicyフレームワークは、クラスタでのアクティビティを管理し、外部FPolicyサーバに通知を送信します。外部FPolicyサーバは、Data ONTAP FPolicyから送信された通知を処理します。

Data ONTAPのフレームワークでは、FPolicyの設定の作成と管理、ファイル イベントの監視、および外部FPolicyサーバへの通知の送信を行います。Data ONTAP FPolicyは、外部FPolicyサーバとStorage Virtual Machine (SVM) ノードの間の通信を可能にするインフラを提供します。

FPolicyフレームワークでは、外部FPolicyサーバへの接続を確立し、クライアント アクセスによって特定のファイルシステム イベントが発生した場合にFPolicyサーバに通知を送信します。外部FPolicyサーバでは、それらの通知を処理し、ノードに応答を送信します。通知の処理の結果として実行される処理は、アプリケーションごとに異なるほか、ノードと外部サーバの間の通信が非同期と同期のどちらであるかによっても異なります。

#### 関連コンセプト

[FPolicyの実装でクラスタコンポーネントが果たす役割](#) (466ページ)

[FPolicyと外部FPolicyサーバとの連携](#) (467ページ)

[SVMネームスペースにおけるFPolicyサービスの仕組み](#) (470ページ)

[FPolicyの設定タイプ](#) (470ページ)

[FPolicyの設定手順とは](#) (475ページ)

### 同期通知および非同期通知とは

FPolicyでは、FPolicyインターフェイスを介して外部FPolicyサーバに通知を送信します。通知の送信方法には同期モードと非同期モードの2種類があり、その通知モードによって、FPolicyサーバへの通知の送信後のData ONTAPでの処理が決まります。

#### 非同期通知

非同期通知では、FPolicyサーバからの応答を待たずにノードでの処理を継続できるため、システムの全体的なスループットが向上します。この種類の通知は、通知の評価結果に基づいてFPolicyサーバで処理を行う必要がないアプリケーションに適しています。たとえば、Storage Virtual Machine (SVM) 管理者がファイル アクセスのアクティビティを監視および監査する場合などに使用されます。

#### 同期通知

同期モードで実行するように設定した場合は、それぞれの通知についてFPolicyサーバからの確認応答を受け取ってからでないと、クライアントの処理を続行できません。この種類の通知は、通知の評価結果に基づいて処理を行う必要がある場合に適しています。たとえば、SVM管理者が要求を許可するかどうかを外部FPolicyサーバで指定された条件に基づいて判断する場合などに使用されます。

#### 関連コンセプト

[制御チャネルを使用したFPolicy通信](#) (467ページ)

[権限付きデータ アクセス チャネルを使用した同期通信](#) (467ページ)

#### 同期アプリケーションおよび非同期アプリケーション

FPolicyアプリケーションにはさまざまな用途があり、非同期と同期の両方に対応しています。

非同期アプリケーションとは、ファイルまたはフォルダへのアクセスやStorage Virtual Machine (SVM) のデータが外部FPolicyサーバによって変更されないアプリケーションです。次に例を示します。

- ファイル アクセスと監査ログ
- ストレージ リソースの管理

同期アプリケーションとは、データ アクセスやデータが外部FPolicyサーバによって変更されるアプリケーションです。次に例を示します。

- クォータの管理
- ファイル アクセス ブロックング
- ファイルのアーカイブと階層型ストレージ管理
- 暗号化サービスと復号化サービス
- 圧縮サービスと展開サービス

FPolicyのSDKを使用すると、その他のアプリケーションも識別および実装できます。

#### FPolicyの実装でクラスタ コンポーネントが果たす役割

FPolicyの実装においては、クラスタ、それに含まれるStorage Virtual Machine (SVM)、およびデータLIFのそれぞれに役割があります。

##### クラスタ

クラスタにあるFPolicyの管理フレームワークで、クラスタ内のすべてのFPolicyの設定に関する情報の保守と管理を行います。

##### SVM

FPolicyの設定はSVMレベルで定義されます。設定の範囲はSVMであり、SVMリソースにのみ適用されます。1つのSVMの設定で、別のSVMにあるデータに対するファイル アクセス要求を監視して通知を送信することはできません。

FPolicyの設定は管理SVMで定義できます。管理SVMで定義した設定は、すべてのSVMで表示および使用できます。

##### データLIF

FPolicyサーバへの接続は、FPolicyの設定が格納されたSVMに属するデータLIFを通じて行われます。これらの接続に使用されるデータLIFは、通常のクライアント アクセスに使用されるデータLIFと同じ方法でフェイルオーバーできます。

## FPolicyと外部FPolicyサーバとの連携

Storage Virtual Machine (SVM) で FPolicy を設定して有効にすると、SVM に含まれているすべてのノードで FPolicy が実行されるようになります。FPolicy は、外部 FPolicy サーバ (FPolicy サーバ) との接続の確立と維持、通知の処理、および FPolicy サーバ とやり取りする通知メッセージの管理を行います。

また、接続管理の一貫として、FPolicy は次の役割を果たします。

- ファイル通知が正しい LIF を通過して FPolicy サーバに送信されるようにする。
- ポリシーに複数の FPolicy サーバが関連付けられている場合に、FPolicy サーバへの通知の送信時にロード バランシングが行われるようにする。
- FPolicy サーバへの接続が切断されたときに再接続を試行する。
- 認証されたセッションを介して FPolicy サーバに通知を送信する。
- パススルー リードが有効な場合にクライアント要求を処理するために FPolicy サーバによって確立されたパススルー リード データ接続を管理する。

### 制御チャネルを使用した FPolicy 通信

FPolicy は、Storage Virtual Machine (SVM) に含まれている各ノードのデータ LIF から外部 FPolicy サーバへの制御チャネル接続を開始します。FPolicy は制御チャネルを使用してファイル通知を送信するため、FPolicy サーバでは、SVM のトポロジに基づいて複数の制御チャネル接続が認識される場合があります。

### 権限付きデータ アクセス チャネルを使用した同期通信

同期通信では、FPolicy サーバは、権限付きデータ アクセス パスを介して Storage Virtual Machine (SVM) 上のデータにアクセスします。権限付きパスを介したアクセスでは、FPolicy サーバにファイルシステム全体が公開されます。サーバは、データファイルにアクセスして情報を収集したり、ファイルのスキャン、ファイルの読み取り、またはファイルへの書き込みを行ったりできます。

外部 FPolicy サーバが権限付きデータ チャネルを介して SVM のルートからファイルシステム全体にアクセスできるため、権限付きデータ チャネル接続はセキュアである必要があります。

#### 関連コンセプト

[権限付きデータ アクセスのためのスーパー ユーザ クレデンシャルの付与とは](#) (468 ページ)

### 権限付きデータ アクセス チャネルでの FPolicy 接続クレデンシャルの使用

FPolicy サーバは、FPolicy の設定で保存されている特定の Windows ユーザ クレデンシャルを使用して、クラスタ ノードへの権限付きデータ アクセス接続を確立します。権限付きデータ アクセス チャネル接続の確立用としてサポートされているプロトコルは、SMB だけです。

FPolicy サーバで権限付きデータ アクセスが必要となる場合は、次の条件を満たす必要があります。

- クラスタで CIFS ライセンスが有効になっている。
- FPolicy サーバが FPolicy の設定で指定されたクレデンシャルで実行されている。

データ チャネル接続を確立するとき、FPolicy では、指定された Windows ユーザ名のクレデンシャルが使用されます。データ アクセスは、管理共有 ONTAP\_ADMIN\$ を介して確立されます。

## 権限付きデータ アクセスのためのスーパー ユーザ クレデンシャルの付与とは

Data ONTAPでは、FPolicy設定で設定されたIPアドレスとユーザ クレデンシャルを組み合わせ、FPolicyサーバにスーパーユーザ クレデンシャルを付与します。

スーパーユーザのステータスは、FPolicyサーバがデータにアクセスする際に次の権限を付与します。

- 権限チェックの省略  
ファイルやディレクトリに対するアクセスのチェックが省略されます。
- 特殊なロック権限  
ファイルにロックが設定されていても、読み取り、書き込み、変更が許可されます。バイト単位のロックが設定されたファイルをFPolicyサーバで取得した場合、ファイルに対する既存のロックがすぐに解除されます。
- すべてのFPolicyチェックの省略  
アクセス時にFPolicy通知が生成されません。

## FPolicyによるポリシーの処理方法

Storage Virtual Machine (SVM)には、優先度が異なる複数のFPolicyポリシーが割り当てられる場合があります。SVMで適切なFPolicyの設定を作成するには、FPolicyによるポリシーの処理方法を理解しておくことが重要です。

最初に各ファイル アクセス要求が評価され、このイベントを監視するポリシーが判別されます。このイベントが監視対象イベントの場合は、関連するポリシーとともにそのイベントに関する情報が評価を行うFPolicyに渡されます。各ポリシーは、割り当てられた優先度の順に評価されます。

ポリシーの設定時には、次の推奨事項を考慮してください。

- あるポリシーが常に他のポリシーの前に評価されるようにするには、そのポリシーの優先度を高く設定します。
- 監視対象イベントで要求されたファイル アクセス処理が正常に実行されることが、別のポリシーに対して評価されるファイル要求の前提条件となる場合は、最初のファイル処理の成功または失敗を制御するポリシーの優先度を高く設定します。  
たとえば、1つ目のポリシーでFPolicyのファイルのアーカイブおよびリストア機能を管理し、2つ目のポリシーでオンライン ファイルに対するファイル アクセス処理を管理する場合は、ファイルのリストアを管理するポリシーの優先度を高くして、2つ目のポリシーで管理される処理を許可する前にファイルがリストアされるようにする必要があります。
- ファイル アクセス処理に適用される可能性があるすべてのポリシーを評価するには、同期ポリシーの優先度を低く設定します。

既存のポリシーの優先度を変更するには、ポリシーのシーケンス番号を変更します。ただし、変更した優先度に基づいてポリシーを評価するには、変更したシーケンス番号のポリシーを無効にしてから再度有効にする必要があります。

### 関連コンセプト

[FPolicyポリシーの設定の計画](#) (488ページ)

## ノードと外部FPolicyサーバの間の通信プロセス

外部FPolicyの設定を適切に計画するには、ノードとFPolicyサーバの間の通信プロセスについて理解しておく必要があります。

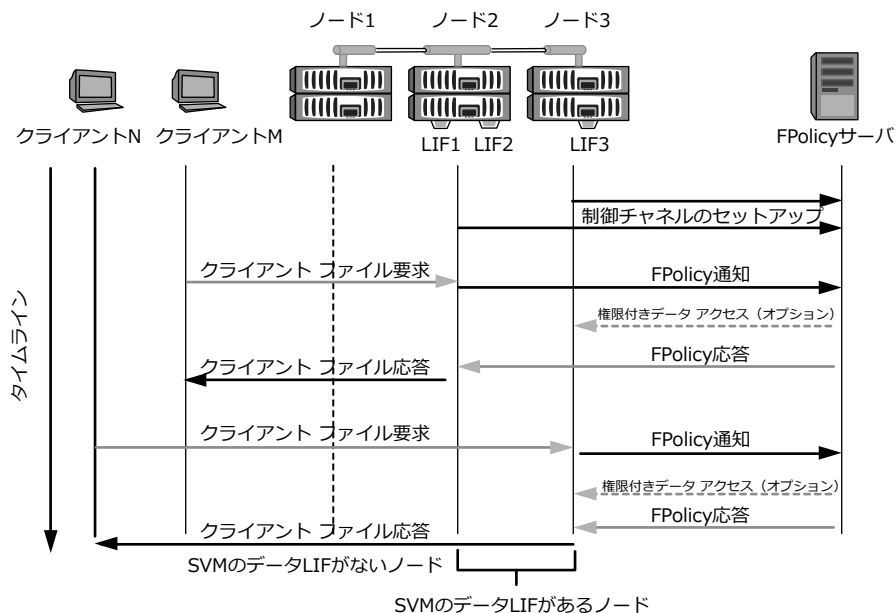
Storage Virtual Machine (SVM)に属しているすべてのノードは、TCP/IPを使用して外部FPolicyサーバへの接続を開始します。FPolicyサーバへの接続のセットアップには、ノードのデータLIFを使

用します。そのため、接続のセットアップは、ノードでSVMのデータLIFが稼働している場合しか実行できません。

ポリシーが有効になっている場合は、各ノードのそれぞれのFPolicyプロセスで、FPolicyサーバとの接続の確立が試行されます。これには、ポリシーの設定で指定されたFPolicy外部エンジンのIPアドレスとポートが使用されます。

この接続により、SVMに属する各ノードからFPolicyサーバへのデータLIFを介した制御チャンネルが確立されます。さらに、データLIFのアドレスとして同じノードでIPv4とIPv6の両方が設定されている場合、FPolicyはIPv4とIPv6の両方の接続の確立を試みます。そのため、SVMが複数のノードに展開されている場合、またはIPv4とIPv6の両方のアドレスが設定されている場合は、SVMでFPolicyポリシーを有効にしたあとに、クラスタからの複数の制御チャンネルのセットアップ要求に対応する必要があります。

たとえば、クラスタに3つのノード（ノード1、ノード2、およびノード3）があり、SVMのデータLIFがノード2とノード3だけで設定されている場合、データボリュームの配置に関係なく、制御チャンネルはノード2とノード3からのみ開始されます。ノード2にSVMに属するデータLIFが2つ（LIF1とLIF2）あり、最初にLIF1から接続を行うとします。LIF1で障害が発生した場合、FPolicyはLIF2から制御チャンネルの確立を試みます。



### LIFの移行またはフェイルオーバー時におけるFPolicyによる外部通信の実行方法

データLIFは、同じノードのデータポート、またはリモートノードのデータポートに移行できます。

データLIFがフェイルオーバーまたは移行されると、FPolicyサーバへの新しい制御チャンネル接続が確立されます。その後、FPolicyはSMBクライアントおよびNFSクライアントのタイムアウトした要求を再試行でき、新しい通知が外部FPolicyサーバに送信されます。ノードは、SMBとNFSの元のタイムアウトした要求に対するFPolicyサーバの応答を拒否します。

### ノードのフェイルオーバー時におけるFPolicyによる外部通信の実行方法

FPolicy通信に使用されるデータポートをホストするクラスタノードに障害が発生した場合は、FPolicyサーバとノードの間の接続が切断されます。

クラスタフェイルオーバーがFPolicyサーバに与える影響は、FPolicy通信に使用されるデータポートを別のアクティブノードに移行するようにLIFマネージャを設定することで軽減できます。移行が完了したら、新しいデータポートを使用して新しい接続が確立されます。



データ ポートを移行するようにLIFマネージャが設定されていない場合、FPolicyサーバは障害が発生したノードが稼働するまで待機する必要があります。ノードが稼働したら、新しいセッションIDを使用してそのノードから新しい接続が開始されます。

**注:** FPolicyサーバでは、切断された接続を検出するためにキープアライブ プロトコル メッセージが使用されます。セッションIDをパージするためのタイムアウトは、FPolicyの設定時に決定します。デフォルトのキープアライブのタイムアウトは2分です。

## SVMネームスペースにおけるFPolicyサービスの仕組み

Data ONTAPは、統合Storage Virtual Machine(SVM)ネームスペースを提供します。ジャンクションによってクラスタ全体のボリュームを統合し、単一の論理ファイルシステムを実現します。FPolicyサーバはネームスペーストポロジを認識し、ネームスペース全体にFPolicyサービスを提供します。

ネームスペースはSVMに固有で、SVM内に含まれています。したがって、ネームスペースはSVMコンテキストからのみ表示できます。ネームスペースには次のような特徴があります。

- 各SVMには単一のネームスペースが存在します。ネームスペースのルートはルート ボリュームで、ネームスペース内ではスラッシュ(/)として表されます。
- その他すべてのボリュームは、ルート(/)より下のジャンクション ポイントを保持します。
- ボリューム ジャンクションは、クライアントに対して透過的です。
- 単一のNFSエクスポートは、ネームスペース全体へのアクセスを提供できます。あるいは、エクスポート ポリシーで特定のボリュームをエクスポートできます。
- ネームスペース内のボリューム、ボリューム内のqtree、またはディレクトリにSMB共有を作成できます。
- ネームスペース アーキテクチャは柔軟です。  
一般的なネームスペース アーキテクチャの例を次に示します。
  - ルートからの分岐が1つだけのネームスペース
  - ルートからの分岐が複数あるネームスペース
  - ルートから分岐していないボリュームが複数あるネームスペース

### 関連コンセプト

[FlexVolを備えたSVMでネームスペースとボリューム ジャンクションがSMBアクセスに与える影響](#)(15ページ)

[NASネームスペースでのデータ ボリュームの作成と管理](#)(150ページ)

## FPolicyの設定タイプ

FPolicyの基本設定には2つのタイプがあります。一方の設定では、通知を受けて処理と対応を行う外部FPolicyサーバを使用します。もう一方の設定では外部FPolicyサーバを使用しません。代わりに、Data ONTAP内部のネイティブFPolicyサーバを使用して、拡張子に基づく単純なファイルブロッキングを行います。

### 外部FPolicyサーバ設定

FPolicyサーバに通知が送信され、そのサーバが要求をスクリーニングし、要求されたファイル処理をノードで許可するかどうかを決定するルールを適用します。同期ポリシーの場合、FPolicyサーバは、要求されたファイル処理を許可または拒否する応答をノードに送信します。

### ネイティブFPolicyサーバ設定

通知は内部的にスクリーニングされます。要求は、FPolicyスコープで設定されているファイル拡張子に基づいて許可または拒否されます。

#### 関連コンセプト

[FPolicyポリシーの設定の計画](#)(488ページ)

[FPolicyの設定の作成](#)(496ページ)

[FPolicyのパススルー リードによる階層型ストレージ管理のユーザビリティ向上](#)(472ページ)

### ネイティブFPolicyの設定を作成する場合

ネイティブFPolicyの設定では、Data ONTAPに組み込まれているFPolicyエンジンを使用して、ファイルの拡張子に基づいてファイル処理の監視とブロックングを行います。このソリューションは外部FPolicyサーバ(FPolicyサーバ)を必要としません。このネイティブ ファイル ブロックの設定は、このシンプルなソリューションが必要とされるあらゆる場合に適しています。

ネイティブ ファイル ブロックングを使用すると、設定した操作およびフィルタリング イベントに一致する任意のファイル処理を監視した後、特定の拡張子を持つファイルへのアクセスを拒否することができます。これはデフォルトの設定です。

この設定では、ファイルの拡張子に基づいてファイルへのアクセスをブロックすることができます。たとえば、.mp3拡張子を含むファイルをブロックするには、拡張子が.mp3のファイルをターゲットとする特定の処理に対する通知を送信するようにポリシーを設定します。このポリシーは、通知を生成する操作を求める.mp3ファイルに関する要求を拒否するように設定されます。

ネイティブFPolicy設定には次の条件が適用されます。

- FPolicyサーバベース ファイル スクリーニングでサポートされているフィルタとプロトコルのセットが、ネイティブ ファイル ブロックングでもサポートされます。
- ネイティブ ファイル ブロックングとFPolicyサーバベース ファイル スクリーニング アプリケーションは同時に設定できます。  
そうするために、Storage Virtual Machine (SVM)に2種類のFPolicyポリシーを設定できます。1つはネイティブ ファイル ブロックングのために設定したポリシーで、もう1つはFPolicyのサーバベースのファイルスクリーニングのために設定したポリシーです。
- ネイティブ ファイル ブロックング機能では、ファイルの内容でなく、拡張子のみに基づいてファイルがスクリーニングされます。
- シンボリック リンクの場合には、ネイティブ ファイル ブロックングは、ルート ファイルのファイル拡張子を使用します。

### 外部FPolicyサーバを使用する設定を作成する状況

ファイル拡張子に基づいて単にファイルをブロックする以上のことが求められるユース ケースの場合、通知の処理と管理に外部のFPolicyサーバを使用するようにFPolicyを設定することは、堅牢なソリューションとなります。

次のようなケースでは、外部のFPolicyサーバを使用するようにFPolicyを設定することができます。ファイル アクセス イベントの監視および記録、クォータ サービスの提供、単純なファイルの拡張子以外の基準にもとづくファイル ブロックング、階層型ストレージ管理アプリケーションを使用したデータ移行サービス、Storage Virtual Machine (SVM)内のデータのサブセットのみを監視する詳細なポリシー セットの提供など。

## FPolicyのパススルー リードによる階層型ストレージ管理のユーザビリティ向上

FPolicyのパススルー リードにより、Hierarchical Storage Management (HSM; 階層型ストレージ管理) のユーザビリティが向上します。パススルー リードを使用すると、移行されたオフライン ファイルに対する読み取りアクセスを (HSM サーバとして機能している) FPolicy サーバから提供できます。セカンダリ ストレージ システムからプライマリ ストレージ システムにファイルをリコールする必要はありません。

CIFS サーバ上にあるファイルに対して HSM を提供するように FPolicy サーバが構成されている場合、ポリシーベースのファイル移行が実行され、ファイルはセカンダリ ストレージ上にオフラインで格納され、プライマリ ストレージ上にはスタブ ファイルのみが残ります。スタブ ファイルはクライアントからは通常のファイルのように見えますが、実際には元のファイルと同じサイズのスパース ファイルです。スパース ファイルには CIFS のオフライン ビットが設定されており、セカンダリ ストレージに移行された実際のファイルを参照しています。

通常は、オフライン ファイルに対する読み取り要求を受け取ると、要求されたコンテンツはプライマリ ストレージにリコールされた (戻した) うえで、プライマリ ストレージ経由でアクセスされます。この方法はデータをプライマリ ストレージにリコールする必要があるため、いくつかのデメリットがあります。コンテンツをリコールしてから要求に応じるためにクライアント要求に対する遅延が大きくなる点や、ファイルをリコールするためのプライマリ ストレージでのスペース消費量の増加などです。

FPolicy のパススルー リードを使用すると、移行されたオフライン ファイルに対する読み取りアクセスを HSM サーバ (FPolicy サーバ) から提供できます。セカンダリ ストレージ システムからプライマリ ストレージ システムにファイルをリコールする必要はありません。プライマリ ストレージにファイルをリコールして戻す代わりに、セカンダリ ストレージが直接読み取り要求を処理できます。

パススルー リードには次のようなメリットがあり、ユーザビリティが向上します。

- 要求されたデータをリコールするための十分な領域がプライマリ ストレージになくても、読み取り要求を処理できます。
- スクリプトまたはバックアップ ソリューションで多数のオフライン ファイルへのアクセスが必要になった場合など、データのリコールが急増した場合でも容量やパフォーマンスを適切に管理できます。
- Snapshot コピー内のオフライン ファイルに対する読み取り要求を処理できます。  
Snapshot コピーは読み取り専用なので、スタブ ファイルが Snapshot コピー内にある場合、FPolicy サーバは元のファイルをリストアできません。パススルー リードを使用するとこの問題は解消されます。
- ポリシーを設定し、セカンダリ ストレージ上のファイルにアクセスすることで読み取り要求を処理するタイミング、およびオフライン ファイルをプライマリ ストレージにリコールするタイミングを制御できます。  
たとえば、所定の期間内にオフライン ファイルにアクセスできる回数を指定し、その回数を超えるとオフライン ファイルがプライマリ ストレージ上にリコールされるポリシーを HSM サーバ上に作成できます。このようなポリシーを設定することで、減多にアクセスされないファイルはリコールされなくなります。

### 関連コンセプト

[パススルー リードのアップグレードおよびリバートに関する考慮事項](#) (474 ページ)



## FPolicyパススルー リードが有効になっている場合の読み取り要求の処理方法

Storage Virtual Machine (SVM) およびFPolicyサーバ間の接続を最適な形で設定できるように、FPolicyパススルー リードが有効になっている場合の読み取り要求の処理方法を理解しておく必要があります。

FPolicyパススルー リードが有効になっている場合にSVMがオフライン ファイルに対する要求を受け取ると、FPolicyは標準の接続チャンネル経由でFPolicyサーバ(HSMサーバ)に通知を送信します。

通知を受け取ったFPolicyサーバは通知にあるファイル パスからデータを読み取り、要求されたデータをSVMとFPolicyとの間に確立されたパススルー リード権限のあるデータ接続を介してSVMに送信します。

データの送信後、FPolicyサーバは読み取り要求にALLOW (許可) またはDENY (拒否) で応答します。読み取り要求が許可されたか拒否されたかによって、Data ONTAPは要求された情報またはエラー メッセージをクライアントに送信します。

## FPolicyを設定するための要件、考慮事項、およびベストプラクティス

FlexVolを備えたStorage Virtual Machine (SVM) でFPolicyの設定を作成して設定する前に、FPolicyの設定に関する一定の要件、考慮事項、およびベストプラクティスについて確認しておく必要があります。

### 関連コンセプト

[パススルー リードのアップグレードおよびリバートに関する考慮事項](#) (474ページ)

[FPolicyポリシーの設定の計画](#) (488ページ)

[FPolicyの設定の作成](#) (496ページ)

## FPolicyの設定方法

FPolicy機能の設定には、コマンドライン インターフェイス (CLI) またはAPIを使用します。このガイドでは、CLIを使用して、クラスタのFPolicyの設定の作成、管理、および監視を行います。

## FPolicyを設定するための要件

Storage Virtual Machine (SVM) でFPolicyを設定して有効にする前に、一定の要件について確認しておく必要があります。

- クラスタ内のすべてのノードで、FPolicyがサポートされているバージョンのData ONTAPが実行されている必要があります。
- Data ONTAPの標準のFPolicyエンジンを使用しない場合は、外部FPolicyサーバ(FPolicyサーバ)をインストールしておく必要があります。
- FPolicyポリシーが有効になっているSVMのデータLIFからアクセスできるサーバに、FPolicyサーバがインストールされている必要があります。
- FPolicyポリシーの外部エンジンの設定で、FPolicyサーバのIPアドレスがプライマリ サーバまたはセカンダリ サーバとして設定されている必要があります。
- FPolicyサーバで権限付きデータ チャンネルを使用してデータにアクセスする場合は、次に示す追加の要件を満たしている必要があります。
  - クラスタでCIFSのライセンスが有効になっている必要があります。
  - 権限付きデータ アクセスはSMB接続を使用して実行されます。

- 権限付きデータ チャンネルを使用してファイルにアクセスするためのユーザ クレデンシャルが設定されている必要があります。
- FPolicyサーバがFPolicyの設定で指定されたクレデンシャルで実行されている。
- FPolicyサーバとの通信に使用されるすべてのデータLIFは、許可されているプロトコルの1つとしてcifsが設定されている必要があります。  
これには、パススルー リード接続で使用されるLIFも含まれます。

#### 関連コンセプト

[FPolicy外部エンジンの設定の計画](#)(476ページ)

[権限付きデータ アクセス チャンネルを使用した同期通信](#)(467ページ)

[権限付きデータ アクセス チャンネルでのFPolicy接続クレデンシャルの使用](#)(467ページ)

[権限付きデータ アクセスのためのスーパー ユーザ クレデンシャルの付与とは](#)(468ページ)

### FPolicyを設定する際のベストプラクティスと推奨事項

FlexVolを備えたStorage Virtual Machine(SVM)でFPolicyを設定するときは、FPolicyの設定によって監視のパフォーマンスが向上し、要件を満たす結果が得られるようにするため、設定に関するベストプラクティスと推奨事項を理解しておく必要があります。

- レイテンシを最小限に抑え、広帯域幅接続を確保するために、外部FPolicyサーバ(FPolicyサーバ)は広帯域幅接続が確保されたクラスタの近くに配置する必要があります。
- 特にポリシーが同期スクリーニング用に設定されている場合は、FPolicyサーバの通知処理の耐障害性と高可用性を確保するために、FPolicy外部エンジンを複数のFPolicyサーバで構成する必要があります。
- 設定を変更する前に、FPolicyポリシーを無効にすることを推奨します。  
たとえば、有効になっているポリシーに設定されたFPolicy外部エンジンのIPアドレスを追加または変更する場合は、まずポリシーを無効にしてください。
- SVMがクライアント要求に応答する際のレイテンシの原因となる可能性があるFPolicyサーバの過負荷状態を防ぐために、クラスタ ノードとFPolicyサーバの比率を最適化する必要があります。  
最適な比率は、FPolicyサーバが使用されているアプリケーションによって異なります。

#### 関連コンセプト

[FPolicy外部エンジンの設定の計画](#)(476ページ)

#### 関連タスク

[FPolicyポリシーの有効化と無効化](#)(502ページ)

### パススルー リードのアップグレードおよびリバートに関する考慮事項

パススルー リードをサポートしているData ONTAPリリースへのアップグレードまたはパススルー リードをサポートしていないリリースへのリバートを行う前に、アップグレードおよびリバートに関する考慮事項を把握しておく必要があります。

#### アップグレード

FPolicyパススルー リードをサポートしているData ONTAPのバージョンにすべてのノードをアップグレードしたあと、クラスタはパススルー リードを使用できるようになります。ただし、既存のFPolicy設定ではパススルー リードがデフォルトで無効になっています。既存のFPolicy設定でパススルー リードを使用するには、FPolicyポリシーを無効にして設定を変更したうえで、設定を再び有効にする必要があります。

## リバート

FPolicyをサポートしていないData ONTAPのバージョンにリバートする前に、以下の条件を満たす必要があります。

- パススルー リードを使用しているすべてのポリシーを無効にしたうえで、影響を受ける設定を変更してパススルー リードを使用しないようにする必要があります。
- クラスタ上のすべてのFPolicyポリシーを無効にして、クラスタのFPolicy機能を無効にする必要があります。

## FPolicyの設定手順とは

FPolicyでファイル アクセスを監視するには、FPolicyの設定を作成し、FPolicyサービスが必要なStorage Virtual Machine(SVM)で有効にする必要があります。

以下に、SVMでFPolicy設定をセットアップして有効にする手順を示します。

1. FPolicy外部エンジンを作成します。  
FPolicy外部エンジンでは、特定のFPolicyの設定に関連付けられた外部FPolicyサーバ（FPolicyサーバ）を識別します。内部の「標準」のFPolicyエンジンを使用してネイティブ ファイル ブロッキングの設定を作成する場合は、FPolicy外部エンジンを作成する必要はありません。
2. FPolicyイベントを作成します。  
FPolicyイベントでは、FPolicyポリシーで監視する対象を定義します。監視対象のプロトコルとファイル処理を指定し、一連のフィルタを含めることができます。それらのフィルタを使用して、監視対象イベントの中から、FPolicy外部エンジンで通知を送信する必要があるイベントだけを抽出できます。また、イベントでは、ポリシーでボリューム処理を監視するかどうかも指定します。
3. FPolicyポリシーを作成します。  
FPolicyポリシーでは、監視する必要がある一連のイベントと、指定のFPolicyサーバ（FPolicyサーバが設定されていない場合は標準のエンジン）に通知を送信する必要がある監視対象イベントを、適切な範囲で関連付けます。また、通知を受け取ったデータへの権限付きアクセスをFPolicyサーバに許可するかどうかも定義します。FPolicyサーバからデータにアクセスする必要がある場合は、権限付きアクセスが必要になります。権限付きアクセスが必要になる典型的なユースケースとしては、ファイル ブロッキング、クォータ管理、階層型ストレージ管理などがあります。さらに、ポリシーの設定でFPolicyサーバと内部の「標準」のFPolicyサーバのどちらを使用するかを指定します。  
スクリーニングを必須にするかどうかはポリシーで指定します。スクリーニングを必須にすると、すべてのFPolicyサーバが停止した場合や定義された時間内にFPolicyサーバからの応答を得られない場合に、ファイル アクセスが拒否されます。  
ポリシーはSVM単位で適用されます。1つのポリシーを複数のSVMに適用することはできません。ただし、ある特定のSVMに複数のFPolicyポリシーを含めることは可能で、範囲、イベント、外部サーバの設定を同じ組み合わせにすることも、それぞれで異なる組み合わせにすることもできます。
4. ポリシーの範囲を設定します。  
FPolicyスコープでは、ボリューム、共有、またはエクスポート ポリシーについて、ポリシーで監視するものと除外するものを指定します。また、ファイル拡張子についても、FPolicyの監視対象に含めるものと除外するものを指定します。  
**注:** 除外リストの方が対象リストよりも優先されます。
5. FPolicyポリシーを有効にします。  
ポリシーを有効にすると、制御チャネルおよび権限付きデータ チャネル（オプション）の接続が確立されます。SVMが属するノードのFPolicyプロセスで、ファイルおよびフォルダに対するア

クセスの監視が開始され、設定された条件に当てはまるイベントが見つかったら、FPolicyサーバ (FPolicyサーバが設定されていない場合は標準のエンジン) に通知が送信されます。

注: ポリシーでネイティブ ファイル ブロッキングを使用する場合は、外部エンジンは設定されず、関連付けられることはありません。

#### 関連コンセプト

[FPolicy構成の計画](#) (476ページ)

[FPolicyの設定の作成](#) (496ページ)

## FPolicy構成の計画

FPolicy構成を作成する前に、構成の各ステップの設定タスクを理解する必要があります。FPolicyの構成に必要な設定タスクを決定し、計画ワークシートに記入する必要があります。

次の設定タスクを計画する必要があります。

- FPolicy外部エンジンの作成
- FPolicyポリシー イベントの作成
- FPolicyポリシーの作成
- FPolicyポリシー スコープの作成

FPolicyはFlexVolを備えたStorage Virtual Machine (SVM) でサポートされます。Infinite Volumeを備えたSVMではFPolicyはサポートされません。

#### 関連コンセプト

[FPolicyの設定手順とは](#) (475ページ)

[FPolicyの設定の作成](#) (496ページ)

## FPolicy外部エンジンの設定の計画

FPolicy外部エンジンを設定する前に、外部エンジンを作成することの意味を理解し、使用可能な設定パラメータを理解する必要があります。この情報は、各パラメータに設定する値を決めるのに役立ちます。

#### FPolicy外部エンジンの作成時に定義される情報

外部エンジンの設定では、外部FPolicyサーバ (FPolicyサーバ) への接続を作成および管理するためにFPolicyが必要とする、次のような情報を定義します。

- Storage Virtual Machine (SVM) 名
- エンジンの名前
- FPolicyサーバへの接続時に使用するプライマリおよびセカンダリFPolicyサーバのIPアドレスとTCPポート番号
- エンジンのタイプが同期または非同期であるかどうか
- ノードとFPolicyサーバ間の接続を認証する方法  
相互SSL認証を設定することを選択した場合は、SSL証明書情報を提供するパラメータを設定する必要があります。
- 各種の高度な権限設定を使用して接続を管理する方法

これには、タイムアウト値、リトライ値、キープアライブ値、および最大要求値、送信および受信バッファ サイズ値、セッション タイムアウト値などを定義するパラメータが含まれます。

vserver fpolicy policy external-engine createコマンドは、FPolicy外部エンジンの作成に使用します。

### 外部エンジンの基本パラメータ

次に示すFPolicy基本設定パラメータの一覧は、設定を計画するのに役立ちます。

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | オプション                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <p><i>SVM</i></p> <p>この外部エンジンに関連付けるSVMの名前を指定します。</p> <p>各FPolicy構成は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。</p>                                                                                                                                                                                                                                                                                                      | <p>-vserver<br/>vserver_name</p>           |
| <p><i>エンジンの名前</i></p> <p>外部エンジンの設定に割り当てる名前を指定します。FPolicyポリシーを作成した場合、あとで外部エンジンの名前を指定する必要があります。こうすることで、外部エンジンがポリシーに関連付けられます。この名前に指定できる文字数は最大256文字です。</p> <p><b>注:</b> MetroClusterまたはSVMディザスタリカバリ設定で外部エンジンの名前を設定する場合、この名前は最大200文字にする必要があります。</p> <p>名前には、次のASCII文字を自由に組み合わせて使用できます。</p> <ul style="list-style-type: none"> <li>• a～z</li> <li>• A～Z</li> <li>• 0～9</li> <li>• 「_」、「-」、および「.」</li> </ul>                                                                    | <p>-engine-name<br/>engine_name</p>        |
| <p><i>プライマリFPolicyサーバ</i></p> <p>所定のFPolicyポリシーに関してノードが送信する通知の宛先となるプライマリFPolicyサーバを指定します。IPアドレスの値を指定します。複数の値を指定する場合は、カンマで区切ります。</p> <p>複数のプライマリ サーバのIPアドレスを指定した場合、SVMが参加しているすべてのノードに、ポリシーが有効にされたときに指定されたすべてのプライマリFPolicyサーバへの制御接続が作成されます。複数のプライマリFPolicyサーバを設定した場合、通知は各FPolicyサーバにラウンドロビン方式で送信されます。</p> <p>外部エンジンがMetroClusterまたはSVMディザスタリカバリ設定で使用されている場合は、ソース サイトでのFPolicyサーバのIPアドレスをプライマリ サーバとして指定する必要があります。デスティネーション サイトのFPolicyサーバのIPアドレスは、セカンダリ サーバとして指定してください。</p> | <p>-primary-servers<br/>IP_address,...</p> |
| <p><i>ポート番号</i></p> <p>FPolicyサービスのポート番号を指定します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>-port integer</p>                       |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | オプション                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>セカンダリFPolicyサーバ</b></p> <p>所定のFPolicyポリシーに関して、ファイル アクセス イベントの送信先となるセカンダリFPolicyサーバを指定します。IPアドレスの値を指定します。複数の値を指定する場合は、カンマで区切ります。</p> <p>セカンダリサーバは、いずれのプライマリにも到達できない場合にのみ使用されます。ポリシーが有効な場合にセカンダリ サーバへの接続が確立されますが、通知がセカンダリ サーバへ送信されるのは、いずれのプライマリ サーバへも着信できない場合のみです。複数のセカンダリ FPolicyサーバを設定した場合、通知は各FPolicyサーバにラウンドロビン方式で送信されます。</p>                                                                                                                                                                                            | <p>-secondary-servers<br/>IP_address,...</p>                                                                                                                                                |
| <p><b>外部エンジンのタイプ</b></p> <p>外部エンジンが同期モードで動作するか非同期モードで動作するかを指定します。デフォルトでは、FPolicyは同期モードで動作します。</p> <p><b>synchronous</b>に設定すると、ファイル要求処理によって通知はFPolicyサーバに送信されますが、その後FPolicyサーバから応答を受信するまでは、それ以降の通知は送信されません。この時点で、FPolicyサーバからの応答が要求されたアクションを許可するかどうかによって、要求フローが継続するか、または処理が否定されます。</p> <p><b>asynchronous</b>に設定すると、ファイル要求処理は、FPolicyサーバに通知を送信した後も処理を続行します。</p>                                                                                                                                                                   | <p>-extern-engine-type<br/>external_engine_type</p> <p>このパラメータには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>• <b>synchronous</b></li> <li>• <b>asynchronous</b></li> </ul> |
| <p><b>FPolicyサーバとの通信のためのSSLオプション</b></p> <p>FPolicyサーバとの通信のためのSSLオプションを指定します。これは必須パラメータです。次の情報に基づいて、いずれかのオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• <b>no-auth</b>に設定すると、認証処理は行われません。通信リンクはTCPを介して確立されます。</li> <li>• <b>server-auth</b>に設定すると、SVMはSSLサーバ認証を使用してFPolicyサーバを認証します。</li> <li>• <b>mutual-auth</b>に設定すると、SVMとFPolicyサーバ間で相互認証が行われ、SVMはFPolicyサーバを認証し、FPolicyサーバはSVMを認証します。<br/>相互SSL認証を設定することを選択した場合は、-certificate-common-name、-certificate-serial、および -certifcate-caの各パラメータを設定する必要があります。</li> </ul> | <p>-ssl-option {no-auth server-auth mutual-auth}</p>                                                                                                                                        |
| <p><b>証明書のFQDNまたはカスタム共通名</b></p> <p>SVMとFPolicyサーバ間のSSL認証が設定されている場合、認証に使用される証明書の名前を指定します。証明書の名前は、FQDNまたはカスタム共通名として指定できます。</p> <p><b>mutual-auth</b>を-ssl-optionパラメータに指定した場合は、-certificate-common-nameパラメータの値も指定する必要があります。</p>                                                                                                                                                                                                                                                                                                    | <p>-certificate-common-name text</p>                                                                                                                                                        |
| <p><b>証明書のシリアル番号</b></p> <p>SVMとFPolicyサーバ間のSSL認証が設定されている場合、認証に使用される証明書のシリアル番号を指定します。</p> <p><b>mutual-auth</b>を-ssl-optionパラメータに指定した場合は、-certificate-serialパラメータの値も指定する必要があります。</p>                                                                                                                                                                                                                                                                                                                                             | <p>-certificate-serial text</p>                                                                                                                                                             |

| 情報の種類                                                                                                                                                     | オプション                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>認証局</b><br>SVMとFPolicyサーバ間のSSL認証が設定されている場合、認証に使用される証明書のCA名を指定します。<br><b>mutual-auth</b> を-ssl-option/パラメータに指定した場合は、-certificate-caパラメータの値も指定する必要があります。 | -certificate-ca<br>text |

### 外部エンジンの詳細オプションについて

次に示すFPolicyの高度な設定パラメータの一覧を使用して、これらのパラメータを使用して設定をカスタマイズするかどうかを計画できます。これらのパラメータは、クラスターノードとFPolicyサーバ間の通信動作を変更するために使用します。

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                      | オプション                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| <b>タイムアウトによる要求のキャンセル</b><br>ノードがFPolicyサーバからの応答を待つ時間間隔を時間(h)、分(m)、または秒(s)で指定します。<br>タイムアウト間隔が経過すると、ノードはFPolicyサーバにキャンセル要求を送信します。その後、ノードから代替FPolicyサーバへ通知が送信されます。このタイムアウトは、応答しないFPolicyサーバを処理するのに役立ちます。これによりSMB / NFSクライアントの応答を向上させることができます。また、通知要求がパフォーマンスの低い、またはダウンしたFPolicyサーバから代替FPolicyサーバへ移されているため、タイムアウトによってリクエストをキャンセルすることは、システム リソースを解放するのに役立ちます。<br>指定できる値の範囲は、0～100です。値が0に設定されている場合、オプションは無効になり、キャンセルされた要求メッセージはFPolicyサーバには送信されません。デフォルトは20秒です。 | -reqs-cancel-timeout integer[h m s] |
| <b>タイムアウトによる要求の破棄</b><br>要求を破棄するためのタイムアウトを時間(h)、分(m)または秒(s)で指定します。<br>指定できる値の範囲は、0～200です。                                                                                                                                                                                                                                                                                                                                                                  | -reqs-abort-timeout integer[h m s]  |
| <b>ステータス要求の送信間隔</b><br>FPolicyサーバにステータス要求を送信する間隔を時間(h)、分(m)、または秒(s)で指定します。<br>指定できる値の範囲は、0～50です。値が0に設定されている場合、オプションは無効になり、ステータス要求メッセージはFPolicyサーバに送信されません。デフォルトは10sです。                                                                                                                                                                                                                                                                                     | -status-req-interval integer[h m s] |
| <b>FPolicyサーバの未処理要求の最大数</b><br>FPolicyサーバのキューに登録できる未処理要求の最大数を指定します。<br>指定できる値の範囲は、1～10000です。デフォルトは50です。                                                                                                                                                                                                                                                                                                                                                    | -max-server-reqs integer            |

| 情報の種類                                                                                                                                                                                                                                                                                          | オプション                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| <p><b>タイムアウトによる応答しないFPolicyサーバの切断</b></p> <p>FPolicyサーバとの接続を終了するまでの時間間隔を時間(h)、分(m)、または秒(s)で指定します。</p> <p>FPolicyサーバのキューに許容される最大要求数が含まれていて、タイムアウト期間内に応答がない場合のみ、タイムアウト期間が経過した後に接続を終了します。許容される最大要求数は、50(デフォルト)またはmax-server-reqs-パラメータで指定された数です。</p> <p>指定できる値の範囲は、1~100です。デフォルトは60sです。</p>       | <p>-server-progress-timeout <i>integer</i>[h m s]</p>                         |
| <p><b>FPolicyサーバへのキープアライブ メッセージの送信間隔</b></p> <p>FPolicyサーバにキープアライブ メッセージを送信する時間間隔を時間(h)、分(m)、または秒(s)で指定します。</p> <p>キープアライブ メッセージによってハーフオープン接続を検出します。</p> <p>指定できる値の範囲は、10~600です。値が0に設定されている場合、オプションは無効になり、キープアライブメッセージはFPolicyサーバには送信されません。デフォルトは120秒です。</p>                                   | <p>-keep-alive-interval-<i>integer</i>[h m s]</p>                             |
| <p><b>再接続の最大試行回数</b></p> <p>接続が切断された後、SVMがFPolicyサーバへの再接続を試行できる最大回数を指定します。</p> <p>指定できる値の範囲は、0~20です。デフォルトは5回です。</p>                                                                                                                                                                            | <p>-max-connection-retries <i>integer</i></p>                                 |
| <p><b>受信バッファ サイズ</b></p> <p>FPolicyサーバの接続ソケットの受信バッファ サイズを指定します。</p> <p>デフォルト値は256KBに設定されています。値が0に設定されている場合、受信バッファのサイズはシステムによって定義されている値に設定されます。</p> <p>たとえば、ソケットのデフォルト受信バッファ サイズが65,536バイトの場合、この調整可能な値を0に設定すると、ソケットのバッファ サイズは65,536バイトに設定されます。 デフォルト値以外の任意の値を使用して、受信バッファのサイズ(バイト単位)を設定できます。</p> | <p>-recv-buffer-size <i>integer</i></p>                                       |
| <p><b>送信バッファ サイズ</b></p> <p>FPolicyサーバの接続ソケットの送信バッファ サイズを指定します。</p> <p>デフォルト値は256KBに設定されています。値が0に設定されている場合、送信バッファのサイズはシステムによって定義されている値に設定されます。</p> <p>たとえば、ソケットのデフォルト送信バッファ サイズが65,536バイトの場合、この調整可能な値を0に設定すると、ソケットのバッファ サイズは65,536バイトに設定されます。 デフォルト値以外の任意の値を使用して、送信バッファのサイズ(バイト単位)を設定できます。</p> | <p>-send-buffer-size <i>integer</i></p>                                       |
| <p><b>再接続時にセッションIDを破棄するまでのタイムアウト</b></p> <p>再接続の試行時にFPolicyサーバに新しいセッションIDが送信されるまでの間隔を時間(h)、分(m)、または秒(s)で指定します。</p> <p>ストレージ コントローラとFPolicyサーバとの間の接続が終了して-session-timeoutの時間内に再接続が行われた場合は、古い通知に対する応答を送信できるように、古いセッションIDがFPolicyサーバに送信されます。</p> <p>デフォルト値は10秒に設定されています。</p>                      | <p>-session-timeout [<i>integer</i>h] [<i>integer</i>m] [<i>integer</i>s]</p> |



## 関連コンセプト

[SSL認証された接続を使用するためのFPolicy外部エンジンの設定に関する追加情報](#)(481ページ)

[MetroClusterおよびSVMのディザスタリカバリ構成でのクラスター対象FPolicy外部エンジンの制限事項](#)(482ページ)

## 関連情報

[clustered Data ONTAP 8.3 システム アドミニストレーション ガイド](#)

## SSL認証された接続を使用するためのFPolicy外部エンジンの設定に関する追加情報

FPolicyサーバへの接続時にSSLを使用するようにFPolicy外部エンジンを設定する場合は、いくつかの情報を把握しておく必要があります。

### SSLサーバ認証

SSLサーバ認証にFPolicy外部エンジンを設定する場合は、外部エンジンを作成する前に、FPolicyサーバ証明書に署名したCertificate Authority (CA; 認証局) のパブリック証明書をインストールする必要があります。

### 相互認証

Storage Virtual Machine (SVM) のデータLIFを外部FPolicyサーバに接続する際にSSL相互認証を使用するようにFPolicy外部エンジンを設定する場合は、外部エンジンを作成する前に、SVMの認証用のパブリック証明書およびキー ファイルのほかに、FPolicyサーバ証明書に署名したCAのパブリック証明書をインストールする必要があります。インストールした証明書を使用するFPolicyポリシーがある間、この証明書は削除しないでください。

FPolicyポリシーが外部のFPolicyサーバへの接続で相互認証に使用している間にこの証明書を削除すると、その証明書を使用するFPolicyは無効になり、再度有効にできなくなります。この状況では、同じ設定で証明書を新規作成してSVMにインストールしても、FPolicyポリシーを再度有効にすることはできません。

証明書が削除された場合は、新しい証明書をインストールして、その新しい証明書を使用するFPolicy外部エンジンを新たに作成したうえで、無効になっているFPolicyポリシーを変更して新しい外部エンジンを関連付ける必要があります。

### SSL用証明書のインストール方法

FPolicyサーバ証明書に署名したCAのパブリック証明書をインストールするには、`security certificate install` コマンドを使用し、`-type` パラメータに `client_ca` を指定します。SVMの認証に必要な秘密鍵とパブリック証明書をインストールするには、`security certificate install` コマンドを使用し、`-type` パラメータに `server` を指定します。

## 関連コンセプト

[FPolicy外部エンジンの設定の計画](#)(476ページ)

## IDが保持されない設定のSVMディザスタリカバリ関係では証明書がレプリケートされない

FPolicyサーバへの接続確立時のSSL認証に使用されるセキュリティ証明書は、IDが保持されない設定のSVMディザスタリカバリ デスティネーションにはレプリケートされません。SVM上のFPolicy外部エンジンの設定はレプリケートされますが、セキュリティ証明書はレプリケートされません。セキュリティ証明書はデスティネーションに手動でインストールする必要があります。

デスティネーションSVMにレプリケートされる設定内容は、SVMディザスタリカバリ関係の設定時に選択した `snapmirror create` コマンドの `-identity-preserve` オプションの値によって決まります。

-identity-preserveオプションをtrue(IDを保持)に設定すると、セキュリティ証明書の情報を含め、FPolicy 設定の詳細がすべてレプリケートされます。セキュリティ証明書をディザスタリカバリ デステーションにインストールする必要があるのは、このオプションをfalse(IDを保持しない)に設定した場合のみです。

### MetroClusterおよびSVMのディザスタリカバリ構成でのクラスタ対象FPolicy外部エンジンの制限事項

クラスタを対象としたFPolicy外部エンジンは、クラスタStorage Virtual Machine (SVM)を外部エンジンに割り当てて作成できます。ただし、クラスタ対象の外部エンジンをMetroClusterまたはSVMのディザスタリカバリ構成内に作成する場合は、SVMがFPolicyサーバとの外部通信で使用する認証方式を選択する際に特定の制限があります。

外部FPolicyサーバの作成時に選択できる認証オプションとして、認証なし、SSLサーバ認証、SSL相互認証の3つがあります。外部FPolicyサーバがデータSVMに割り当てられている場合は認証オプションを選択する際の制限事項はありませんが、クラスタ対象のFPolicy外部エンジンを作成する際には制限事項があります。

| 設定                                                                       | 許可されるかどうか |
|--------------------------------------------------------------------------|-----------|
| MetroClusterまたはSVMのディザスタリカバリと、認証なし(SSL未設定)のクラスタ対象FPolicy外部エンジン(SSL未設定)   | ○         |
| MetroClusterまたはSVMのディザスタリカバリと、SSLサーバ認証またはSSL相互認証を使用するクラスタ対象FPolicy外部エンジン | ×         |

- SSL認証を行うクラスタ対象FPolicy外部エンジンが存在し、MetroClusterまたはSVMのディザスタリカバリ構成を作成する場合は、認証を使用しないようにこの外部エンジンを変更するか、MetroClusterまたはSVMディザスタリカバリ構成を作成する前に外部エンジンを削除する必要があります。
- MetroClusterまたはSVMのディザスタリカバリ構成がすでに存在する場合は、SSL認証を行うクラスタ対象FPolicy外部エンジンを作成することはできません。

### 関連コンセプト

[FPolicy外部エンジンの設定の計画](#)(476ページ)

### FPolicy外部エンジンの設定ワークシートへの記入

このワークシートを使用して、FPolicy外部エンジンの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、外部エンジンを設定する前に、そのパラメータに使用する値を決定する必要があります。

### 外部エンジンの基本設定に関する情報

外部エンジンの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

| 情報の種類                             | 必須 | 含める | 値 |
|-----------------------------------|----|-----|---|
| Storage Virtual Machine (SVM) の名前 | ○  | ○   |   |
| エンジンの名前                           | ○  | ○   |   |
| プライマリFPolicyサーバ                   | ○  | ○   |   |
| ポート番号                             | ○  | ○   |   |
| セカンダリFPolicyサーバ                   | ×  |     |   |

| 情報の種類                        | 必須 | 含める | 値 |
|------------------------------|----|-----|---|
| 外部エンジンのタイプ                   | ×  |     |   |
| 外部FPolicyサーバとの通信のためのSSLオプション | ○  | ○   |   |
| 証明書のFQDNまたはカスタム共通名           | ×  |     |   |
| 証明書のシリアル番号                   | ×  |     |   |
| 認証局                          | ×  |     |   |

### 外部エンジンの詳細パラメータに関する情報

外部エンジンを詳細パラメータで設定するには、advanced権限モードで設定コマンドを入力する必要があります。

| 情報の種類                          | 必須 | 含める | 値 |
|--------------------------------|----|-----|---|
| タイムアウトによる要求のキャンセル              | ×  |     |   |
| タイムアウトによる要求の破棄                 | ×  |     |   |
| ステータス要求の送信間隔                   | ×  |     |   |
| FPolicyサーバの未処理要求の最大数           | ×  |     |   |
| タイムアウトによる応答しないFPolicyサーバの切断    | ×  |     |   |
| FPolicyサーバへのキープアライブ メッセージの送信間隔 | ×  |     |   |
| 再接続の最大試行回数                     | ×  |     |   |
| 受信バッファ サイズ                     | ×  |     |   |
| 送信バッファ サイズ                     | ×  |     |   |
| 再接続時にセッションIDを破棄するまでのタイムアウト     | ×  |     |   |

## FPolicyイベントの設定の計画

FPolicyイベントを構成する前に、FPolicyイベントを作成することの意味を理解する必要があります。イベントが監視するプロトコル、監視対象のイベント、使用するイベント フィルタを決定する必要があります。この情報は、設定する値を計画するのに役立ちます。

### FPolicyイベントを作成することの意味

FPolicyイベントを作成することは、どのファイル アクセス処理を監視するか、そしてどの監視対象 イベント通知を外部FPolicyサーバに送信するかを決定するために、FPolicyプロセスで必要とされる情報を定義することを意味します。FPolicyイベントの設定では、次の設定情報を定義します。

- Storage Virtual Machine (SVM) 名
- イベント名
- 監視するプロトコル

FPolicyは、SMB、NFSv3、およびNFSv4のファイル アクセス処理を監視できます。

- 監視するファイル処理  
すべてのファイル処理が、各プロトコルに対して有効とは限りません。
- 構成するファイル フィルタ  
ファイル処理とフィルタの特定の組み合わせだけが有効です。プロトコルごとに、サポートされる独自の組み合わせがあります。
- ボリュームのマウントおよびアンマウント処理を監視するかどうか

注: 3つのパラメータ(-protocol、-file-operations、-filters)の間には、依存関係があります。以下に、3つのパラメータの有効な組み合わせを示します。

- -protocolパラメータと-file-operationsパラメータを同時に指定する。
- 3つのパラメータをすべて同時に指定する。
- 3つのパラメータをどれも指定しない。

### FPolicyイベント構成に含まれるもの

次に示す使用可能なFPolicyイベント設定パラメータの一覧は、構成を計画するのに役立ちます。

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                          | オプション                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <p><i>SVM</i></p> <p>このFPolicyイベントに関連付けるSVMの名前を指定します。</p> <p>各FPolicy構成は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。</p>                                                                                                                                                                                                       | <p>-vserver<br/>vserver_name</p>  |
| <p><i>イベント名</i></p> <p>FPolicyイベントに割り当てる名前を指定します。FPolicyポリシーを作成する際には、イベント名を使用してFPolicyイベントをポリシーと関連付けます。</p> <p>この名前に指定できる文字数は最大256文字です。</p> <p>注: MetroClusterまたはSVMディザスタリカバリ設定でイベントを設定する場合、この名前は最大200文字にする必要があります。</p> <p>名前には、次のASCII文字を自由に組み合わせて使用できます。</p> <ul style="list-style-type: none"> <li>• a～z</li> <li>• A～Z</li> <li>• 0～9</li> <li>• 「_」、「-」、および「.」</li> </ul> | <p>-event-name<br/>event_name</p> |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | オプション                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| <p><b>プロトコル</b></p> <p>FPolicyイベントで設定するプロトコルを指定します。-protocolパラメータには、次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>• <b>cifs</b></li> <li>• <b>nfsv3</b></li> <li>• <b>nfsv4</b></li> </ul> <p>注: -protocolを指定する場合、-file-operationsパラメータに有効な値を指定する必要があります。プロトコルのバージョンによって、有効な値が異なることがあります。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>-protocol<br/><i>protocol</i></p>                   |
| <p><b>ファイル処理</b></p> <p>FPolicyイベントのファイル処理のリストを指定します。</p> <p>FPolicyイベントは、-protocolパラメータで指定されたプロトコルを使用して、すべてのクライアント要求についてこのパラメータに指定された処理をチェックします。複数のファイル処理を指定する場合は、各処理をカンマで区切ります。-file-operationsパラメータには、次の値を1個以上指定できます。</p> <ul style="list-style-type: none"> <li>• <b>close</b>: ファイル クローズ処理</li> <li>• <b>create</b>: ファイル作成処理</li> <li>• <b>create-dir</b>: ディレクトリ作成処理</li> <li>• <b>delete</b>: ファイル削除処理</li> <li>• <b>delete_dir</b>: ディレクトリ削除処理</li> <li>• <b>getattr</b>: 属性取得処理</li> <li>• <b>link</b>: リンク処理</li> <li>• <b>lookup</b>: 検索処理</li> <li>• <b>open</b>: ファイル オープン処理</li> <li>• <b>read</b>: ファイル読み取り処理</li> <li>• <b>write</b>: ファイル書き込み処理</li> <li>• <b>rename</b>: ファイル名変更処理</li> <li>• <b>rename_dir</b>: ディレクトリ名変更処理</li> <li>• <b>setattr</b>: 属性設定処理</li> <li>• <b>symlink</b>: シンボリック リンク処理</li> </ul> <p>注: -file-operationsパラメータを指定する場合、-protocolパラメータに有効なプロトコルを指定する必要があります。</p> | <p>-file-operations<br/><i>file_operations,...</i></p> |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | オプション                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <p><b>フィルタ</b></p> <p>指定したプロトコルにおける所定のファイル処理に対するフィルタのリストを指定します。-filtersパラメータ内の値は、クライアント要求をフィルタリングするために使用されます。パラメータには次の値を1個以上指定できます。</p> <ul style="list-style-type: none"> <li>• <b>monitor-ads</b>: 代替データ ストリームを要求するクライアント要求をフィルタリングします。</li> <li>• <b>close-with-modification</b>: 変更してクローズ処理を要求するクライアント要求をフィルタリングします。</li> <li>• <b>close-without-modification</b>: 変更せずにクローズ処理を要求するクライアント要求をフィルタリングします。</li> <li>• <b>first-read</b>: 初回の読み取りを要求するクライアント要求をフィルタリングします。</li> <li>• <b>first-write</b>: 初回の書き込みを要求するクライアント要求をフィルタリングします。</li> <li>• <b>offline-bit</b>: オフライン ビットの設定を求めるクライアント要求をフィルタリングします。<br/>このフィルタを設定すると、オフラインのファイルがアクセスされたときのみFPolicyサーバが通知を受信します。</li> <li>• <b>open-with-delete-intent</b>: 削除するためにファイルのオープン処理を要求するクライアント要求をフィルタリングします。<br/>このフィルタを設定すると、削除するためにファイルが開かれた場合のみFPolicyサーバが通知を受信します。これはFILE_DELETE_ON_CLOSEフラグを指定した場合に、ファイルシステムによって使用されます。</li> <li>• <b>open-with-write-intent</b>: 書き込むためにファイルのオープン処理を要求するクライアント要求をフィルタリングします。<br/>このフィルタを設定すると、書き込むためにファイルを開いた場合のみFPolicyサーバが通知を受信します。</li> <li>• <b>write-with-size-change</b>: 書き込みと同時にサイズの変更を求めるクライアント要求をフィルタリングします。</li> </ul> <p><b>注:</b> -filtersパラメータを指定する場合、-file-operationsと-protocolの各パラメータに有効な値を指定する必要があります。</p> | -filters <i>filter</i> , ...   |
| <p><b>ボリューム処理が必要かどうか</b></p> <p>ボリュームのマウントおよびアンマウント処理に対して監視が必要かどうかを指定します。デフォルトはfalseです。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | -volume-operation {true false} |

### FPolicyで監視可能なサポートされるファイル処理とフィルタの組み合わせリスト(SMB)

FPolicyイベントを設定する場合、SMBのファイル アクセスの監視では、サポートされるファイル処理とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、FPolicyによるSMBファイル アクセス イベントの監視で、サポートされるファイル処理とフィルタの組み合わせを示します。

| サポートされるファイル処理 | サポートされるフィルタ                                                                |
|---------------|----------------------------------------------------------------------------|
| close         | monitor-ads、offline-bit、close-with-modification、close-without-modification |
| create        | monitor-ads、offline-bit                                                    |
| create_dir    | 現在、このファイル処理をサポートするフィルタはありません。                                              |
| delete        | monitor-ads、offline-bit                                                    |
| delete_dir    | 現在、このファイル処理をサポートするフィルタはありません。                                              |
| getattr       | offline-bit                                                                |
| open          | monitor-ads、offline-bit、open-with-delete-intent、open-with-write-intent     |
| read          | monitor-ads、offline-bit、first-read                                         |
| write         | monitor-ads、offline-bit、first-write、write-with-size-change                 |
| rename        | monitor-ads、offline-bit                                                    |
| rename_dir    | 現在、このファイル処理をサポートするフィルタはありません。                                              |
| setattr       | monitor-ads、offline-bit                                                    |

#### FPolicyで監視可能なサポートされるファイル処理とフィルタの組み合わせリスト(NFSv3)

FPolicyイベントを設定する場合、NFSv3のファイル アクセス操作の監視では、サポートされるファイル処理とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、FPolicyによるNFSv3ファイル アクセス イベントの監視でサポートされるファイル処理とフィルタの組み合わせを示します。

| サポートされるファイル処理 | サポートされるフィルタ                        |
|---------------|------------------------------------|
| create        | offline-bit                        |
| create_dir    | 現在、このファイル処理をサポートするフィルタはありません。      |
| delete        | offline-bit                        |
| delete_dir    | 現在、このファイル処理をサポートするフィルタはありません。      |
| link          | offline-bit                        |
| lookup        | offline-bit                        |
| read          | offline-bit                        |
| write         | offline-bit、write-with-size-change |
| rename        | offline-bit                        |
| rename_dir    | 現在、このファイル処理をサポートするフィルタはありません。      |
| setattr       | offline-bit                        |
| symlink       | offline-bit                        |

#### FPolicyで監視可能なサポートされるファイル処理とフィルタの組み合わせリスト(NFSv4)

FPolicyイベントを設定する場合、NFSv4のファイル アクセス操作の監視では、サポートされるファイル処理とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、FPolicyによるNFSv4ファイル アクセス イベントの監視でサポートされるファイル処理とフィルタの組み合わせを示します。

| サポートされるファイル処理 | サポートされるフィルタ                        |
|---------------|------------------------------------|
| close         | offline-bit                        |
| create        | offline-bit                        |
| create_dir    | 現在、このファイル処理をサポートするフィルタはありません。      |
| delete        | offline-bit                        |
| delete_dir    | 現在、このファイル処理をサポートするフィルタはありません。      |
| getattr       | offline-bit                        |
| link          | offline-bit                        |
| lookup        | offline-bit                        |
| open          | offline-bit                        |
| read          | offline-bit                        |
| write         | offline-bit、write-with-size-change |
| rename        | offline-bit                        |
| rename_dir    | 現在、このファイル処理をサポートするフィルタはありません。      |
| setattr       | offline-bit                        |
| symlink       | offline-bit                        |

### FPolicyイベントの設定ワークシートへの記入

このワークシートを使用して、FPolicyイベントの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、FPolicyイベントを設定する前に、そのパラメータに使用する値を決定する必要があります。

FPolicyイベントの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

| 情報の種類                             | 必須                                  | 含める                   | 値 |
|-----------------------------------|-------------------------------------|-----------------------|---|
| Storage Virtual Machine (SVM) の名前 | <input type="radio"/>               | <input type="radio"/> |   |
| イベント名                             | <input type="radio"/>               | <input type="radio"/> |   |
| プロトコル                             | <input checked="" type="checkbox"/> |                       |   |
| ファイル処理                            | <input checked="" type="checkbox"/> |                       |   |
| フィルタ                              | <input checked="" type="checkbox"/> |                       |   |
| ボリューム処理が必要かどうか                    | <input checked="" type="checkbox"/> |                       |   |

### FPolicyポリシーの設定の計画

FPolicyポリシーを設定する前に、ポリシーの作成時に必要なパラメータや、特定のオプション パラメータを設定する理由を理解しておく必要があります。この情報は、各パラメータに設定する値を決めるのに役立ちます。

FPolicyポリシーの作成時にこのポリシーと関連付ける要素は次のとおりです。

- Storage Virtual Machine (SVM)
- 1つ以上のFPolicyイベント



- FPolicy外部エンジン

いくつかのオプション ポリシーの設定を行うこともできます。

### FPolicyポリシーの設定項目

FPolicyポリシーで使用できる必須パラメータとオプション パラメータを次に示します。これは設定について計画するときに役立ちます。

| 情報の種類                                                                                                                                                                                                                                                                                                        | オプション                              | 必須 | デフォルト値 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|--------|
| <b>SVM名</b><br>FPolicyスコープを作成するSVMの名前を指定します。                                                                                                                                                                                                                                                                 | -vserver<br><i>vserver_name</i>    | ○  | なし     |
| <b>ポリシー名</b><br>FPolicyポリシーの名前を指定します。<br>この名前に指定できる文字数は最大256文字です。<br><br><b>注:</b> MetroClusterまたはSVMディザスタリカバリ設定でポリシーを設定する場合、この名前は最大200文字にする必要があります。<br><br>名前には、次のASCII文字を自由に組み合わせることができます。 <ul style="list-style-type: none"> <li>• a～z</li> <li>• A～Z</li> <li>• 0～9</li> <li>• 「_」、「-」、および「.」</li> </ul> | -policy-name<br><i>policy_name</i> | ○  | なし     |
| <b>イベント名</b><br>FPolicyポリシーに関連付けるイベントをカンマで区切って指定します。 <ul style="list-style-type: none"> <li>• 1つのポリシーに複数のイベントに関連付けることができます。</li> <li>• イベントはプロトコルに固有です。</li> <li>• 1つのポリシーで複数のプロトコルのファイル アクセス イベントを監視するには、ポリシーで監視する各プロトコルのイベントを作成し、それらのイベントをポリシーに関連付けます。</li> <li>• 既存のイベントを指定する必要があります。</li> </ul>          | -events<br><i>event_name, ...</i>  | ○  | なし     |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                               | オプション                                               | 必須                                         | デフォルト値               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------------------------------------|----------------------|
| <p><b>外部エンジン名</b><br/>FPolicyポリシーに関連付ける外部エンジンの名前を指定します。</p> <ul style="list-style-type: none"> <li>外部エンジンには、ノードからFPolicyサーバに通知を送信するための必要な情報が格納されています。</li> <li>単純なファイル ブロッキングを行うためにData ONTAPの標準の外部エンジンを使用したり、より高度なファイル ブロッキングとファイル管理を行うために外部FPolicyサーバ(FPolicyサーバ)を使用するように設定された外部エンジンを使用したりするようにFPolicyを設定できます。</li> <li>標準の外部エンジンを使用する場合は、このパラメータの値を省略するか、<b>native</b>を指定します。</li> <li>FPolicyサーバを使用する場合は、外部エンジンの設定がすでに存在している必要があります。</li> </ul> | <p>-engine<br/><i>engine_name</i></p>               | <p>○(ポリシーで内部のData ONTAP標準エンジンを使用しない場合)</p> | <p><b>native</b></p> |
| <p><b>スクリーニングを必須にするかどうか</b><br/>ファイル アクセス スクリーニングを必須にするかどうかを指定します。</p> <ul style="list-style-type: none"> <li>必須スクリーニング設定は、プライマリサーバとセカンダリサーバがすべて停止した場合や、指定した時間内にFPolicyサーバからの応答を得られない場合に、ファイル アクセス イベントをどのように処理するかを決定します。</li> <li><b>true</b>に設定すると、ファイル アクセス イベントが拒否されます。</li> <li><b>false</b>に設定すると、ファイル アクセス イベントが許可されます。</li> </ul>                                                                                                           | <p>-is-mandatory<br/>{<b>true</b> <b>false</b>}</p> | <p>×</p>                                   | <p><b>true</b></p>   |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                            | オプション                                      | 必須                             | デフォルト値    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|--------------------------------|-----------|
| <p><b>権限付きアクセスを許可するかどうか</b></p> <p>権限付きデータ接続による監視対象のファイルやフォルダに対する権限付きアクセスをFPolicyサーバに許可するかどうかを指定します。</p> <p>設定されている場合、FPolicyサーバは権限付きデータ接続を使用して、監視対象データが格納されているSVMのルートにあるファイルにアクセスできます。</p> <p>権限付きデータアクセスの場合は、クラスターでCIMSがライセンスされているとともに、FPolicyサーバへの接続に使用されるすべてのデータLIFで、許可されているプロトコルの1つとしてcifsが設定されている必要があります。</p> <p>ポリシーで権限付きアクセスを許可する場合は、FPolicyサーバで権限付きアクセスに使用するアカウントのユーザ名も指定する必要があります。</p> | <p>-allow-privileged-access {yes no}</p>   | <p>×(パススルーリードが有効になっていない場合)</p> | <p>no</p> |
| <p><b>権限があるユーザの名前</b></p> <p>FPolicyサーバが権限付きデータアクセスで使用するアカウントのユーザ名を指定します。</p> <ul style="list-style-type: none"> <li>このパラメータの値は、「domain\username」の形式で指定します。</li> <li>-allow-privileged-accessがnoに設定されている場合、このパラメータの値は無視されます。</li> </ul>                                                                                                                                                          | <p>-privileged-user-name<br/>user_name</p> | <p>×(権限付きアクセスが有効になっていない場合)</p> | <p>なし</p> |

| 情報の種類                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | オプション                                                | 必須 | デフォルト値 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|----|--------|
| <p><b>パススルー リードを許可する</b></p> <p>FPolicyサーバによってセカンダリ ストレージ(オフライン ファイル)にアーカイブされているファイルに対して、FPolicyサーバがパススルー リード サービスを提供できるかどうかを指定します。</p> <ul style="list-style-type: none"> <li>パススルー リードは、オフライン ファイルのデータをプライマリ ストレージにリストアすることなく読み取る方法です。読み取り要求に応答する前にファイルをプライマリ ストレージにリコールする必要がないので、応答レイテンシが短縮されます。また、読み取り要求にこたえるためだけにリコールされるファイルによってストレージ領域を消費する必要がなくなるので、ストレージ効率が最適化されます。</li> <li>パススルー リードが有効になっている場合、FPolicyサーバはパススルー リード専用に使われている権限付きデータチャネル経由でファイルのデータを提供します。</li> <li>パススルー リードを設定する場合は、ポリシーでも権限付きアクセスを許可するように設定されている必要があります。</li> </ul> | <p>-is-passthrough-read-enabled<br/>{true false}</p> | ×  | false  |

#### 関連コンセプト

[FPolicyによるポリシーの処理方法](#)(468ページ)

[FPolicyを設定するための要件、考慮事項、およびベストプラクティス](#)(473ページ)

[FPolicyのパススルー リードによる階層型ストレージ管理のユーザビリティ向上](#)(472ページ)

[FPolicyポリシーでネイティブ エンジンを使用する場合のFPolicyスコープ設定の要件](#)(492ページ)

#### FPolicyポリシーでネイティブ エンジンを使用する場合のFPolicyスコープ設定の要件

標準のエンジンを使用するようにFPolicyポリシーを設定する場合には、ポリシーで設定されるFPolicyスコープの定義方法に関して特定の要件があります。

FPolicyスコープは、たとえば指定のボリュームまたは共有にFPolicyポリシーが適用されるかどうかといった、FPolicyポリシーが適用される範囲を定義します。FPolicyポリシーが適用されるスコープをさらに制限するパラメータが数多くあります。その1つが-is-file-extension-check-on-directories-enabledで、ディレクトリ上でファイル拡張子をチェックするかどうかを指定します。デフォルト値はfalseで、ディレクトリ上のファイル拡張子はチェックされません。

標準のエンジンを使用するFPolicyポリシーが共有またはボリュームで有効になっていて、ポリシーのスコープで-is-file-extension-check-on-directories-enabledパラメータがfalseに設定されている場合、ディレクトリへのアクセスは拒否されます。この設定では、ディレクトリでファイル拡張子がチェックされないため、このポリシーのスコープ下にあるすべてのディレクトリ処理が拒否されます。

標準のエンジンを使用している場合にディレクトリ アクセスを成功させるには、スコープの作成時に `-is-file-extension-check-on-directories-enabled` パラメータを `true` に設定する必要があります。

このパラメータが `true` に設定されている場合、ディレクトリ処理に対して拡張子チェックが実行され、FPolicyスコープ設定に含まれている / 含まれていない拡張子に基づいてアクセスを許可するか拒否するかが決定されます。

## 関連コンセプト

[FPolicyの設定タイプ](#) (470ページ)

[ネイティブFPolicyの設定を作成する場合](#) (471ページ)

[FPolicyスコープの設定の計画](#) (493ページ)

## FPolicyポリシーのワークシートへの記入

このワークシートを使用して、FPolicyポリシー設定プロセスに必要な値を記録することができます。FPolicyポリシー設定の各パラメータについて、値を指定するかどうかを記録した後、指定するパラメータの値を記録する必要があります。

| 情報の種類                             | 含める                   | 値 |
|-----------------------------------|-----------------------|---|
| Storage Virtual Machine (SVM) の名前 | <input type="radio"/> |   |
| ポリシー名                             | <input type="radio"/> |   |
| イベント名                             | <input type="radio"/> |   |
| 外部エンジン名                           |                       |   |
| スクリーニングを必須にするかどうか                 |                       |   |
| 権限付きアクセスを許可するかどうか                 |                       |   |
| 権限があるユーザの名前                       |                       |   |
| パススルー リードが有効かどうか                  |                       |   |

## FPolicyスコープの設定の計画

FPolicyスコープを設定する前に、スコープを作成することの意味を理解する必要があります。また、スコープの構成要素を理解する必要があります。さらに、スコープの優先規則についても理解する必要があります。この情報は、設定する値を計画するのに役立ちます。

### FPolicyスコープを作成することの意味

FPolicyスコープを作成することは、FPolicyポリシーの適用範囲を定義することを意味します。Storage Virtual Machine (SVM) は基本の適用範囲です。FPolicyポリシーのスコープを作成する場合、スコープが適用されるFPolicyポリシーを定義する必要があり、さらにスコープを適用するSVMを指定する必要があります。

指定したSVM内でさらにスコープを制限するためのパラメータが数多くあります。スコープに含めるものを指定したり、スコープから除外するものを指定することでスコープを制限することができます。有効なポリシーにスコープを適用すると、ポリシー イベントのチェックがこのコマンドで定義されたスコープに適用されます。

「include」オプションの指定と一致するファイル アクセス イベントが見つかった場合に、通知が生成されます。「exclude」オプションの指定と一致するファイル アクセス イベントが見つかった場合は、通知は生成されません。

FPolicyスコープの構成では、次の設定情報を定義します。

- SVM名
- ポリシー名
- 監視対象に含めるまたは監視対象から除外する共有
- 監視対象に含めるまたは監視対象から除外するエクスポート ポリシー
- 監視対象に含めるまたは監視対象から除外するボリューム
- 監視対象に含めるまたは監視対象から除外するファイル拡張子
- ディレクトリ オブジェクトのファイル拡張子を監視対象にするかどうか

**注:** クラスタのFPolicyポリシーのスコープには、特に考慮すべき事項があります。クラスタのFPolicyポリシーは、クラスタ管理者が管理SVM用に作成するポリシーです。クラスタ管理者がそのクラスタのFPolicyポリシーのスコープも作成する場合、SVM管理者はそのポリシーのスコープを作成することはできません。ただし、クラスタ管理者がクラスタのFPolicyポリシーのスコープを作成しない場合は、すべてのSVM管理者がそのクラスタ ポリシーのスコープを作成することができます。SVM管理者がそのクラスタのFPolicyポリシーのスコープを作成した場合、クラスタ管理者はそれ以降、その同じクラスタ ポリシーのクラスタスコープを作成することはできません。これは、クラスタ管理者が同じクラスタ ポリシーのスコープを上書きできないためです。

### スコープの優先規則について

スコープの構成では、次の優先規則が適用されます。

- 共有を `-shares-to-include` パラメータに指定し、その共有の親ボリュームを `-volumes-to-exclude` パラメータに指定した場合は、`-volumes-to-exclude` が `-shares-to-include` よりも優先されます。
- エクスポート ポリシーを `-export-policies-to-include` パラメータに指定し、そのエクスポート ポリシーの親ボリュームを `-volumes-to-exclude` パラメータに指定した場合、`-volumes-to-exclude` が `-export-policies-to-include` よりも優先されます。
- 管理者は、`-file-extensions-to-include` と `-file-extensions-to-exclude` の両方のパラメータを指定できます。  
`-file-extensions-to-exclude` パラメータは、`-file-extensions-to-include` パラメータの前にチェックされます。

### FPolicyスコープの構成要素

次に示す使用可能なFPolicyスコープの設定パラメータの一覧は、構成を計画するのに役立ちます。

**注:** スコープに対して含めるまたは除外する共有の種類、エクスポート ポリシー、ボリューム、およびファイル拡張子を設定する場合、`include` と `exclude` パラメータに正規表現を使用することができます、「`?`」や「`*`」などのワイルドカード文字も使用できます。

| 情報の種類                                                                                                                                                                 | オプション                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| <p><i>SVM</i></p> <p>FPolicyスコープを作成するSVMの名前を指定します。</p> <p>各FPolicy設定は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。</p> | <p><code>-vserver</code><br/><code>vserver_name</code></p> |

| 情報の種類                                                                                                                                                                                                                                                                                               | オプション                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>ポリシー名</b><br>スコープをアタッチするFPolicyポリシーの名前を指定します。FPolicyポリシーが既に存在している必要があります。                                                                                                                                                                                                                        | -policy-name<br><i>policy_name</i>                            |
| <b>共有を含める</b><br>カンマで区切って複数の共有を指定し、FPolicyポリシーの監視対象となるスコープに含めます。                                                                                                                                                                                                                                    | -shares-to-include<br><i>share_name, ...</i>                  |
| <b>共有を除外する</b><br>カンマで区切って複数の共有を指定し、FPolicyポリシーの監視対象となるスコープから除外します。                                                                                                                                                                                                                                 | -shares-to-exclude<br><i>share_name, ...</i>                  |
| <b>ボリュームを含める</b><br>カンマで区切って複数のボリュームを指定し、FPolicyポリシーの監視対象となるスコープに含めます。                                                                                                                                                                                                                              | -volumes-to-include<br><i>volume_name, ...</i>                |
| <b>ボリュームを除外する</b><br>カンマで区切って複数のボリュームを指定し、FPolicyポリシーの監視対象となるスコープから除外します。                                                                                                                                                                                                                           | -volumes-to-exclude<br><i>volume_name, ...</i>                |
| <b>エクスポート ポリシーを含める</b><br>カンマで区切って複数のエクスポート ポリシーを指定し、FPolicyポリシーの監視対象となるスコープに含めます。                                                                                                                                                                                                                  | -export-policies-to-include<br><i>export_policy_name, ...</i> |
| <b>エクスポート ポリシーを除外する</b><br>カンマで区切って複数のボリュームを指定し、FPolicyポリシーの監視対象となるスコープから除外します。                                                                                                                                                                                                                     | -export-policies-to-exclude<br><i>export_policy_name, ...</i> |
| <b>ファイル拡張子を含める</b><br>カンマで区切って複数のファイル拡張子を指定し、FPolicyポリシーの監視対象となるスコープに含めます。                                                                                                                                                                                                                          | -file-extensions-to-include<br><i>file_extensions, ...</i>    |
| <b>ファイル拡張子を除外する</b><br>カンマで区切って複数のファイル拡張子を指定し、FPolicyポリシーの監視対象となるスコープから除外します。                                                                                                                                                                                                                       | -file-extensions-to-exclude<br><i>file_extensions, ...</i>    |
| <b>ディレクトリのファイル拡張子の監視を有効にする</b><br>ファイル名の拡張子の監視をディレクトリ オブジェクトに適用するかどうかを指定します。このパラメータをtrueに設定すると、通常のファイルと同じく、ディレクトリ オブジェクトの拡張子も監視対象となります。このパラメータをfalseに設定すると、ディレクトリ名の拡張子は照合されず、その名前の拡張子が一致しない場合でも、ディレクトリに関する通知は行われます。<br>スコープの割り当て先となるFPolicyポリシーが標準のエンジンを使用するように設定されている場合は、このパラメータをtrueに設定する必要があります。 | -is-file-extension-check-on-directories-enabled {true false}  |

## 関連コンセプト

[FPolicyポリシーでネイティブ エンジンを使用する場合のFPolicyスコープ設定の要件](#) (492ページ)

## FPolicyスコープのワークシートへの記入

このワークシートを使用して、FPolicyスコープの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、FPolicyスコープを設定する前に、そのパラメータに使用する値を決定する必要があります。

FPolicyスコープの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

| 情報の種類                             | 必須 | 含める | 値 |
|-----------------------------------|----|-----|---|
| Storage Virtual Machine (SVM) の名前 | ○  | ○   |   |
| ポリシー名                             | ○  | ○   |   |
| 共有を含める                            | ×  |     |   |
| 共有を除外する                           | ×  |     |   |
| ボリュームを含める                         | ×  |     |   |
| ボリュームを除外する                        | ×  |     |   |
| エクスポート ポリシーを含める                   | ×  |     |   |
| エクスポート ポリシーを除外する                  | ×  |     |   |
| ファイル拡張子を含める                       | ×  |     |   |
| ファイル拡張子を除外する                      | ×  |     |   |
| ディレクトリのファイル拡張子の監視を有効にする           | ×  |     |   |

## FPolicyの設定の作成

FPolicyの設定を作成するためには、いくつかの手順を実行する必要があります。まず、設定を計画する必要があります。次に、FPolicy外部エンジン、FPolicyイベント、およびFPolicyポリシーを作成します。そのあと、FPolicyスコープを作成し、FPolicyポリシーに関連付けてから、FPolicyポリシーを有効にします。

FPolicyはFlexVolを備えたStorage Virtual Machine (SVM) でサポートされます。Infinite Volumeを備えたSVMではFPolicyはサポートされません。

### 手順

#### 1. FPolicy外部エンジンの作成 (497ページ)

FPolicyの設定を作成するための最初の手順は、外部エンジンの作成です。外部エンジンは、FPolicyで外部FPolicyサーバへの接続を確立および管理する方法を定義します。内部のData ONTAPエンジン(標準の外部エンジン)を単純なファイル ブロッキングに使用している設定の場合は、FPolicy外部エンジンを別途設定する必要がないので、この手順の実行は不要です。

#### 2. FPolicyポリシー イベントの作成 (498ページ)

FPolicyポリシーの設定を作成する手順の一環として、Fpolicyイベントを作成する必要があります。FPolicyポリシーを作成するときに、このイベントをポリシーに関連付けます。イベントは、監視するプロトコルと、監視およびフィルタリングするファイル アクセス イベントを定義します。

#### 3. FPolicyポリシーの作成 (499ページ)



FPolicyポリシーを作成する際には、外部エンジンと1つ以上のイベントをこのポリシーに関連付けます。このポリシーでは、必須のスクリーニングが要求されるかどうか、FPolicyサーバに Storage Virtual Machine (SVM) 上のデータへの権限付きアクセスが許可されているかどうか、オフライン ファイルのパススルー リードが有効かどうかも指定します。

#### 4. FPolicyスコープの作成 (500ページ)

FPolicyポリシーを作成したあと、FPolicyスコープを作成する必要があります。スコープを作成するときに、スコープをFPolicyポリシーに関連付けます。スコープは、FPolicyポリシーを適用する範囲を定義します。共有、エクスポート ポリシー、ボリューム、およびファイル拡張子に基づいて、対象とするファイルまたは除外するファイルを指定できます。

#### 5. FPolicyポリシーの有効化 (501ページ)

FPolicyポリシーの設定が完了したら、FPolicyポリシーを有効にします。ポリシーを有効にするとその優先度が設定され、そのポリシーのファイル アクセスの監視が開始されます。

### 関連コンセプト

[FPolicyの設定手順とは](#) (475ページ)

[FPolicy構成の計画](#) (476ページ)

[FPolicyを設定するための要件、考慮事項、およびベストプラクティス](#) (473ページ)

[FPolicyの設定に関する情報の表示](#) (503ページ)

[FPolicyのパススルー リードによる階層型ストレージ管理のユーザビリティ向上](#) (472ページ)

## FPolicy外部エンジンの作成

FPolicyの設定を作成するための最初の手順は、外部エンジンの作成です。外部エンジンは、FPolicyで外部FPolicyサーバへの接続を確立および管理する方法を定義します。内部のData ONTAPエンジン (標準の外部エンジン) を単純なファイル ブロッキングに使用している設定の場合は、FPolicy外部エンジンを別途設定する必要がないので、この手順の実行は不要です。

### 開始する前に

外部エンジン ワークシートを完成させる必要があります。

### タスク概要

外部エンジンがMetroCluster構成で使用されている場合は、ソース サイトでFPolicyサーバのIPアドレスをプライマリ サーバとして指定する必要があります。デスティネーション サイトのFPolicyサーバのIPアドレスは、セカンダリ サーバとして指定してください。

### 手順

1. `vserver fpolicy policy external-engine create` コマンドを使用してFPolicy外部エンジンを作成します。

#### 例

次のコマンドは、Storage Virtual Machine (SVM) `vs1.example.com` 上に外部エンジンを作成します。FPolicyサーバとの外部通信に認証は一切必要ありません。

```
vserver fpolicy policy external-engine create -vserver-name
vs1.example.com -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3
-port 6789 -ssl-option no-auth
```

2. `vserver fpolicy policy external-engine show` コマンドを使用してFPolicy外部エンジンの設定を確認します。

**例**

次のコマンドは、SVM vs1.example.comで設定されているすべての外部エンジンに関する情報を表示します。

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

| Vserver         | Engine  | Primary Servers       | Secondary Servers | Port | External Engine Type |
|-----------------|---------|-----------------------|-------------------|------|----------------------|
| vs1.example.com | engine1 | 10.1.1.2,<br>10.1.1.3 | -                 | 6789 | synchronous          |

次のコマンドは、SVM vs1.example.com上の「engine1」という外部エンジンに関する詳細情報を表示します。

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -  
engine-name engine1
```

```

Vserver: vs1.example.com
Engine: engine1
Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
Port Number of FPolicy Service: 6789
Secondary FPolicy Servers: -
External Engine Type: synchronous
SSL Option for External Communication: no-auth
FQDN or Custom Common Name: -
Serial Number of Certificate: -
Certificate Authority: -

```

## FPolicyポリシー イベントの作成

FPolicyポリシーの設定を作成する手順の一環として、Fpolicyイベントを作成する必要があります。FPolicyポリシーを作成するときに、このイベントをポリシーに関連付けます。イベントは、監視するプロトコルと、監視およびフィルタリングするファイル アクセス イベントを定義します。

**開始する前に**

FPolicyイベント ワークシートを完成させる必要があります。

**手順**

1. vserver fpolicy policy event createコマンドを使用してFPolicyイベントを作成します。

**例**

```
vserver fpolicy policy event create -vserver-name vs1.example.com -  
event-name event1 -protocol cifs -file-operations open,close,read,write
```

2. vserver fpolicy policy event showコマンドを使用して、FPolicyイベント設定を確認します。

**例**

```
vserver fpolicy policy event show -vserver vs1.example.com
```

| Vserver         | Event Name | Protocols | File Operations             | Filters | Is Volume Operation |
|-----------------|------------|-----------|-----------------------------|---------|---------------------|
| vs1.example.com | event1     | cifs      | open, close,<br>read, write | -       | false               |

## FPolicyポリシーの作成

FPolicyポリシーを作成する際には、外部エンジンと1つ以上のイベントをこのポリシーに関連付けます。このポリシーでは、必須のスクリーニングが要求されるかどうか、FPolicyサーバにStorage Virtual Machine (SVM) 上のデータへの権限付きアクセスが許可されているかどうか、オフラインファイルのパススルー リードが有効かどうかも指定します。

### 開始する前に

- FPolicyポリシー ワークシートを完成させる必要があります。
- FPolicyサーバを使用するようにポリシーを設定する場合は、外部エンジンが存在している必要があります。
- FPolicyポリシーに関連付けるFPolicyイベントが少なくとも1つは存在している必要があります。
- 権限付きデータ アクセスを設定する場合は、SVM上にCIFSサーバが存在している必要があります

### 手順

1. FPolicyポリシーを作成します。

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name  
policy_name -engine engine_name -events event_name,... [-is-mandatory  
{true|false}] [-allow-privileged-access {yes|no}] [-privileged-user-name  
domain\user_name] [-is-passthrough-read-enabled {true|false}]
```

- FPolicyポリシーには1つ以上のイベントを追加できます。
- デフォルトでは、必須のスクリーニングが有効になっています。
- `-allow-privileged-access` パラメータを `yes` に設定して権限付きアクセスを許可する場合は、権限付きアクセスを許可するユーザ名も設定する必要があります。
- `-is-passthrough-read-enabled` パラメータを `true` に設定してパススルー リードを設定する場合は、権限付きデータ アクセスの設定も行う必要があります。

### 例

次のコマンドは、「event1」というイベントと「engine1」という外部エンジンが関連付けられた「policy1」というポリシーを作成します。このポリシーではデフォルト値をポリシー設定に使用しています。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name  
policy1 -events event1 -engine engine1
```

次のコマンドは、「event2」というイベントと「engine2」という外部エンジンが関連付けられた「policy2」というポリシーを作成します。このポリシーは、指定されたユーザ名を使用して権限付きアクセスを使用するように設定されています。また、パススルー リードが有効になっています。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name  
policy2 -events event2 -engine engine2 -allow-privileged-access yes  
-privileged-user-name example\archive_acct -is-passthrough-read-enabled  
true
```

次のコマンドは、「event3」というイベントが関連付けられた「native1」というポリシーを作成します。このポリシーでは、標準のエンジンを使用し、デフォルト値をポリシー設定に使用しています。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name  
native1 -events event3 -engine native
```

2. `vserver fpolicy policy show`コマンドを使用してFPolicyポリシーの設定を確認します。

#### 例

次のコマンドは、次の情報を含む、設定された3つのFpolicyポリシーに関する情報を表示します。

- ポリシーに関連付けられているSVM
- ポリシーに関連付けられている外部エンジン
- ポリシーに関連付けられているイベント
- 必須のスクリーニングが要求されているかどうか
- 権限付きアクセスが要求されているかどうか

`vserver fpolicy policy show`

| Vserver         | Policy Name | Events | Engine  | Is Mandatory | Privileged Access |
|-----------------|-------------|--------|---------|--------------|-------------------|
| vs1.example.com | policy1     | event1 | engine1 | true         | no                |
| vs1.example.com | policy2     | event2 | engine2 | true         | yes               |
| vs1.example.com | native1     | event3 | native  | true         | no                |

## FPolicyスコープの作成

FPolicyポリシーを作成したあと、FPolicyスコープを作成する必要があります。スコープを作成するときに、スコープをFPolicyポリシーに関連付けます。スコープは、FPolicyポリシーを適用する範囲を定義します。共有、エクスポート ポリシー、ボリューム、およびファイル拡張子に基づいて、対象とするファイルまたは除外するファイルを指定できます。

#### 開始する前に

FPolicyスコープ ワークシートを完成させる必要があります。FPolicyポリシーには、関連付けられた外部エンジンが存在する必要がある(外部FPolicyサーバを使用するよう設定されている場合)、少なくとも1つのFPolicyイベントが関連付けられている必要があります。

#### 手順

1. `vserver fpolicy policy scope create`コマンドを使用してFPolicyスコープを作成します。

#### 例

`vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1,datavol2`

2. `vserver fpolicy scope show`コマンドを使用してFPolicyスコープの設定を確認します。

#### 例

`vserver fpolicy policy scope show -vserver vs1.example.com -instance`

```

Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -

```

```
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

## FPolicyポリシーの有効化

FPolicyポリシーの設定が完了したら、FPolicyポリシーを有効にします。ポリシーを有効にするとその優先度が設定され、そのポリシーのファイル アクセスの監視が開始されます。

### 開始する前に

FPolicyポリシーには、関連付けられた外部エンジンが存在する必要がある（外部FPolicyサーバを使用するように設定されている場合）、少なくとも1つのFPolicyイベントが関連付けられている必要があります。FPolicyポリシー スコープが存在し、FPolicyポリシーに割り当てられている必要があります。

### タスク概要

Storage Virtual Machine (SVM) で複数のポリシーを有効にし、複数のポリシーを同じファイル アクセス イベントに登録している場合は、優先度が使用されます。標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てたシーケンス番号に関係なく、その他のエンジンのポリシーよりも優先度が高くなります。

**注:** 管理SVMではポリシーを有効にできません。

### 手順

1. `vserver fpolicy enable` コマンドを使用して、FPolicyポリシーを有効にします。

#### 例

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name
policy1 -sequence-number 1
```

2. `vserver fpolicy show` コマンドを使用して、FPolicyポリシーが有効になっていることを確認します。

#### 例

```
vserver fpolicy show -vserver vs1.example.com
```

| Vserver         | Policy Name | Sequence Number | Status | Engine  |
|-----------------|-------------|-----------------|--------|---------|
| vs1.example.com | policy1     | 1               | on     | engine1 |

## FPolicyの設定の変更

FPolicyの設定を変更するには、設定の各構成要素を変更します。外部エンジン、FPolicyイベント、FPolicyスコープ、FPolicyポリシーを変更できます。FPolicyポリシーを有効または無効にすることもできます。FPolicyポリシーを無効にすると、そのポリシーのファイル監視が中断されます。

設定を変更する前に、FPolicyポリシーを無効にすることをお勧めします。

### 関連コンセプト

[FPolicyの設定の作成](#) (496ページ)

[FPolicyサーバの接続の管理](#) (505ページ)

## FPolicy設定の変更用コマンド

FPolicyの外部エンジン、イベント、スコープ、およびポリシーを変更できます。

| 変更する項目 | 使用するコマンド                                                   |
|--------|------------------------------------------------------------|
| 外部エンジン | <code>vserver fpolicy policy external-engine modify</code> |
| イベント   | <code>vserver fpolicy policy event modify</code>           |
| スコープ   | <code>vserver fpolicy policy scope modify</code>           |
| ポリシー   | <code>vserver fpolicy policy modify</code>                 |

詳細については、各コマンドのマニュアル ページを参照してください。

### 関連参照情報

[FPolicyの設定に関する情報を表示するコマンド](#)(503ページ)

## FPolicyポリシーの有効化と無効化

設定の完了後に、FPolicyポリシーを有効にできます。ポリシーを有効にするとその優先度が設定され、そのポリシーのファイル アクセスの監視が開始されます。そのポリシーのファイル アクセスの監視を停止するには、FPolicyポリシーを無効にします。

### 開始する前に

FPolicyポリシーを有効にする前に、FPolicyの設定が完了している必要があります。

### タスク概要

- Storage Virtual Machine(SVM)で複数のポリシーを有効にし、複数のポリシーを同じファイル アクセス イベントに登録している場合は、優先度が使用されます。
- 標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てたシーケンス番号に関係なく、その他のエンジンのポリシーよりも優先度が高くなります。
- FPolicyポリシーの優先度を変更する場合は、ポリシーを無効にしてから、新しいシーケンス番号を使用して再度有効にする必要があります。

### 手順

- 適切な処理を実行します。

| 状況                | 入力するコマンド                                                                                                                              |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| FPolicyポリシーを有効にする | <code>vserver fpolicy enable -vserver-name <i>vserver_name</i> -policy-name <i>policy_name</i> -sequence-number <i>integer</i></code> |
| FPolicyポリシーを無効にする | <code>vserver fpolicy disable -vserver-name <i>vserver_name</i> -policy-name <i>policy_name</i></code>                                |

### 関連タスク

[FPolicyポリシーのステータスに関する情報の表示](#)(504ページ)

[有効なFPolicyポリシーに関する情報の表示](#)(505ページ)

## FPolicyの設定に関する情報の表示

FPolicyの設定に関する情報を表示して、各Storage Virtual Machine (SVM) の設定が正しいかどうかを確認したり、FPolicyポリシーの設定が有効になっているかどうかを確認したりできます。FPolicy外部エンジン、FPolicyイベント、FPolicyスコープ、およびFPolicyポリシーに関する情報を表示できます。

### 関連コンセプト

[FPolicyの設定の作成](#) (496ページ)

[FPolicyの設定の変更](#) (501ページ)

### showコマンドの仕組み

showコマンドの仕組みについて理解しておく、FPolicyの設定に関する情報を表示する際に役立ちます。

パラメータを追加せずにshowコマンドを実行すると、情報は要約形式で表示されます。さらに、各showコマンドには、2つのオプション パラメータ-instanceおよび-fieldsが用意されています。これらのパラメータは同時には指定できません。

showコマンドで-instanceパラメータを使用すると、コマンド出力には詳細情報がリスト形式で表示されます。場合によっては、詳細出力は長くなり、不要な情報が含まれる可能性があります。-fields fieldname[, fieldname...]パラメータを使用すると、指定したフィールドの情報のみが表示されるように出力をカスタマイズできます。指定できるフィールドを確認するには、?を-fieldsパラメータのあとに入力します。

**注:** showコマンドに-fieldsパラメータを指定した場合の出力には、要求したフィールドに関係する他の関連フィールドや必須フィールドが表示されることがあります。

各showコマンドには、その出力をフィルタして、コマンド出力に表示される情報の範囲を限定することができる、1つ以上のオプション パラメータが用意されています。コマンドで使用できるオプションパラメータを確認するには、?をshowコマンドのあとに入力します。

showコマンドでは、UNIX形式のパターンおよびワイルドカードがサポートされており、コマンド パラメータ引数の複数の値を照合できます。たとえば、値を指定するときに、ワイルドカード演算子(\*)、NOT演算子(!)、OR演算子(|)、範囲演算子(整数...整数)、less-than演算子(<)、greater-than演算子(>)、less-than-or-equal-to演算子(<=)、greater-than-or-equal-to演算子(>=)を使用できます。

UNIX形式のパターンおよびワイルドカードの使用の詳細については、『*clustered Data ONTAPシステム アドミニストレーション ガイド (SVM管理)*』の「Data ONTAPコマンドライン インターフェイスの使用」を参照してください。

### FPolicyの設定に関する情報を表示するコマンド

fpolicy showコマンドを使用すると、FPolicy外部エンジン、イベント、スコープ、およびポリシーに関する情報など、FPolicyの設定に関する情報を表示できます。

| FPolicyに関する情報の表示 | 使用するコマンド                                    |
|------------------|---------------------------------------------|
| 外部エンジン           | vserver fpolicy policy external-engine show |
| イベント             | vserver fpolicy policy event show           |
| スコープ             | vserver fpolicy policy scope show           |

| FPolicyに関する情報の表示 | 使用するコマンド                                 |
|------------------|------------------------------------------|
| ポリシー             | <code>vserver fpolicy policy show</code> |

詳細については、各コマンドのマニュアル ページを参照してください。

## FPolicyポリシーのステータスに関する情報の表示

FPolicyポリシーのステータスに関する情報を表示して、ポリシーが有効になっているかどうか、使用するように設定されている外部エンジン、ポリシーのシーケンス番号、およびFPolicyポリシーが関連付けられているStorage Virtual Machine (SVM)を確認できます。

### タスク概要

パラメータを何も指定しない場合、このコマンドでは次の情報が表示されます。

- SVM名
- ポリシー名
- ポリシーのシーケンス番号
- ポリシーのステータス

クラスタまたは特定のSVMで設定されているFPolicyポリシーのステータスに関する情報の表示に加え、コマンド パラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

-instanceパラメータを指定して、一覧にあるポリシーに関する詳細情報を表示できます。また、-fieldsパラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます。-fields ?を指定すると、使用できるフィールドを確認できます。

### 手順

1. 適切なコマンドを使用して、FPolicyポリシーのステータスに関する情報をフィルタリングして表示します。

| ステータス情報を表示するポリシー    | 入力するコマンド                                                          |
|---------------------|-------------------------------------------------------------------|
| クラスタのポリシー           | <code>vserver fpolicy show</code>                                 |
| 指定したステータスのポリシー      | <code>vserver fpolicy show -status {on off}</code>                |
| 指定したSVMのポリシー        | <code>vserver fpolicy show -vserver <i>vserver_name</i></code>    |
| 指定したポリシー名のポリシー      | <code>vserver fpolicy show -policy-name <i>policy_name</i></code> |
| 指定した外部エンジンを使用するポリシー | <code>vserver fpolicy show -engine <i>engine_name</i></code>      |

次の例では、クラスタのFPolicyポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show
```

| Vserver         | Policy Name    | Sequence Number | Status | Engine |
|-----------------|----------------|-----------------|--------|--------|
| -----           | -----          | -----           | -----  | -----  |
| FPolicy         | cserver_policy | -               | off    | eng1   |
| vs1.example.com | v1p1           | -               | off    | eng2   |



|                 |                |   |     |        |
|-----------------|----------------|---|-----|--------|
| vs1.example.com | v1p2           | - | off | native |
| vs1.example.com | v1p3           | - | off | native |
| vs1.example.com | cserver_policy | - | off | eng1   |
| vs2.example.com | v1p1           | 3 | on  | native |
| vs2.example.com | v1p2           | 1 | on  | eng3   |
| vs2.example.com | cserver_policy | 2 | on  | eng1   |

## 有効なFPolicyポリシーに関する情報の表示

有効なFPolicyポリシーに関する情報を表示して、使用するよう設定されている外部エンジン、ポリシーの優先順位、およびFPolicyポリシーが関連付けられているStorage Virtual Machine (SVM)を確認できます。

### タスク概要

パラメータを何も指定しない場合、このコマンドでは次の情報が表示されます。

- SVM名
- ポリシー名
- ポリシーの優先度

コマンド パラメータを使用して、指定した条件によってコマンドの出力をフィルタリングすることができます。

### 手順

1. 適切なコマンドを使用して、有効なFPolicyポリシーに関する情報を表示します。

| 情報を表示する有効なポリシー   | 入力するコマンド                                                            |
|------------------|---------------------------------------------------------------------|
| クラスタのポリシー        | <b>vserver fpolicy show-enabled</b>                                 |
| 指定したSVMのポリシー     | <b>vserver fpolicy show-enabled -vserver <i>vserver_name</i></b>    |
| 指定したポリシー名のポリシー   | <b>vserver fpolicy show-enabled -policy-name <i>policy_name</i></b> |
| 指定したシーケンス番号のポリシー | <b>vserver fpolicy show-enabled -priority <i>integer</i></b>        |

次の例では、クラスタの有効なFPolicyポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show-enabled
Vserver          Policy Name      Priority
-----
vs1.example.com  pol_native       native
vs1.example.com  pol_native2      native
vs1.example.com  pol1             2
vs1.example.com  pol2             4
```

## FPolicyサーバの接続の管理

FPolicyサーバ接続の管理では、外部FPolicyサーバへの接続、外部FPolicyサーバからの切断、接続および接続ステータスに関する情報の確認などができます。

## 関連コンセプト

[FPolicyソリューションの2つの要素とは](#)(465ページ)

[同期通知および非同期通知とは](#)(465ページ)

[FPolicyと外部FPolicyサーバとの連携](#)(467ページ)

[ノードと外部FPolicyサーバの間の通信プロセス](#)(468ページ)

## 外部FPolicyサーバへの接続

接続がすでに終了している場合、ファイル処理を有効にするために、外部FPolicyサーバへの手動での接続が必要になることがあります。接続は、サーバタイムアウトになった場合や特定のエラーによって終了します。または、管理者が接続を手動で終了することもあります。

### タスク概要

致命的なエラーが発生した場合、FPolicyサーバへの接続が終了することがあります。致命的なエラーの原因となった問題を解決したあと、FPolicyサーバに手動で再接続する必要があります。

### 手順

1. `vserver fpolicy engine-connect`コマンドを使用して、外部FPolicyサーバに接続します。  
コマンドの詳細については、[マニュアル ページ](#)を参照してください。
2. `vserver fpolicy show-engine`コマンドを使用して、外部FPolicyサーバに接続していることを確認します。  
コマンドの詳細については、[マニュアル ページ](#)を参照してください。

## 外部FPolicyサーバからの切断

外部FPolicyサーバからの手動での切断が必要になることがあります。これは、FPolicyサーバで通知要求の処理に関する問題が発生した場合や、FPolicyサーバでメンテナンスを実施する必要がある場合に役立つことがあります。

### 手順

1. `vserver fpolicy engine-disconnect`コマンドを使用して、外部FPolicyサーバから切断します。  
コマンドの詳細については、[マニュアル ページ](#)を参照してください。
2. `vserver fpolicy show-engine`コマンドを使用して、外部FPolicyサーバから切断されたことを確認します。  
コマンドの詳細については、[マニュアル ページ](#)を参照してください。

## 外部FPolicyサーバへの接続に関する情報の表示

クラスタまたは指定したStorage Virtual Machine(SVM)の外部FPolicyサーバ(FPolicyサーバ)への接続に関するステータス情報を表示できます。この情報は、接続されているFPolicyサーバを確認するのに役立ちます。

### タスク概要

パラメータを何も指定しない場合、このコマンドでは次の情報が表示されます。

- SVM名
- ノード名
- FPolicyポリシー名

- FPolicyサーバのIPアドレス
- FPolicyサーバのステータス
- FPolicyサーバのタイプ

クラスタまたは特定のSVMのFPolicy接続に関する情報の表示に加え、コマンド パラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

-instanceパラメータを指定して、一覧にあるポリシーに関する詳細情報を表示できます。また、-fieldsパラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます。?を -fieldsパラメータのあとに入力すると、使用できるフィールドを確認できます。

## 手順

1. 適切なコマンドを使用して、ノードとFPolicyサーバの間の接続ステータスに関する情報をフィルタリングして表示します。

| 接続ステータス情報を表示するFPolicyサーバ | コマンド                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 指定のもの                    | <code>vserver fpolicy show-engine -server <i>IP_address</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 指定したSVMのもの               | <code>vserver fpolicy show-engine -vserver <i>vserver_name</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 指定したポリシーに関連付けられているもの     | <code>vserver fpolicy show-engine -policy-name <i>policy_name</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 指定したサーバステータスのもの          | <code>vserver fpolicy show-engine -server-status <i>status</i></code><br>サーバのステータスとしては、次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• <code>connected</code></li> <li>• <code>disconnected</code></li> <li>• <code>connecting</code></li> <li>• <code>disconnecting</code></li> </ul>                                                                                                                                                                                                                                                                                           |
| 指定したタイプのもの               | <code>vserver fpolicy show-engine -server-type <i>type</i></code><br>FPolicyサーバのタイプとしては、次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• <code>primary</code></li> <li>• <code>secondary</code></li> </ul>                                                                                                                                                                                                                                                                                                                                                                        |
| 指定の理由によって切断されたもの         | <code>vserver fpolicy show-engine -disconnect-reason <i>text</i></code><br>切断の理由はさまざまです。一般的な切断の理由は次のとおりです。 <ul style="list-style-type: none"> <li>• <code>Disconnect command received from CLI.</code></li> <li>• <code>Error encountered while parsing notification response from FPolicy server.</code></li> <li>• <code>FPolicy Handshake failed.</code></li> <li>• <code>SSL handshake failed.</code></li> <li>• <code>TCP Connection to FPolicy server failed.</code></li> <li>• <code>The screen response message received from the FPolicy server is not valid.</code></li> </ul> |

次の例は、SVM vs1.example.com上のFPolicyサーバへの外部エンジン接続に関する情報を表示したものです。

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy
Vserver      Policy      Node      Server      Server-
status      Server-
type
-----
vs1.example.com policy1    node1      10.1.1.2    connected  primary
vs1.example.com policy1    node1      10.1.1.3    disconnected primary
vs1.example.com policy1    node2      10.1.1.2    connected  primary
vs1.example.com policy1    node2      10.1.1.3    disconnected primary
```

次の例は、接続されているFPolicyサーバに関する情報のみを表示したものです。

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node      vserver      policy-name server
-----
node1     vs1.example.com policy1      10.1.1.2
node2     vs1.example.com policy1      10.1.1.2
```

## 関連コンセプト

[FPolicyと外部FPolicyサーバとの連携](#)(467ページ)

[ノードと外部FPolicyサーバの間の通信プロセス](#)(468ページ)

## 関連タスク

[FPolicyパススルー リード接続のステータスに関する情報の表示](#)(508ページ)

## FPolicyパススルー リード接続のステータスに関する情報の表示

クラスタまたは指定したStorage Virtual Machine(SVM)の外部FPolicyサーバ(FPolicyサーバ)へのFPolicyパススルー リード接続のステータスに関する情報を表示できます。この情報は、どのFPolicyサーバにパススルー リード データ接続があり、どのFPolicyサーバでパススルー リード データ接続が切断されているかを確認するのに役立ちます。

### タスク概要

パラメータを何も指定しない場合、このコマンドでは次の情報が表示されます。

- SVM名
- FPolicyポリシー名
- ノード名
- FPolicyサーバのIPアドレス
- FPolicyパススルー リード接続のステータス

クラスタまたは特定のSVMのFPolicy接続に関する情報の表示に加え、コマンド パラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

-instanceパラメータを指定して、一覧にあるポリシーに関する詳細情報を表示できます。また、-fieldsパラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます。?を-fieldsパラメータのあとに入力すると、使用できるフィールドを確認できます。

## 手順

- 適切なコマンドを使用して、ノードとFPolicyサーバの間の接続ステータスに関する情報をフィルタリングして表示します。

| 表示する接続ステータス情報                      | 入力するコマンド                                                                                                                                                                                                                                                            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クラスタのFPolicyパススルーリード接続ステータス        | <code>vserver fpolicy show-passthrough-read-connection</code>                                                                                                                                                                                                       |
| 指定したSVMのFPolicyパススルーリード接続ステータス     | <code>vserver fpolicy show-passthrough-read-connection -vserver <i>vserver_name</i></code>                                                                                                                                                                          |
| 指定したポリシーのFPolicyパススルーリード接続ステータス    | <code>vserver fpolicy show-passthrough-read-connection -policy-name <i>policy_name</i></code>                                                                                                                                                                       |
| 指定したポリシーの詳細なFPolicyパススルーリード接続ステータス | <code>vserver fpolicy show-passthrough-read-connection -policy-name <i>policy_name</i> -instance</code>                                                                                                                                                             |
| 指定したステータスのFPolicyパススルーリード接続ステータス   | <code>vserver fpolicy show-passthrough-read-connection -policy-name <i>policy_name</i> -server-status <i>status</i></code><br>サーバのステータスとしては、次のいずれかを指定できます。 <ul style="list-style-type: none"><li><code>connected</code></li><li><code>disconnected</code></li></ul> |

次のコマンドは、クラスタ上のすべてのFPolicyサーバからのパススルーリード接続に関する情報を表示します。

```
cluster1::> vserver fpolicy show-passthrough-read-connection
Vserver      Policy Name  Node      FPolicy Server  Server Status
-----
vs2.example.com pol_cifs_2  FPolicy-01  2.2.2.2        disconnected
vs1.example.com pol_cifs_1  FPolicy-01  1.1.1.1        connected
```

次のコマンドは、ポリシー「pol\_cifs\_1」に設定されているFPolicyサーバからのパススルーリード接続に関する詳細情報を表示します。

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name pol_cifs_1 -instance
Node: FPolicy-01
Vserver: vs1.example.com
Policy: pol_cifs_1
Server: 1.1.1.1
Session ID of the Control Channel: 8cef052e-2502-11e3-88d4-123478563412
Server Status: connected
Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

## 関連コンセプト

[FPolicyと外部FPolicyサーバとの連携](#)(467ページ)

[FPolicyのパススルーリードによる階層型ストレージ管理のユーザビリティ向上](#)(472ページ)

## 関連タスク

[外部FPolicyサーバへの接続に関する情報の表示](#)(506ページ)

## 著作権に関する情報

---

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103(1988年10月)および FAR 52-227-19(1987年6月)のRights in Technical Data and Computer Software(技術データおよびコンピュータソフトウェアに関する諸権利)条項の(c) (1) (ii)項、に規定された制限が適用されます。

## 商標に関する情報

---

NetApp、NetAppのロゴ、Go Further, Faster、AltaVault、ASUP、AutoSupport、Campaign Express、Cloud ONTAP、clustered Data ONTAP、Customer Fitness、Data ONTAP、DataMotion、Fitness、Flash Accel、Flash Cache、Flash Pool、FlashRay、FlexArray、FlexCache、FlexClone、FlexPod、FlexScale、FlexShare、FlexVol、FPolicy、GetSuccessful、LockVault、Manage ONTAP、Mars、MetroCluster、MultiStore、NetApp Insight、OnCommand、ONTAP、ONTAPI、RAID DP、RAID-TEC、SANtricity、SecureShare、Simplicity、Simulate ONTAP、Snap Creator、SnapCenter、SnapCopy、SnapDrive、SnapIntegrator、SnapLock、SnapManager、SnapMirror、SnapMover、SnapProtect、SnapRestore、Snapshot、SnapValidator、SnapVault、StorageGRID、Tech OnTap、Unbound Cloud、WAFL、その他の名称は、米国またはその他の国あるいはその両方におけるNetApp, Inc.の登録商標です。その他のブランドまたは製品は、それぞれを保有する各社の商標または登録商標であり、相応の取り扱いが必要です。ネットアップの商標の最新のリストは、<http://www.netapp.com/jp/legal/netapptmlist.aspx>でご覧いただけます。

## マニュアルの更新について

---

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitterアカウントもあります。

ご意見やご要望は、[ng-gpso-jp-documents@netapp.com](mailto:ng-gpso-jp-documents@netapp.com)までお寄せください。その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。



# 索引

## 数字

### 8.3形式

ファイル名とディレクトリ名の作成時にclustered  
Data ONTAPで使用する仕組み [147](#)

## A

### ACE

セキュリティ記述子のDACLへの追加 [265](#)  
セキュリティ記述子のSACLへの追加 [278](#)  
ダイナミック アクセス制御が無効な場合のダイナミ  
ック アクセス制御ACEを含むリソース上での管理  
[204](#)  
定義 [259](#)

### ACL

Data ONTAPでの共有レベルの使用法 [191](#)  
NTFSを使用する利点, SMBクライアントへのUNIX  
セキュリティ形式のデータの提供 [77](#)  
SMB共有での作成 [191](#)  
SMB共有の作成時のデフォルト [175](#)  
SMB共有レベルの管理の概要 [191](#)  
SMBの管理用コマンド [193](#)  
ダイナミック アクセス制御が無効な場合のダイナミ  
ック アクセス制御ACEを含むリソース上での管理  
[204](#)  
定義 [259](#)

### Active Directory

SVMのコンピュータ アカウント, 情報の表示 [30](#)  
SVMのコンピュータ アカウントの削除 [30](#)  
SVMのドメインへの参加 [141](#)  
コンピュータ アカウント, LDAPサーバおよびドメ  
イン コントローラのリセットと再検出 [33](#)  
コンピュータ アカウント, SVMが関連付けられてい  
るドメインの変更 [28](#)  
コンピュータ アカウント, CIFSサーバの代わりに作  
成するかどうかを選択する方法 [26, 36](#)  
コンピュータ アカウント, SVMの設定と管理(CIFS  
ライセンスなし) [26](#)  
コンピュータ アカウント, SVMのパスワードの変更  
またはリセット [31](#)  
コンピュータ アカウント, 管理の概要 [27](#)  
コンピュータ アカウント, 検出されたLDAPサーバお  
よびドメイン コントローラに関する情報の表示 [32](#)  
コンピュータ アカウント, ドメイン コントローラ接続の  
管理の概要 [32](#)  
コンピュータ アカウント, 優先ドメイン コントローラに  
関する情報の表示 [35](#)  
コンピュータ アカウント, 優先ドメイン コントローラの  
追加または削除 [34](#)  
コンピュータ アカウントの作成(CIFSライセンスな  
し) [27](#)  
制限されたグループのGPOに関する詳細の表示  
[125](#)  
定義されているGPO設定に関する情報の表示 [122](#)  
定義されている集約型アクセス ポリシーに関する  
情報の表示 [127](#)

定義されている集約型アクセス ポリシー ルールに  
関する情報の表示 [128](#)

### Active Directoryコンピュータ アカウント

Active Directory LDAPサーバおよびドメイン コント  
ローラのリセットと再検出 [33](#)  
SVM, 情報の表示 [30](#)  
SVM, パスワードの変更またはリセット [31](#)  
SVMが関連付けられているActive Directoryドメ  
インの変更 [28](#)  
SVMでの削除 [30](#)  
管理の概要 [27](#)  
検出されたLDAPサーバおよびドメイン コントローラ  
に関する情報の表示 [32](#)  
作成するかどうかを選択する方法, CIFSサーバの  
代わり [26, 36](#)  
ドメイン コントローラ接続の管理の概要 [32](#)  
優先ドメイン コントローラに関する情報の表示 [35](#)  
優先ドメイン コントローラの追加または削除 [34](#)

### AD

次を参照: Active Directory

admin\$デフォルト共有

概要と用途 [176](#)

Administratorsグループ, Windows

ルートへのマッピング [103](#)

### AES暗号化

CIFSサーバでKerberos通信用に強固なセキュリ  
ティを設定するための有効化と無効化 [86](#)  
CIFSサーバでのKerberos通信での強固なセキュリ  
ティ設定の使用法 [85](#)

## B

### BranchCache

CIFSサーバの設定 [348](#)  
Data ONTAPのバージョン要件 [346](#)  
GPOサポート [362](#)  
SMB共有での無効化の概要 [363](#)  
SMB共有での有効化の概要 [352](#)  
SMB共有の作成時の有効化 [352](#)  
Windowsホストのバージョン要件 [346](#)  
既存のSMB共有での有効化 [353](#)  
共有プロパティ [353](#)  
サーバ キーの変更 [357](#)  
サポートされるSMB 2.1の機能 [106](#)  
サポートするバージョンの変更 [355](#)  
サポート対象のバージョン [345](#)  
すべてのSMB共有での自動キャッシュの停止 [365](#)  
設定に関する情報の表示 [356](#)  
設定の推奨事項 [347](#)  
設定の変更 [355](#)  
設定の前提条件 [348](#)  
設定の要件、考慮事項、推奨事項の概要 [345](#)  
設定を削除した場合の動作 [367](#)  
設定を削除する方法 [367](#)  
単一のSMB共有での無効化 [364](#)  
定義および適用されているGPOに関する情報の表  
示 [362](#)  
統計の表示 [359](#)

動作モードの変更 [355](#)  
 ネットワーク プロトコルのサポート要件 [345](#)  
 ハッシュ ストアからのハッシュのフラッシュ [359](#)  
 ハッシュ ストア ディレクトリの最大サイズの変更 [355](#)  
 ハッシュ ストア ディレクトリのパスの変更 [355](#)  
 ハッシュ ストア ディレクトリのパスのボリュームサイズの増加 [355](#)  
 ハッシュ ストア の場所を選択する際の考慮事項 [347](#)  
 ハッシュの事前計算 [358](#)  
 ハッシュの統計の表示 [313](#)  
 ブランチ オフィスでSMB共有をキャッシュするために使用 [344](#)  
 無効化と有効化に関する情報 [365](#)  
 無効にした場合の動作 [365](#)  
 有効化と無効化 [366](#)  
 リバートした場合の動作 [368](#)  
 リモート オフィスでの設定に関する情報の参照先 [351](#)

#### BranchCache/ハッシュ

Data ONTAPが無効になる理由 [346](#)  
 統計, 使用可能なカウンタとオブジェクトの確認 [311](#), [418](#)

#### BUILTINグループ

事前定義のローカル グループ [222](#)  
 使用時の考慮事項 [221](#)

## C

#### c\$デフォルト共有

概要と用途 [176](#)

#### CA共有 [385](#)

次も参照: 継続的可用性を備えた共有

#### CA証明書

自己署名ルートインストール, SVM上 [100](#)  
 自己署名ルートのコピーのASCIIテキストへの変換 [99](#)  
 自己署名ルートのコピーのエクスポート [99](#)

#### CIFS

Data ONTAPでの共有レベルのACLの使用法 [191](#)  
 Microsoftの以前のバージョン機能によるファイルとフォルダのリカバリ [323](#)  
 SMBアクセスでのエクスポート ポリシーの役割 [25](#)  
 SMB共有でのBranchCacheの有効化の概要 [352](#)  
 アクセス制御リストの管理用コマンド [193](#)  
 以前のバージョン機能のアクセスを有効にする Snapshot設定の作成 [326](#)  
 オフライン ファイルを使用するための要件 [316](#)  
 オフライン ファイルを導入する際の考慮事項 [316](#)  
 サーバベースのサービスの導入の概要 [327](#)  
 統計, 使用可能なカウンタとオブジェクトの確認 [311](#), [418](#)  
 統計の表示 [313](#)

#### CIFS-NDOSubシステム

ヘルスモニタの設定情報の表示 [421](#)

#### CIFSオプション [71](#)

次も参照: CIFSサーバ オプション

#### CIFSサーバ

BranchCacheのGPOのサポート [362](#)  
 BranchCacheの設定 [348](#)

CIFSサーバを別のドメインに移動する前のSVM上の動的DNSの設定 [140](#)  
 Data ONTAPのアップグレード後のSMBアクセスのエクスポート ポリシーの扱い [210](#)  
 DFS対応の自動通知の管理 [80](#), [341](#)  
 SVM用のDNSサービスの設定 [63](#)  
 GPOサポートの有効化と無効化 [120](#)  
 GPO設定の手動更新 [122](#)  
 GPOの更新方法 [121](#)  
 GPOの適用 [115](#)  
 Hyper-V over SMBの要件 [393](#)  
 Hyper-VおよびSQL Server over SMB構成のオプション設定の確認 [408](#)  
 IPv6の要件 [143](#)  
 Kerberosセキュリティ設定の変更 [83](#)  
 Kerberos通信での強固なセキュリティ設定のためのAES暗号化の使用法 [85](#)  
 Kerberos通信のセキュリティ強化のためのAES暗号化の有効化と無効化 [86](#)  
 LDAP over SSL/TLSの有効化 [99](#)  
 LDAP over SSL/TLSを設定するタスク [98](#)  
 LDAPサーバおよびドメイン コントローラ サーバのリセットと再検出 [132](#)  
 LIFの作成 [61](#)  
 LMCompatibilityLevel設定 [84](#)  
 NetBIOSエイリアスの管理の概要 [134](#)  
 NetBIOSエイリアスのリストの作成 [134](#)  
 NetBIOSエイリアスのリストの表示 [136](#)  
 ODXの有効化と無効化 [373](#)  
 SMBアクセスに関するローカル ユーザ認証の有効化と無効化 [225](#)  
 SMB共有の作成 [180](#)  
 SMB共有の命名に関する考慮事項 [177](#)  
 SMB署名ポリシーがSMB通信に与える影響 [87](#)  
 SMB署名要求の有効化と無効化 [90](#)  
 SMBセッションが署名されているかどうかの確認 [91](#)  
 SMBの設定の概要 [105](#)  
 SMBを介したデータ転送でのセキュリティ強化のためのSMB暗号化の使用法 [94](#)  
 SQL Server over SMBの要件 [394](#)  
 SVM上でデータLIFの作成用に収集する情報 [44](#)  
 SVM上のNISまたはLDAPネーム サービスの設定 [68](#)  
 SVMディザスタリカバリ構成のセキュリティ設定に関する重要な考慮事項 [81](#)  
 SVMでの動的DNSの設定 [65](#)  
 SVMのActive Directoryドメインへの参加 [141](#)  
 SVMのIPspaceの作成 [52](#)  
 SVMを作成する前に収集する情報 [42](#)  
 SVMを含むIPspaceのブロードキャストドメインの作成 [56](#), [58](#)  
 VSSシャドウ コピーの有効化と無効化 [416](#)  
 移動プロファイルを使用してユーザ プロファイルを格納する利点 [319](#)  
 オプションの一覧 [71](#)  
 オプションの設定 [75](#)  
 オプションを使用したカスタマイズ [71](#)  
 外部サーバへのIPv6接続の使用法 [145](#)  
 管理の概要 [71](#)  
 管理用コマンド [142](#)  
 既存のリストへのNetBIOSエイリアスの追加 [134](#)

クライアントがNetBIOSエイリアスを使用して接続しているかどうかの確認 [137](#)  
 クライアントが暗号化されたSMBセッションを使用して接続しているかどうかの確認 [96](#)  
 権限を使用したリソースへのアクセスの管理 [216](#)  
 検出されたLDAPおよびドメイン コントローラ サーバに関する情報の表示 [132](#)  
 構成計画の概要 [38](#)  
 コンピュータ アカウント パスワードの自動変更の設定 [130](#)  
 コンピュータ アカウント パスワードの自動変更の無効化 [131](#)  
 コンピュータ アカウント パスワードの変更の概要 [130](#)  
 最低限の認証セキュリティレベルの設定 [84](#)  
 削除した場合のローカル ユーザとローカル グループに対する影響 [219](#)  
 削除時のSMB共有の動作 [175](#)  
 作成 [65](#)  
 作成準備の際にネーム サービスの設定用に収集する情報 [46](#)  
 作成するかどうかを選択する方法, Active Directory コンピュータ アカウントの代わり [26, 36](#)  
 作成前に収集しておくべき情報 [39, 49](#)  
 作成前のタイム サービスの設定 [52](#)  
 サポートされるGPO [116](#)  
 自動ノード リファラルの有効化と無効化 [377](#)  
 受信SMBトラフィックのSMB暗号化要求の有効化と無効化 [95](#)  
 セキュリティ設定情報の表示 [81](#)  
 セキュリティ設定の管理の概要 [81](#)  
 設定の概要 [36](#)  
 セットアップ, 新しいブロードキャストドメインに追加できるポートの確認 [53](#)  
 セットアップ, 新しいブロードキャストドメインへの追加前の既存のブロードキャストドメインからのポートの削除 [55](#)  
 セットアップについて確認しておく項目 [50](#)  
 セットアップの前提条件 [37](#)  
 その他のタスクの管理の概要 [137](#)  
 ダイナミック アクセス制御でサポートされる機能とサポートされない機能 [201](#)  
 ダイナミック アクセス制御と集約型アクセス ポリシーでを使用してデータへのアクセスを保護する際の考慮事項 [202](#)  
 定義および適用されているBranchCache GPOに関する情報の表示 [362](#)  
 停止と起動 [139](#)  
 データへのアクセスを保護する集約型アクセス ポリシーの設定 [204](#)  
 適用されているGPO設定に関する情報の表示 [122](#)  
 適用されている集約型アクセス ポリシーに関する情報の表示 [127](#)  
 適用されている集約型アクセス ポリシー ルールに関する情報の表示 [128](#)  
 適用されている制限されたグループのGPOに関する詳細の表示 [125](#)  
 デフォルト ユーザ マッピングの設定の概要 [100](#)  
 統計カウンタによるSMB自動ノード リファラルのアクティビティの監視 [377](#)  
 ドメイン アカウントのパスワードの変更またはリセット [130](#)

ネーム マッピングの作成の概要 [167](#)  
 複数のデータLIFでSMB署名の要求を変更する場合の考慮事項 [89](#)  
 別のOUへの移動 [140](#)  
 ホストするためのSVMの作成 [59](#)  
 マルチドメイン ネーム マッピングの検索, 検出された信頼できるドメインに関する情報の表示 [173](#)  
 マルチドメイン ネーム マッピングの検索, 信頼できるドメインの再検出 [173](#)  
 マルチドメイン ネーム マッピングの検索, 信頼できるドメインの優先リストに関する情報の表示 [175](#)  
 マルチドメイン ネーム マッピングの検索, 信頼できるドメインの優先リストの設定 [174](#)  
 マルチドメイン ネーム マッピングの検索, 有効化と無効化 [172](#)  
 優先ドメイン コントローラの追加 [133](#)  
 リストからのNetBIOSエイリアスの削除 [135](#)  
 リストからのすべてのNetBIOSエイリアスの削除 [135](#)  
 リモートVSSによる仮想マシンの共有ベースのバックアップ [387](#)  
 ローカル ユーザおよびローカル グループを使用した認証と許可 [216](#)  
 ローカル ユーザとローカル グループの有効化と無効化 [224](#)  
 CIFSサーバ オプション  
   CIFSサーバのカスタマイズの使用 [71](#)  
   DFSの自動通知の処理の制御方法 [79, 340](#)  
   Hyper-VおよびSQL Server over SMB構成の設定の確認 [408](#)  
   restrict anonymous, 匿名ユーザに対するアクセス制限の設定 [76](#)  
   使用できるオプションの一覧 [71](#)  
   設定 [75](#)  
 CIFSサーバの移動  
   SVM上の動的DNSの変更 [140](#)  
 CIFSサーバの設定  
   計画の概要 [38](#)  
 CIFSサービス  
   IPv6のサポート [144](#)  
   通信でのIPv6ネットワークのサポート [143](#)  
 CIFSセッション  
   次を参照: SMBセッション  
 CIFSのセットアップ  
   新しいブロードキャストドメインに追加できるポートの確認 [53](#)  
 CIFSライセンスなし  
   SVM用のActive Directoryコンピュータ アカウントの設定と管理 [26](#)

## D

DAC  
 次を参照: ダイナミック アクセス制御  
 DACL  
   NTFSのACEの管理用コマンド [288](#)  
   セキュリティ記述子へのACEの追加 [265](#)  
   定義 [259](#)  
   次も参照: NTFSファイル権限  
   次も参照: NTFSファイル権限  
 Data ONTAP

- Hyper-V over SMBおよびSQL Server over SMB構成の要件 [392](#)
- SMBアクセスのアップグレード後のエクスポートポリシーの扱い [210](#)
- SMBファイル アクセスの理解 [15](#)
- [以前のバージョン]を使用するための要件 [323](#)
- 監査プロセスの仕組み [433](#)
- 共有パス コンポーネントのロックの処理に関するWindowsとの違い [303](#)
- ローカル ユーザとグループ [216](#)
- Data ONTAP CLI
  - NTFS監査ポリシーの設定方法 [454](#)
- DDNS
  - 次を参照: 動的DNS
- DFSの通知
  - CIFSサーバが自動で提供するかどうかの管理 [80](#), [341](#)
  - 自動, clustered Data ONTAPでCIFSサーバ オプションを使用して制御する方法 [79](#), [340](#)
- DNS
  - サービス, SVMでの設定 [63](#)
  - 設定用に収集する情報 [46](#)
- E**
- EVTX
  - サポートされる監査イベント ログのファイル形式 [436](#)
  - ファイル形式, 監査イベント ログの表示 [436](#)
- F**
- FlexVol
  - NFSからSMBへの文字マッピングを管理するコマンド [166](#)
  - SMBファイル名の変換のための文字マッピングの設定 [164](#)
  - セキュリティ形式の設定 [149](#)
- FlexVolを備えたSVM
  - セキュリティ ポリシーの適用 [272](#), [285](#)
- FPolicy
  - パススルー リードが有効になっている場合の読み取り要求の処理方法 [473](#)
  - パススルー リードによるHSMのユーザビリティ向上方法 [472](#)
  - パススルー リードのアップグレードおよびリバートに関する考慮事項 [474](#)
- FPolicyイベント
  - FPolicyでSMBを監視するために、サポートされるファイル処理とフィルタの組み合わせ [486](#)
  - NFSv3でサポートされるファイル処理とフィルタの組み合わせ [487](#)
  - NFSv4でサポートされるファイル処理とフィルタの組み合わせ [487](#)
  - 作成 [498](#)
  - 設定の計画 [483](#)
  - 設定用に収集する情報 [488](#)
- FPolicy外部エンジン
  - SVMのIDが保持されない設定でFPolicyのSSL認証用セキュリティ証明書がレプリケートされない [481](#)
- MetroClusterおよびSVMディザスタリカバリ, 認証方式を選択する際の制限事項 [482](#)
- SSL認証された接続の設定に関する追加情報 [481](#)
- 作成 [497](#)
- 設定の計画 [476](#)
- 設定用に収集する情報 [482](#)
- FPolicy外部通信
  - ノードのフェイルオーバー時の実行方法 [469](#)
- FPolicy構成
  - 構成計画の概要 [476](#)
  - 作成 [496](#)
  - 情報の表示 [503](#)
  - 情報を表示するコマンド [503](#)
  - 情報を表示する際のshowコマンドの仕組み [503](#)
  - セットアップ手順 [475](#)
  - 変更用コマンド [502](#)
  - 要件、考慮事項、およびベストプラクティスに関する情報 [473](#)
- FPolicyサーバ
  - FPolicy設定を作成するときに使用する外部の [471](#)
  - FPolicyと外部FPolicyサーバとの連携 [467](#)
  - FPolicyパススルー リード接続のステータスに関する情報の表示 [508](#)
  - 外部からの切断 [506](#)
  - 外部への接続 [506](#)
  - 外部への接続に関する情報の表示 [506](#)
  - 機能 [465](#)
  - ノードへの通信プロセス [468](#)
- FPolicyサービス
  - SVMネームスペースにおける仕組み [470](#)
- FPolicyスコープ
  - FPolicyポリシーで標準のエンジンを使用する場合の要件 [492](#)
  - 作成 [500](#)
  - 収集する設定情報 [496](#)
  - 設定の計画 [493](#)
- FPolicy接続
  - 外部FPolicyサーバへの接続時の管理責任 [467](#)
  - 外部サーバ接続に関する情報の表示 [506](#)
  - 権限付きデータ アクセス チャネルでの接続クレデンシャルの使用法 [467](#)
  - 権限付きデータ アクセス チャネルの使用法 [467](#)
  - 権限付きデータ アクセスのためのスーパー ユーザクレデンシャルの付与とは [468](#)
  - 制御チャネルの使用法 [467](#)
  - データLIFの移行とフェイルオーバーの処理方法 [469](#)
  - 同期アプリケーションおよび非同期アプリケーション [466](#)
  - 同期通知と非同期通知, 定義 [465](#)
  - ノードと外部FPolicyサーバの間の通信プロセス [468](#)
- FPolicy通信
  - 同期通知と非同期通知, 定義 [465](#)
- FPolicyの設定タイプ
  - FPolicy設定を作成するときに使用する外部FPolicyサーバ [471](#)
  - 定義 [470](#)
  - ネイティブFPolicyの設定を作成する場合 [471](#)
- FPolicyのセットアップ
  - 推奨事項 [474](#)
  - 要件 [473](#)



## FPolicyの通知

同期と非同期, 定義 465

## FPolicyのベストプラクティス

セットアップ 474

## FPolicyフレームワーク

監視できるプロトコル 465

機能 465

クラスタコンポーネントの役割 466

定義 465

## FPolicyポリシー

FPolicyによる複数の処理方法 468

作成 499

収集する設定情報 493

ステータスに関する情報の表示 504

設定の計画 488

標準のエンジンを使用する場合のFPolicyスコープの要件 492

有効化 501

有効化と無効化 502

有効な対象に関する情報の表示 505

## G

## GPO

BranchCacheのサポート 362

CIFSサーバで使用するための要件 120

CIFSサーバでの更新方法 121

CIFSサーバに適用されているかActive Directoryで定義されている集約型アクセス ポリシーに関する情報の表示 127

CIFSサーバに適用されているかActive Directoryで定義されている集約型アクセス ポリシー ルールに関する情報の表示 128

CIFSサーバに適用されている制限されたグループおよびActive Directoryで定義されている制限されたグループに関する詳細の表示 125

CIFSサーバに適用されている設定およびActive Directoryで定義されている設定に関する情報の表示 122

CIFSサーバへの適用 115

更新が失敗した場合の対応 121

サポート対象 116

サポートの有効化と無効化 120

設定の手動更新 122

定義および適用されているBranchCacheに関する情報の表示 362

## H

## HSM

FPolicyのパススルー リードによるユーザビリティ向上方法 472

## Hyper-V over SMB

Kerberos認証とNTLMv2認証が許可されていることの確認 404

LIFステータスの確認 424

NDOのCIFSサーバ オプション設定の確認 408

ODXコピー オフロードの使用法 390

ODXコピー オフロードを使用する場合の要件 399

SMB 3.0の機能がサポートする仕組み 385

SMB共有の継続的な可用性の設定の確認 422

SMB共有を介したバックアップでのVSSシャドウ コピーの有効化と無効化 416

SnapManager for Hyper-VによるリモートVSSベースのバックアップの管理方法 389

VSSシャドウのディレクトリ階層の設定 413

概念 383

継続的な可用性を備えた共有のNTFSデータ ボリュームの作成 410

継続的な可用性を確保するための既存の共有の設定 414

継続的な可用性を実装したSMB共有の作成のために収集する情報 401

構成, ボリュームを作成するために収集する情報 400

構成時のネットワークおよびデータLIF要件 393

構成の管理に関する情報 413

コンピュータ アカウントがデフォルトのUNIXユーザにマッピングされていることの確認 405

サポートされるノンストップ オペレーション 382

システム ヘルスモニタを使用したノンストップ オペレーションのステータスの確認方法 420

自動ノード リファラルの無効化の確認 409

スタンドアロン構成とクラスタ構成のサポート 382

設定, 継続的な可用性を備えた共有の作成 411

設定計画タスクの概要 400

設定時のCIFSサーバの要件 393

設定時のData ONTAPとライセンスの要件 392

設定時の推奨事項 399

設定する際のボリューム要件 393

設定するときの要件と考慮事項 395

設定する必要がある内容 382

設定要件と考慮事項についての情報 392

統計を使用したSMBアクティビティの監視についての情報 418

ノンストップ オペレーション, 定義 382

ノンストップ オペレーション機能を提供するプロトコル 383

ノンストップ オペレーションを実現するData ONTAPの設定作成の概要 403

リポート時の考慮事項 417

リモートVSSで使用されるディレクトリ構造の例 388

リモートVSSに対応したバックアップ ソリューションを使用する場合の考慮事項 398

リモートVSSによる仮想マシンの共有ベースのバックアップ 387

ルート ボリュームがNTFSセキュリティ形式に設定されていることの確認 407

## I

## IDの破棄

SVMディザスタリカバリ デスティネーションでローカル ユーザまたはグループを使用するファイルとディレクトリのポリシーを適用する際の考慮事項 260

SVMのディザスタリカバリ構成でのCIFSサーバ セキュリティ設定に関する重要な考慮事項 81

## Infinite Volume

SMBサポートに関する情報の参照先 70

セキュリティ スタイルに関する情報の参照先 148

## ipc\$デフォルト共有

概要と用途 176

## IPspace

CIFSサーバが配置されるSVM用で作成 [52](#)  
 CIFSサーバのセットアップ用の新しいブロードキャストドメインへの追加前の既存のブロードキャストドメインからのポートの削除 [55](#)  
 CIFSサーバを作成する前に収集する情報 [39](#)  
 新しいブロードキャストドメインに追加できるポートの確認 [53](#)  
 ブロードキャストドメインの作成 [56, 58](#)

## IPv6

CIFSサーバが使用する方法, 外部サーバへの接続時 [145](#)  
 SMBアクセスとCIFSサービスでサポートされるネットワーク [143](#)  
 SMBセッション情報の表示 [146](#)  
 SMBセッションの監視 [146](#)  
 SMBとCIFSサービスでのサポート [144](#)  
 SMBの要件 [143](#)  
 SMB用のクラスタでの有効化 [146](#)  
 クラスタでの無効化方法 [146](#)

## K

## KDCリソース

SID圧縮のサポート [22](#)

## Kerberos

CIFS認証用のタイム サービスを設定するために収集する情報 [38](#)  
 Hyper-V over SMB構成で認証方法として許可されていることの確認 [404](#)  
 SMBアクセスでの認証のためのエクスポート ポリシーの使用方法 [209](#)  
 通信, CIFSサーバで強固なセキュリティを設定するためのAES暗号化の有効化と無効化 [86](#)  
 認証 [22](#)

## Kerberos通信

CIFSサーバでの強固なセキュリティ設定のためのAES暗号化の使用方法 [85](#)

## L

## LDAP

検出されたサーバに関する情報の表示 [132](#)  
 ネーム サービス, SVM上の設定 [68](#)

## LDAP over SSL/TLS

CIFSサーバでの有効化 [99](#)  
 CIFSサーバを設定するタスク [98](#)  
 エクスポートされた自己署名ルートCA証明書のコピーのASCIIテキストへの変換 [99](#)  
 自己署名ルートCA証明書のコピーのエクスポート [99](#)

## LDAPサーバ

Active Directoryのリセットと再検出 [33](#)  
 検出されたActive Directoryに関する情報の表示 [32](#)

## LIF

CIFSサーバ用の作成 [61](#)  
 FPolicyによるデータの移行とフェイルオーバーの処理方法 [469](#)  
 Hyper-V over SMBおよびSQL Server over SMB構成の要件 [393](#)  
 Hyper-V over SMB構成のステータスの確認 [424](#)

SQL Server over SMB構成のステータスの確認 [424](#)

データ, FPolicyの実装での役割 [466](#)

データ, SVM上での作成用に収集する情報 [44](#)

ファイルアクセス管理の設定要件 [19](#)

## LMCompatibilityLevel

CIFSサーバの設定 [84](#)

## M

## MetroCluster構成

クラスタを対象としたFPolicy外部エンジンの認証方式を選択する際の制限事項 [482](#)

## Microsoft SQL Server

次を参照: SQL Server

## Microsoft SQL Server over SMB

サポートされるノンストップ オペレーション [382](#)

## Microsoft管理コンソール

ローカル ユーザとローカル グループに対して実行できる管理タスク [219](#)

ローカル ユーザとローカル グループの情報の表示 [219](#)

次も参照: MMC

## MMC

SVMへの接続とSMB共有の表示 [189](#)

共有でのオフライン ファイル サポートの設定に使用 [318](#)

## N

## NAS

一般的なネームスペース アーキテクチャ [16](#)  
 ジャンクション ポイントが指定されていないボリュームの作成 [151](#)

ジャンクション ポイントを指定したボリュームの作成 [150](#)

ネームスペースに対するボリュームのマウントまたはアンマウント [152](#)

ボリューム マウント ポイントとジャンクション ポイントに関する情報の表示 [153](#)

## NASネームスペース

データ ボリュームの作成と管理の概要 [150](#)

## NBエイリアス

次を参照: NetBIOSエイリアス

## NDO

次を参照: ノンストップ オペレーション

## NetBIOS

TCP経由, 情報の表示 [142](#)

## NetBIOSエイリアス

CIFSサーバ エイリアス リストからの削除 [135](#)

CIFSサーバ上での管理の概要 [134](#)

CIFSサーバ上での既存のリストへの追加 [134](#)

CIFSサーバ上でのリストの作成 [134](#)

CIFSサーバのための追加または削除, コマンド [142](#)  
 クライアントが使用して接続しているかどうかの確認 [137](#)

使用して接続しているクライアントの確認 [137](#)

リストの表示, CIFSサーバ [136](#)

## NFS

Data ONTAPによる読み取り専用ビットの処理方法 [302](#)

NFSv4監査情報, 表示 [255](#)

監査設定 [455](#)

- 監査できるイベント [442](#)
  - ファイルとディレクトリの命名規則 [147](#)
  - プロトコル間のファイル ロックの説明 [302](#)
  - SVMのプロトコルの変更 [138](#)
  - NFSエクスポート
    - ボリューム ジャンクションの使用法 [16](#)
  - NFSクライアント
    - FlexVolでのSMBファイル名の変換のための文字マッピングの設定 [164](#)
  - NIS
    - 設定用に収集する情報 [46](#)
    - ネーム サービス, SVM上の設定 [68](#)
  - No space left on deviceエラー:
    - トラブルシューティング方法 [464](#)
  - NT STATUS\_DUPLICATE\_NAMEエラー
    - GPO更新の場合の対応 [121](#)
  - NTFS
    - DACLのACE, 管理用コマンド [288](#)
    - Data ONTAP CLIを使用した監査ポリシーの設定方法 [454](#)
    - mixed形式のボリュームのダイナミック アクセス制御セキュリティに関する情報の表示 [206](#)
    - mixed形式のボリュームのファイル セキュリティ, 情報の表示 [250](#)
    - NTFSセキュリティ形式のボリュームのファイル セキュリティ情報の表示 [247](#)
    - SACLのACE, 管理用コマンド [288](#)
    - Windowsの[セキュリティ]タブを使用した詳細なファイルやフォルダの権限の設定 [196](#)
    - Windowsの[セキュリティ]タブを使用した標準のファイルやフォルダの権限の設定 [194](#)
    - セキュリティ記述子, 管理用コマンド [288](#)
    - セキュリティ記述子の作成 [263](#), [276](#)
    - データ ボリューム, 継続的可用性を備えた共有用の作成 [410](#)
    - ルート ボリュームのセキュリティ形式, Hyper-VおよびSQL Server over SMB構成の確認 [407](#)
  - NTFS ACL
    - SMBクライアントへのUNIXセキュリティ形式のデータの提供に使用する利点 [77](#)
  - NTFS代替データ ストリーム
    - ファイルを監査する際の考慮事項 [441](#)
  - NTFSファイル権限
    - Data ONTAP CLIを使用した設定方法 [199](#)
  - NTLM
    - SMBアクセスでの認証のためのエクスポート ポリシーの使用法 [209](#)
    - 認証 [23](#)
  - NTLMv2
    - Hyper-V over SMB構成で認証方法として許可されていることの確認 [404](#)
  - NTP
    - 次を参照: タイム サービス
  - nullユーザ
    - CIFSのアクセス制限の設定 [76](#)
- ## O
- ODX
    - Hyper-V over SMBおよびSQL Server over SMB構成での使用法 [390](#)
    - 仕組み [369](#)
    - 使用するための要件 [370](#)
    - 使用する場合の考慮事項 [371](#)
    - トークン [369](#)
    - 有効化と無効化 [373](#)
    - ユースケース [372](#)
    - リモートコピーのパフォーマンスの向上 [368](#)
  - ODXコピー オフロード
    - Hyper-V over SMBソリューションとともに使用する場合の要件 [399](#)
    - SQL Server over SMBソリューションとともに使用する場合の要件 [399](#)
  - oplocks
    - SMB共有の作成時における有効化と無効化 [110](#)
    - 監視 [113](#)
    - 既存のSMB共有での有効化と無効化 [111](#)
    - ボリュームやqtreeで有効または無効にするためのコマンド [112](#)
  - oplock
    - SMBクライアント パフォーマンスの向上 [110](#)
    - 書き込みキャッシュ データ消失に関する考慮事項 [110](#)
  - oplockリリース
    - SMB共有の作成時における有効化と無効化 [110](#)
    - SMBクライアント パフォーマンスの向上 [110](#)
    - 監視 [113](#)
    - 既存のSMB共有での有効化と無効化 [111](#)
    - サポートされるSMB 2.1の機能 [106](#)
  - Organizational Unit
    - 次を参照: OU
  - OU
    - CIFSサーバを別に移動 [140](#)
- ## Q
- qtree
    - oplockを有効または無効にするためのコマンド [112](#)
    - oplockを有効または無効にできるタイミング [112](#)
    - ストレージレベルのアクセス保護セキュリティのファイル セキュリティ情報の表示 [162](#)
    - ストレージレベルのアクセス保護の削除 [163](#)
    - ストレージレベルのアクセス保護の設定 [157](#)
    - セキュリティ形式の設定 [149](#)
- ## R
- restrict anonymousオプション
    - 匿名ユーザに対するCIFSアクセス制限の設定 [76](#)
- ## S
- SACL
    - NTFSのACEの管理用コマンド [288](#)
    - セキュリティ記述子へのACEの追加 [278](#)
    - 定義 [259](#)
  - SeChangeNotifyPrivilege
    - 権限, トラバース チェックのバイパスを可能にするための追加 [244](#)
    - トラバース チェックのバイパスの設定についての情報 [242](#)
  - SeChangeNotifyPrivilege権限

- 使用したユーザとグループに対するトラバース チェックのバイパスの禁止 [245](#)
- SeSecurityPrivilege権限
  - SQL Serverのインストールに使用するユーザ アカウントへの追加 [412](#)
- SFOパートナー
  - 透過的なフェイルオーバーのために監視の役割を果たす仕組み [386](#)
- Shadowコピー
  - VSSのディレクトリ階層の設定 [413](#)
  - 定義 [387](#)
- showコマンド
  - FPolicyの設定を表示する際の仕組み [503](#)
- SID圧縮
  - KDCリソースのサポート [22](#)
- SLAG
  - 次を参照: ストレージレベルのアクセス保護
- SMB
  - 2.0の永続性ハンドル機能のサポート [105](#)
  - BranchCacheを使用したブランチ オフィスでのキャッシュ [344](#)
  - CIFSサーバでの自動ノード リファールの有効化と無効化 [377](#)
  - Data ONTAPでの共有レベルのACLの使用法 [191](#)
  - Data ONTAPによる読み取り専用ビットの処理方法 [302](#)
  - FlexVolを備えたSVMでサポートされるバージョン [105](#)
  - FlexVolを備えたSVMでの2.xの有効化と無効化 [108](#)
  - Infinite Volumeを備えたSVMでサポートされるバージョン [105](#)
  - IPv6セッション情報の表示 [146](#)
  - IPv6のサポート [144](#)
  - IPv6の要件 [143](#)
  - Kerberos認証 [22](#)
  - NFS文字マッピングを管理するコマンド [166](#)
  - NTLM認証 [23](#)
  - SMBアクセスでのIPv6ネットワークのサポート [143](#)
  - SMB自動ノード リファールを使用する際の考慮事項と要件 [374](#)
  - SMB署名統計情報の監視 [92](#)
  - SQL Serverのインストールに使用するユーザ アカウントへのSeSecurityPrivilege権限の追加 [412](#)
  - アクセス制御リストの管理用コマンド [193](#)
  - アクセスのためのネーム マッピングの使用法 [23](#)
  - [以前のバージョン]をサポートするバージョン [323](#)
  - [以前のバージョン]を使用するための要件 [323](#)
  - 移動プロファイルを使用するための要件 [320](#)
  - オフライン ファイルを使用するための要件 [316](#)
  - 監査できるイベント [438](#)
  - 共有パス コンポーネントのロックの処理に関するData ONTAPとWindowsの違い [303](#)
  - 共有レベルACLの管理の概要 [191](#)
  - クラスタでのIPv6の無効化方法 [146](#)
  - クラスタでのIPv6の有効化 [146](#)
  - 継続的可用性を備えた共有用のNTFSデータボリュームの作成 [410](#)
  - サポートされない2.0の機能 [105](#)
  - サポートされない2.1の機能 [106](#)
  - サポートされる1.0の機能 [105](#)
  - サポートされる2.0の機能 [105](#)
  - サポートされる2.1の機能 [106](#)
  - サポート対象のクライアント [37](#)
  - サポート対象のドメイン コントローラ [37](#)
  - サポートに関する情報の参照先, Infinite Volume [70](#)
  - 自動ノード リファールでクライアントの応答時間を改善する方法 [373](#)
  - 自動ノード リファールのサポート [376](#)
  - 署名, パフォーマンスへの影響 [88](#)
  - 署名ポリシーが通信に与える影響 [87](#)
  - データ転送でのセキュリティ強化のためのSMB暗号化の使用法 [94](#)
  - 統計, 使用可能なカウンタとオブジェクトの確認 [311, 418](#)
  - 統計カウンタによる自動ノード リファールのアクティビティの監視 [377](#)
  - 統計の表示 [313, 420](#)
  - ファイルとディレクトリの命名規則 [147](#)
  - フォルダ リダイレクトを使用するための要件 [321](#)
  - プロトコル間のファイル ロックの説明 [302](#)
  - SVMのプロトコルの変更 [138](#)
  - メタデータ キャッシュ エントリの有効期間の設定 [301](#)
  - メタデータのキャッシングの仕組み [300](#)
  - メタデータのキャッシングの有効化 [301](#)
  - ローカル ユーザに対するパスワードの複雑さの要件の有効化と無効化 [82](#)
- SMB 3.0
  - FlexVolを備えたSVMでの有効化と無効化 [109](#)
  - Hyper-V over SMBおよびSQL Server over SMBのノンストップ オペレーションをサポートする仕組み [385](#)
  - Hyper-VおよびSQL Server over SMB構成用の継続的可用性を備えた共有の作成 [411](#)
  - ODXの使用要件 [370](#)
  - 継続的可用性を備えた保護に関する情報の表示 [306, 425](#)
  - サポートされない機能 [107](#)
  - サポートされる機能 [107](#)
  - サポートされるノンストップ オペレーション [107](#)
- SMBアクセス
  - Data ONTAPのアップグレード後のエクスポート ポリシーの扱い [210](#)
  - UNIXシンボリック リンク サポートの設定 [342](#)
  - UNIXシンボリック リンクの使用法 [339](#)
  - UNIXシンボリック リンクを設定する場合の制限 [340](#)
  - アクセス制御にUNIXファイル権限を使用する場合 [199](#)
  - エクスポート ポリシーの使用法 [209](#)
  - エクスポート ポリシーの役割 [25](#)
  - エクスポート ポリシーの有効化と無効化 [210](#)
  - エクスポート ポリシーをリバートする際の考慮事項 [215](#)
  - 許可するエクスポート ポリシー ルールの例 [213](#)
  - シンボリック リンク マッピングの作成 [343](#)
  - 認証が果たす役割 [22](#)
  - ローカル ユーザとローカル グループの有効化と無効化 [224](#)
  - ローカル ユーザ認証の有効化と無効化 [225](#)
- SMB暗号化



- SMBを介したデータ転送でのセキュリティ強化の使用  
方法 [94](#)
- クライアントがSMBセッションで使用しているか  
どうかの確認 [96](#)
- 要求, 受信SMBトラフィックのCIFSサーバ上での有  
効化と無効化 [95](#)
- SMB共有
  - %uを使用したホーム ディレクトリ設定の作成 [333](#)
  - %wと%dを使用したホーム ディレクトリ設定の作  
成 [331](#)
  - 1.0用のメタデータ キャッシュの設定の概要 [300](#)
  - ACLの作成 [191](#)
  - BranchCacheの設定の推奨事項 [347](#)
  - BranchCacheの無効化の概要 [363](#)
  - CIFSサーバでの作成 [180](#)
  - CIFSサーバまたはSVMが削除された場合の動作  
[175](#)
  - clustered Data ONTAPにおける動的ホームディレ  
クトリの仕組み [327](#)
  - Hyper-VおよびSQL Server over SMB構成を作成す  
る際に収集する情報 [401](#)
  - Hyper-VまたはSQL Serverでノンストップ オペレー  
ションを実現するData ONTAPの設定の概要 [403](#)
  - SVMのMMCへの接続と表示 [189](#)
  - UNIXシンボリック リンク サポートの設定 [342](#)
  - VSSシャドウのディレクトリ階層の設定 [413](#)
  - アクセススペースの列挙の有効化と無効化 [380](#)
  - 以前のバージョン機能に対するSnapshotコピーの  
可用性の確認 [325](#)
  - [以前のバージョン]タブを使用したSnapshotコピー  
データの表示および管理 [324](#)
  - オフライン ファイル サポートの設定 [317](#)
  - 管理用コマンド [190](#)
  - 既存でのoplockの有効化と無効化 [111](#)
  - 既存に対する共有プロパティの追加または削除  
[187](#)
  - 既存の対象でのBranchCacheの有効化 [353](#)
  - 共有パスの実行権限の廃止 [178](#)
  - 継続的な可用性, Hyper-VおよびSQL Serverの設  
定の確認 [422](#)
  - 継続的な可用性を確保するための既存の共有の  
設定 [414](#)
  - 権限の設定 [191](#)
  - 作成時におけるoplockの有効化と無効化 [110](#)
  - 作成時に必要な情報 [179](#)
  - 作成時のBranchCacheの有効化 [352](#)
  - 作成時のデフォルトACL [175](#)
  - シンボリック リンク マッピングの作成 [343](#)
  - すべての自動BranchCacheキャッシュの停止 [365](#)
  - 単一のSMBでのBranchCacheの無効化 [364](#)
  - 定義 [175](#)
  - デフォルトの管理共有とは [176](#)
  - ファイル アクセスの管理 [216](#)
  - ファイルの作成時やアクセス時のディレクトリ名の  
大文字と小文字の区別による重大な影響 [178](#)
  - フォースグループ設定を使用した作成 [186](#)
  - フォースグループの設定, 機能 [185](#)
  - フォルダリダイレクトによるCIFSサーバへのデータ  
の格納に関する概要 [320](#)
  - フォルダリダイレクトの設定 [321](#)
  - ホーム ディレクトリの検索パスの追加 [330](#)
  - ホーム ディレクトリの追加 [328](#)
- ボリューム ジャンクションの使用方法 [16](#)
- マルチプロトコル環境でのファイルの作成時やアク  
セス時のファイル名とディレクトリ名の大文字と小  
文字の区別の影響 [147](#)
- 命名に関する考慮事項 [177](#)
- SMBクライアント
  - FlexVolでのファイル名の変換のための文字マッピ  
ングの設定 [164](#)
  - oplockによるパフォーマンスの向上 [110](#)
  - UNIXセキュリティ形式のデータに対するNTFS  
ACLの提供の有効化と無効化 [78](#)
  - UNIXセキュリティ形式のデータの提供にNTFS  
ACLを使用する利点 [77](#)
  - ファイル セキュリティの提供方法の管理, UNIXデ  
ータ [77](#)
- SMB署名
  - Data ONTAPでのサポート [87](#)
  - 設定の推奨事項 [89](#)
  - ネットワークのセキュリティを強化するために使用  
[87](#)
  - パフォーマンスへの影響 [88](#)
  - 複数のデータLIFがある場合の考慮事項 [89](#)
  - 要求の有効化と無効化 [90](#)
- SMB署名要求
  - 有効化と無効化 [90](#)
- SMBセキュリティトレース
  - 作成時の考慮事項 [291](#)
  - 監視されるアクセス チェックの種類 [291](#)
  - 結果の解釈方法 [299](#)
  - 結果の表示 [295](#)
  - 仕組み [290](#)
  - 実行の概要 [292](#)
  - すべてのレコードの削除 [299](#)
  - フィルタの削除 [298](#)
  - フィルタの作成 [293](#)
  - フィルタの表示 [295](#)
  - フィルタの変更 [297](#)
  - レコードの削除 [298](#)
- SMBセッション
  - IPv6情報の表示 [146](#)
  - クライアントが暗号化を使用して接続しているかど  
うかの確認 [96](#)
  - 情報の表示 [305, 306, 425](#)
  - 署名されているかどうかの確認 [91](#)
  - 接続しているユーザのタイプに関する情報の表示  
[104](#)
- SMB統計
  - 情報の表示 [305](#)
- SMBファイル アクセス
  - Data ONTAPの理解 [15](#)
  - セットアップの概要 [147](#)
- SMBホーム ディレクトリ
  - %uを使用した設定の作成 [333](#)
  - %wと%dを使用した設定の作成 [331](#)
  - clustered Data ONTAPにおける動的な仕組み [327](#)
  - 管理の概要 [327](#)
  - 検索パスの追加 [330](#)
- SMBホーム ディレクトリ共有
  - 追加 [328](#)
- SMBユーザ
  - デフォルトのUNIXユーザ マッピングの設定の概要  
[100](#)

- ホーム ディレクトリ パスの情報の表示 [337](#)
- ローカルでのパスワードの複雑さの要件の有効化と無効化 [82](#)
- SnapManager for Hyper-V
  - Hyper-V over SMBのリモートVSSベースのバックアップを管理するための使用方法 [389](#)
  - 設定に関する情報の参照先 [382](#)
- SnapManager for Microsoft SQL Server
  - 設定に関する情報の参照先 [382](#)
- SnapMirror
  - ローカル グループを含むSVM上で使用する際の考慮事項 [219](#)
- Snapshotコピー
  - 以前のバージョン機能に対する可用性の確認 [325](#)
  - 以前のバージョン機能のアクセスを有効にする設定 [326](#)
  - [以前のバージョン]タブを使用したデータの表示および管理 [324](#)
- SQL Server
  - SMBを介したソリューション, SMB 3.0の機能がサポートする仕組み [385](#)
  - インストーラのユーザ アカウントへのSeSecurityPrivilege権限の追加 [412](#)
  - 自動ノード リファラルの無効化の確認 [409](#)
  - 設定に関する情報の参照先 [382](#)
- SQL Server over SMB
  - LIFステータスの確認 [424](#)
  - NDOのCIFSサーバ オプション設定の確認 [408](#)
  - ODXコピー オフロードの使用法 [390](#)
  - ODXコピー オフロードを使用する場合の要件 [399](#)
  - SMB共有の継続的な可用性の設定の確認 [422](#)
  - インストールに使用するユーザ アカウントへのSeSecurityPrivilege権限の追加 [412](#)
  - 概念 [383](#)
  - 継続的可用性を備えた共有用のNTFSデータ ボリュームの作成 [410](#)
  - 継続的な可用性を確保するための既存の共有の設定 [414](#)
  - 継続的な可用性を実装したSMB共有の作成のために収集する情報 [401](#)
  - 構成, ボリュームを作成するために収集する情報 [400](#)
  - 構成時のネットワークおよびデータLIF要件 [393](#)
  - 構成の管理に関する情報 [413](#)
  - サポートされるノンストップ オペレーション [382](#)
  - システム ヘルスモニタを使用したノンストップ オペレーションのステータスの確認方法 [420](#)
  - スタンドアロン構成とクラスタ構成のサポート [382](#)
  - 設定, 継続的可用性を備えた共有の作成 [411](#)
  - 設定計画タスクの概要 [400](#)
  - 設定時のCIFSサーバの要件 [394](#)
  - 設定時のData ONTAPとライセンスの要件 [392](#)
  - 設定する際のボリューム要件 [394](#)
  - 設定するときの要件と考慮事項 [397](#)
  - 設定する必要がある内容 [382](#)
  - 設定要件と考慮事項についての情報 [392](#)
  - ソリューション, SMB 3.0の機能がサポートする仕組み [385](#)
  - 統計を使用したSMBアクティビティの監視についての情報 [418](#)
  - ドメイン アカウントがデフォルトのUNIXユーザにマッピングされていることの確認 [405](#)
  - ノンストップ オペレーション, 定義 [382](#)
  - ノンストップ オペレーション機能を提供するプロトコル [383](#)
  - ノンストップ オペレーション用の設定, リバート時の考慮事項 [417](#)
  - ノンストップ オペレーションを実現するData ONTAPの設定作成の概要 [403](#)
  - ノンストップ オペレーションを設定する際の推奨事項 [399](#)
  - ルート ボリュームがNTFSセキュリティ形式に設定されていることの確認 [407](#)
- SSL
  - SVMのIDが保持されない設定でFPolicyのセキュリティ証明書がレプリケートされない [481](#)
- SSL/TLS経由のLDAP
  - Data ONTAPでのLDAP通信の保護方法の概要 [97](#)
  - SVMでの自己署名ルートCA証明書のインストール [100](#)
  - 通信を保護するための設定および使用法の概要 [97](#)
- SSL証明書
  - FPolicy外部エンジン接続の設定に関する追加情報 [481](#)
- SSLセキュリティ
  - MetroClusterおよびSVMディザスタリカバリを搭載したクラスタ対象FPolicy外部エンジンの認証方式を選択する際の制限事項 [482](#)
- SVM
  - Active Directory LDAPサーバおよびドメイン コントローラのリセットと再検出 [33](#)
  - Active Directoryコンピュータ アカウントとCIFSサーバのどちらを作成するかを選択する方法 [26, 36](#)
  - Active Directoryコンピュータ アカウントに関する情報の表示 [30](#)
  - Active Directoryコンピュータ アカウントの削除 [30](#)
  - Active Directoryコンピュータ アカウントの作成 (CIFSライセンスなし) [27](#)
  - Active Directoryコンピュータ アカウントの設定と管理 (CIFSライセンスなし) [26](#)
  - Active Directoryコンピュータ アカウントの優先ドメイン コントローラに関する情報の表示 [35](#)
  - Active Directoryドメインへの参加 [141](#)
  - Active Directoryコンピュータ アカウントの優先ドメイン コントローラの追加または削除 [34](#)
  - BranchCache/ハッシュ ストアの場所を選択する際の考慮事項 [347](#)
  - CIFSサーバ, 作成前に収集する情報 [42](#)
  - CIFSサーバでサポートされるGPO [116](#)
  - CIFSサーバのIPspaceの作成 [52](#)
  - CIFSサーバのセットアップの主な手順 [50](#)
  - CIFSサーバの停止と起動 [139](#)
  - CIFSサーバの優先ドメイン コントローラの追加 [133](#)
  - CIFSサーバへのGPOの適用 [115](#)
  - CIFSサーバ用のIPspaceのブロードキャストドメインの作成 [56, 58](#)
  - CIFSサーバ用のLIFの作成 [61](#)
  - CIFSサーバ用の作成 [59](#)
  - CIFSサーバを作成する前に収集する情報 [49](#)
  - CIFSサーバを別のドメインに移動する前の動的DNSの設定 [140](#)
  - CLIを使用したNTFSファイル セキュリティと監査ポリシーの管理の概要 [257](#)

FPolicyによるポリシーの処理方法 [468](#)  
 FPolicyの実装での役割 [466](#)  
 FPolicyポリシーの作成 [499](#)  
 IDが保持されないディザスタリカバリ関係でセキュリティ証明書がレプリケートされない [481](#)  
 MMCを使用した接続とSMB共有の表示 [189](#)  
 NASファイル アクセス イベントの監査の概要 [432](#)  
 SMBアクセスのエクスポート ポリシー ルールの例 [213](#)  
 SSL/TLS経由のLDAP用のルートCA自己署名証明書のインストール [100](#)  
 監査を有効にしている場合のリバートのプロセス [463](#)  
 監査が有効なものがある場合のリバート前に実行する必要がある操作 [463](#)  
 監査設定の削除 [462](#)  
 監査設定を変更するコマンド [462](#)  
 監査の有効化 [450](#)  
 監査の有効化と無効化 [459](#)  
 検出されたActive DirectoryのLDAPサーバおよびドメイン コントローラに関する情報の表示 [32](#)  
 コピー オフロード用のODXの使用要件 [370](#)  
 削除時のSMB共有の動作 [175](#)  
 サポートされるSMB 1.0の機能 [105](#)  
 サポートされるSMB 2.0の機能 [105](#)  
 サポートされるSMB 2.1の機能 [106](#)  
 サポートされるSMB 3.0の機能 [107](#)  
 ステージング ボリュームに関するスペースの問題のトラブルシューティング方法 [464](#)  
 ディザスタリカバリ構成でのCIFSサーバセキュリティ設定に関する重要な考慮事項 [81](#)  
 データLIFの作成用に収集する情報 [44](#)  
 ネームスペースにおけるFPolicyサービスの仕組み [470](#)  
 ファイルおよびディレクトリ イベントの監査設定の作成 [448](#)  
 ファイルとディレクトリの監査設定の作成 [448](#)  
 ファイルを監視および管理するためのFPolicyの使用 [465](#)  
 複数のデータLIFを設定する場合の考慮事項 [89](#)  
 プロトコルの変更 [138](#)  
 別のOUへのCIFSサーバの移動 [140](#)  
 ルート ボリュームでのセキュリティ形式の設定 [149](#)

## T

### Twitter

マニュアルの変更に関する自動通知の受信方法 [512](#)

## U

### UNIX

mixed形式のボリュームのファイル セキュリティ、情報の表示 [250](#)  
 UNIXセキュリティ形式のボリュームのファイル セキュリティ情報の表示 [252](#)  
 セキュリティ形式のデータ、SMBクライアントへのNTFS ACLの提供の有効化と無効化 [78](#)  
 セキュリティ形式のデータ、SMBクライアントへのファイル セキュリティの提供方法の管理 [77](#)

### UNIX ID

Windows IDのマッピングの概要 [167](#)

### UNIXアクセス権

Data ONTAPによる維持方法 [78](#)

Windowsの[セキュリティ]タブを使用した管理方法 [78](#)

### UNIX権限

SMB経由でアクセス制御を行う場合 [199](#)

### UNIXシンボリックリンク

SMBアクセス用に設定する場合の制限 [340](#)

SMB共有のマッピングの作成 [343](#)

SMBクライアント アクセスの設定の概要 [338](#)

サポートの設定、SMB共有での [342](#)

### UNIXのユーザとグループ

SMB共有レベルACLの設定の使用の概要 [191](#)

### UNIXユーザ

デフォルトの設定 [101](#)

## V

### Vserver

次を参照 : SVM

### VSSシャドウ コピー

ディレクトリ階層の設定 [413](#)

有効化と無効化 [416](#)

## W

### Windows

ゲストUNIXユーザ アカウントの有効化と無効化 [102](#)

サポートされない機能 [37](#)

### Windows Administratorsグループ

ルートへのマッピング [103](#)

### Windows ID

UNIX IDへのマッピングの概要 [167](#)

### Windows管理者アクセス

ユーザのホーム ディレクトリへの有効化と無効化 [337](#)

### Windowsクライアント

BranchCacheの設定に関する情報の参照先 [351](#)

SMB署名ポリシーがSMB通信に与える影響 [87](#)

### Windowsグループ

ローカルの削除 [237](#)

### Windowsの[セキュリティ]タブ

UNIXアクセス権の管理方法 [78](#)

### Windowsのユーザとグループ

SMB共有レベルACLの設定の使用の概要 [191](#)

### Windowsユーザ アカウント

ローカルの作成 [226](#)

## X

### XML

サポートされる監査イベント ログのファイル形式 [436](#)

ファイル形式、監査イベント ログの表示 [436](#)

## あ

### アーキテクチャ

一般的なNASネームスペース [16](#)

## アカウント

CIFSサーバのドメイン パスワードの変更またはリセット [130](#)

## アクセス

SMBで認証が果たす役割 [22](#)

## アクセス制御エントリ

次を参照: ACE

## アクセス制御リスト

次を参照: ACL

## アクセス制限

CIFS匿名 (null) ユーザに対する設定 [76](#)

## アクセス チェック

セキュリティトレース, 監視される種類 [291](#)

## アクセストークン

ユーザ, 構成方法 [218](#)

## アクセススペースの列挙

SMB共有での有効化と無効化 [380](#)

Windowsクライアントからの有効化と無効化 [381](#)

共有のフォルダのセキュリティ確保の概要 [379](#)

## アグリゲート

有効な監査サブシステムによってステージング ボリュームが作成される場合のスペースに関する考慮事項 [435](#)

## アップグレード

FPolicyパススルー リード機能に関する考慮事項 [474](#)

後に静的ホーム ディレクトリ共有名が受ける影響 [330](#)

後のSMBアクセスのエクスポート ポリシーの扱い [210](#)

## 暗号化されたSMBセッション

クライアントが使用して接続しているかどうかの確認 [96](#)

## アンマウント

NASネームスペースのボリューム [152](#)

## い

## 以前のバージョン

Snapshotコピーが使用できるかどうかの確認 [325](#)

アクセスを有効にするSnapshot設定の作成 [326](#)

ジャンクションがあるフォルダをリストアする場合の考慮事項 [326](#)

使用するための要件 [323](#)

ファイルとフォルダのリカバリ, Microsoftの機能 [323](#)

## [以前のバージョン]タブ

Snapshotコピー データの表示と管理に使用 [324](#)

## 一覧

CIFSサーバ オプション [71](#)

サポートされる権限 [220](#)

## 移動

CIFSサーバを別のドメインへ, コマンド [142](#)

## 移動プロファイル

使用するための要件 [320](#)

設定 [320](#)

ユーザ プロファイルを格納する利点 [319](#)

## イベント

FPolicyでNFSv3を監視するために、サポートされるファイル処理とフィルタの組み合わせ [487](#)

FPolicyでNFSv4を監視するために、サポートされるファイル処理とフィルタの組み合わせ [487](#)

FPolicyでSMBを監視するために、サポートされるフ

ァイル処理とフィルタの組み合わせ [486](#)

FPolicyに関する情報を表示するコマンド [503](#)

FPolicyの作成 [498](#)

FPolicyの設定用に収集する情報 [488](#)

FPolicyのための設定の計画 [483](#)

FPolicyの変更用コマンド [502](#)

SMB, 監査できる [438](#)

ファイルおよびディレクトリの監査設定の作成 [448](#)

## イベントビューア

使用したアクティブな監査ログの表示方法 [437](#)

## イベント ログ

監査でサポートされるファイル形式 [436](#)

監査の手動ローテーション [459](#)

監査の表示 [436](#)

## イベント ログの形式

EVTXファイル形式のサポート [436](#)

XMLファイル形式のサポート [436](#)

## インストール

SVM上の自己署名ルートCA証明書 [100](#)

## う

## 上書き

権限の表示 [242](#)

## え

## 永続性ハンドル

サポートされるSMB 2.0の機能 [105](#)

サポートされるSMB 2.1の機能 [106](#)

## エイリアス

NetBIOS, CIFSサーバ上での管理の概要 [134](#)

NetBIOSのリストの表示, CIFSサーバ [136](#)

クライアントがNetBIOSを使用して接続しているかどうかの確認 [137](#)

特定のNetBIOSを使用して接続しているクライアントの確認 [137](#)

## エクスポート

自己署名ルートCA証明書のコピー [99](#)

## エクスポート ポリシー

SMBアクセスでの使用方法 [209](#)

SMBアクセスでの役割 [25](#)

SMBアクセスに関する有効化と無効化 [210](#)

SMBアクセスのリバート時の考慮事項 [215](#)

SMBアクセスのルール of 例 [213](#)

SMBアクセス用, Data ONTAPのアップグレード後の対処方法 [210](#)

使用したSMBアクセスの保護の概要 [208](#)

## エクスポート ルール

機能 [212](#)

## エクスポートレベルのセキュリティ

アクセスを保護するために使用される仕組み [24](#)

## エラー

クライアント アクセス エラーにつながるステージング ボリュームのスペースに関する問題のトラブルシューティング方法 [464](#)

## エラー メッセージ

No space left on device [464](#)



## お

### 大文字と小文字の区別

- マルチプロトコル環境でのファイル名とディレクトリ名 [147](#)
- マルチプロトコル環境での共有パスのディレクトリ名 [178](#)

### オブジェクト

- 統計, 使用可能な要素の確認 [311](#), [418](#)

### オプション

- CIFSサーバ, DFS対応の自動通知の管理 [80](#), [341](#)  
次を参照: CIFSサーバ オプション

### オプション, CIFSサーバ

- 使用できるオプションの一覧 [71](#)

### オフライン ファイル

- FPolicyパススルー リードが有効になっている場合の読み取り要求の処理方法 [473](#)
  - SMB共有での設定 [317](#)
  - オフラインで使用するファイルのキャッシュに関する概要 [315](#)
  - コンピュータの管理MMCを使用した共有での設定 [318](#)
  - 使用するための要件 [316](#)
  - 導入時の考慮事項 [316](#)
- オフロード データ転送  
次を参照: ODX

## か

### 解釈

- セキュリティトレースの結果 [299](#)

### 解除

- ロック [305](#)

### 階層型ストレージ管理

- 次を参照: HSM

### 概念

- Data ONTAPでのSSL/TLS経由のLDAPを使用したLDAP通信の保護方法の概要 [97](#)
- Hyper-VおよびSQL Server over SMBでのノンストップ オペレーション [383](#)
- リモートVSS, 定義 [387](#)

### 外部FPolicyサーバ

- FPolicy設定を作成するときに使用する [471](#)
- FPolicyと外部FPolicyサーバとの連携 [467](#)
- 接続 [506](#)
- 接続に関する情報の表示 [506](#)
- 切断 [506](#)
- 設定タイプの定義 [470](#)
- 次を参照: FPolicyサーバ

### 外部エンジン

- FPolicyに関する情報を表示するコマンド [503](#)
- FPolicyの作成 [497](#)
- FPolicyの設定用に収集する情報 [482](#)
- FPolicyのための設定の計画 [476](#)
- FPolicyの変更用コマンド [502](#)

### 外部サーバ

- CIFSサーバが接続するときのIPv6の使用法 [145](#)

### 外部通信

- ノードのフェイルオーバー時のFPolicyによる処理方法 [469](#)

### 概要

- Data ONTAPにおけるSMBファイル アクセス [15](#)

### カウンタ

- SMB自動ノードリファラルの監視に使用 [377](#)
- 統計, 使用可能な要素の確認 [311](#), [418](#)

### 書き込みキャッシュ

- oplockを使用するときのデータ消失に関する考慮事項 [110](#)

### 監査

- Data ONTAP CLIを使用したNTFS監査ポリシーに関する情報の表示 [253](#), [457](#)
- Data ONTAPのプロセスの仕組み [433](#)
- NFSv4に関する情報の表示, ポリシー [255](#)
- NFSイベントの一覧 [442](#)
- NFSとSMBのファイルおよびフォルダ アクセスの概要 [432](#)
- NFS用の設定 [455](#)
- NTFS代替データストリームが設定されたファイルに関する考慮事項 [441](#)
- アグリゲートにステージング ボリュームを作成する方法 [435](#)
- イベントビューアを使用したアクティブな監査ログの表示方法 [437](#)
- イベント ログの統合 [433](#)
- イベント ログのローテーション [433](#)
- イベント ログ ボリュームのスペースに関する問題のトラブルシューティング方法 [463](#)
- 監査イベント ログの手動変換 [459](#)
- 監査イベント ログの表示 [436](#)
- 監査が有効なSVMがある場合のリポートのプロセス [463](#)
- 監査対象オブジェクトへの完全パスの決定 [440](#)
- 監査できるSMBイベント [438](#)
- サポートされる監査イベント ログの形式 [436](#)
- シンボリックリンクおよびハードリンクに関する考慮事項 [440](#)
- ステージング ファイル, ステージング ボリューム, 統合タスク, 変換タスク, 定義 [432](#)
- ステージング ボリュームのスペースに関する問題のトラブルシューティング方法 [464](#)
- ストレージレベルのアクセス保護を使用するボリュームまたはqtreeに関する情報の表示 [162](#)
- 設定に関する情報の表示 [461](#)
- 設定に関する要件と考慮事項 [435](#)
- 設定の確認 [450](#)
- 設定の計画 [443](#)
- 設定の削除 [462](#)
- 設定を変更するコマンド [462](#)
- 適用されるポリシーの確認 [286](#)
- 統計, 使用可能なカウンタとオブジェクトの確認 [311](#), [418](#)
- 統計の表示 [313](#)
- ノードが利用できない場合のイベント ログの統合 [433](#)
- ファイルおよびディレクトリ イベントの設定の作成 [448](#)
- ファイルとディレクトリの作成, 設定 [448](#)
- 部分的なイベント ログの統合 [433](#)
- SVMでの有効化 [450](#)
- SVMでの有効化と無効化 [459](#)
- 有効化または無効化するときの処理 [433](#)
- 有効にする際のアグリゲート スペースに関する考慮事項 [435](#)
- 有効になっていることの確認 [461](#)

- リポート前に監査が有効なSVMで実行する必要がある操作 [463](#)
- リポート前に実行する必要がある操作 [463](#)
- 監査イベント ログ
  - 手動ローテーション [459](#)
- 監査が有効なSVM
  - リポート前に実行する必要がある操作 [463](#)
- 監査の保証
  - Data ONTAPによる保証方法 [433](#)
- 監査ポリシー
  - Data ONTAP CLIを使用したNTFSに関する情報の表示 [253](#), [457](#)
  - NTFS, Data ONTAP CLIを使用した設定方法 [454](#)
  - NTFSファイルおよびフォルダに対する設定および適用タスク [275](#)
  - Windowsの[セキュリティ]タブを使用した設定 [451](#)
  - Windowsの[セキュリティ]タブを使用した表示 [455](#)
  - 作成 [268](#), [281](#)
  - 情報の表示の概要, FlexVol [246](#)
  - ジョブの監視 [273](#), [286](#)
  - タスクを追加する [269](#), [282](#)
  - 適用される内容の確認 [286](#)
  - ファイルおよびフォルダの設定の概要 [450](#)
- 監視
  - SMBアクティビティ [305](#)
  - SMB署名統計情報 [92](#)
  - Windowsクライアントを使用した自動ノードリファラール [379](#)
  - 従来のoplockおよびoplockリリース [113](#)
- 監視プロトコル
  - 仕組み [386](#)
  - 透過的なフェイルオーバーを強化する仕組み [385](#)
- 管理
  - SMB共有プロパティ, コマンド [190](#)
  - CIFSサーバ, コマンド [142](#)
  - SMB共有, コマンド [190](#)
  - SMB共有を使用したファイル アクセス [216](#)
  - SVM (CIFSライセンスなし) のActive Directoryコンピュータ アカウント [26](#)
  - 概要, CLIを使用したNTFSファイル セキュリティと監査ポリシー [257](#)
  - 概要, CLIを使用したストレージレベルのアクセス保護 [257](#)
  - シンボリック リンクのマッピング、コマンド [344](#)
  - ネーム マッピング, コマンド [169](#)
  - 優先ドメインコントローラ, コマンド [134](#)
  - ローカル グループ メンバーシップ [235](#)
- 管理共有
  - デフォルトの共有とは [176](#)
- 管理者アカウント
  - ローカルを使用する際の考慮事項 [221](#)

## き

- キー配布センター
  - 次を参照: KDC
- 起動
  - CIFSサーバ [139](#)
  - CIFSサーバ, コマンド [142](#)
- 機能
  - サポートされないWindowsの機能 [37](#)
- 基本概念

- Data ONTAPでのSSL/TLS経由のLDAPを使用したLDAP通信の保護方法の概要 [97](#)
- キャッシュ
  - SMBメタデータ, 仕組み [300](#)
  - SMBメタデータの有効化 [301](#)
  - SMBメタデータの有効期間の設定 [301](#)
  - オフライン ファイルによるファイルのキャッシュに関する概要 [315](#)
  - 提供するためのBranchCacheの設定, SMB共有用 [348](#)
  - メタデータ, SMB 1.0共有の設定の概要 [300](#)
- キャッシュ サーバ
  - BranchCacheの設定に関する情報の参照先 [351](#)
- 共有
  - Hyper-V over SMBの要件 [395](#)
  - Hyper-VおよびSQL Server over SMB構成を作成する際に収集する情報 [401](#)
  - SMBでのBranchCacheの無効化の概要 [363](#)
  - SMBでのBranchCacheの有効化の概要 [352](#)
  - SMBでのアクセススペースの列挙の有効化と無効化 [380](#)
  - SMBでのオフライン ファイル サポートの設定 [317](#)
  - SMBの作成時におけるoplockの有効化と無効化 [110](#)
  - SQL Server over SMBの要件 [397](#)
  - アクセススペースの列挙による保護の概要 [379](#)
  - アップグレード後に静的ホーム ディレクトリ共有名が受ける影響 [330](#)
  - オフライン ファイル サポートの設定 [318](#)
  - 既存のSMBでのoplockの有効化と無効化 [111](#)
  - 既存の設定, 継続的な可用性 [414](#)
  - 継続的可用性, Hyper-VおよびSQL Server over SMB構成用に作成 [411](#)
  - 継続的可用性用のNTFSデータ ボリュームの作成 [410](#)
  - 継続的な可用性, Hyper-VおよびSQL Serverの設定の確認 [422](#)
  - すべてのSMBでの自動BranchCacheキャッシュの停止 [365](#)
  - 単一のSMBでのBranchCacheの無効化 [364](#)
  - フォルダのセキュリティ確保の概要, アクセススペースの列挙を使用 [379](#)
  - ホーム ディレクトリの一意なユーザ名の要件 [330](#)
  - ホーム ディレクトリの追加 [328](#)
  - 次も参照: SMB共有
- 共有, SMB
  - 作成時に必要な情報 [179](#)
- 共有権限
  - SMB共有の作成時のデフォルト [175](#)
  - SMBの設定 [191](#)
- 共有ごとのキャッシュ
  - 提供するためのBranchCacheの設定, SMB共有用 [348](#)
- 共有設定
  - 作成時にSMB共有のカスタマイズに使用 [180](#)
- 共有パス
  - 実行権限の廃止 [178](#)
- 共有パス コンポーネント
  - ロックの処理に関するData ONTAPとWindowsの違い [303](#)
- 共有パラメータ
  - 作成時にSMB共有のカスタマイズに使用 [180](#)

## 共有プロパティ

BranchCache [353](#)SMBの管理用コマンド [190](#)既存のSMB共有の追加または削除 [187](#)作成時にSMB共有のカスタマイズに使用 [180](#)

## 共有ベースのバックアップ

リモートVSSによる仮想マシンのバックアップ [387](#)

## 共有名

静的ホーム ディレクトリ, アップグレード後に受ける影響 [330](#)

## 共有レベルACL

SMBの管理の概要 [191](#)

## 共有レベルのセキュリティ

アクセスを保護するために使用される仕組み [24](#)

## 許可

ローカル ユーザおよびローカル グループを使用 [216](#)

## く

## クライアント

SMB, サポート対象 [37](#)Windowsで移動プロファイルを使用するための要件 [320](#)Windowsでフォルダ リダイレクトを使用するための要件 [321](#)[以前のバージョン]をサポート [323](#)

## クライアント アクセス エラー

ステージング ボリュームのスペースに関する問題のトラブルシューティング方法 [464](#)

## クラスタ

FPolicyの実装での役割 [466](#)

## グループ

BUILTIN使用時の考慮事項 [221](#)CIFSサーバの削除, ローカルのオブジェクトに対する影響 [219](#)事前定義のローカルBUILTIN [222](#)ディレクトリのトラバース チェックのバイパスの禁止 [245](#)ローカルがある場合のリポートに関する考慮事項 [220](#)ローカルからのユーザの削除 [235](#)ローカル データベースでのドメイン オブジェクトの名前の更新 [238](#)ローカルに関する情報の表示 [234](#)ローカルの削除 [237](#)ローカルの作成 [232](#)ローカルの説明の変更 [233](#)ローカルの名前の変更 [233](#)ローカルのメンバーの一覧の表示 [236](#)ローカルのユーザ アクセス トークンの構成方法 [218](#)ローカルへのユーザの追加 [235](#)ローカルまたはドメインに対する権限の追加 [239](#)ローカルまたはドメインの権限の削除 [240](#)ローカルまたはドメインの権限のリセット [241](#)ローカルを含むSVM上でSnapMirrorを使用する際の考慮事項 [219](#)

## グループ, Windows Administrator

ルートへのマッピング [103](#)

## グループ ポリシー オブジェクト

次を参照: GPO

## グループ メンバーシップ

ローカル ユーザの表示 [230](#)

## け

## 計画

CIFSサーバの設定, 概要 [38](#)FPolicyイベントの設定 [483](#)FPolicy外部エンジンの設定 [476](#)FPolicy構成の概要 [476](#)FPolicyスコープの設定 [493](#)FPolicyポリシーの設定 [488](#)監査設定 [443](#)ノンストップ オペレーション用にHyper-VまたはSQL Server over SMBを設定するためのタスクの概要 [400](#)

## 継続的可用性を備えた共有

Hyper-V over SMBの要件 [395](#)Hyper-VおよびSQL Server over SMB構成の確認 [422](#)Hyper-VおよびSQL Server over SMB構成用に作成 [411](#)Hyper-VおよびSQL Server over SMB構成を作成する際に収集する情報 [401](#)NTFSデータ ボリュームの作成 [410](#)SQL Server over SMBの要件 [397](#)透過的なフェイルオーバーを行うための監視との連携 [385](#)

## 権限

Data ONTAPによるUNIXの維持方法 [78](#)SeChangeNotifyPrivilege, 削除によるユーザとグループに対するトラバース チェックのバイパスの禁止 [245](#)SeChangeNotifyPrivilege, トラバース チェックのバイパスの設定についての情報 [242](#)SeChangeNotifyPrivilege, トラバース チェックのバイパスを可能にするための追加 [244](#)SMB共有の設定 [191](#)UNIX, Windowsの[セキュリティ]タブを使用した管理方法 [78](#)上書きの表示 [242](#)サポートされるローカル権限 [220](#)事前定義のBUILTINグループのデフォルト [222](#)セキュリティ形式によるファイル権限に対する影響 [20](#)定義, ローカル [220](#)ローカルの割り当て方法 [221](#)ローカルまたはドメインのユーザまたはグループに対する追加 [239](#)ローカルまたはドメインのユーザやグループから削除 [240](#)ローカルまたはドメインのユーザやグループについてリセット [241](#)

## 権限付きデータ アクセス

FPolicyのためのスーパーユーザ クレデンシャルの付与とは [468](#)

## 検索パス

管理用コマンド [336](#)ホーム ディレクトリ, 追加 [330](#)

## 検出された信頼できるドメイン

情報の表示 [173](#)

## 検証

Hyper-V over SMB構成で自動ノード リファラールが無効になっていることの確認 [409](#)  
 Hyper-V over SMB構成でのKerberos認証とNTLMv2認証の許可 [404](#)  
 Hyper-V over SMB構成でのルート ボリュームのNTFSセキュリティ形式 [407](#)  
 Hyper-V over SMB構成用のCIFSサーバ オプションの設定 [408](#)  
 Hyper-VおよびSQL Server over SMB構成のLIFS テータス [424](#)  
 Hyper-VおよびSQL Server SMB共有構成の継続的な可用性の設定 [422](#)  
 SQL Server over SMB構成で自動ノード リファラールが無効になっていることの確認 [409](#)  
 SQL Server over SMB構成でのルート ボリュームのNTFSセキュリティ形式 [407](#)  
 SQL Server over SMBのNDOのCIFSサーバ オプションの設定 [408](#)  
 監査設定 [450, 461](#)  
 適用される監査ポリシー [286](#)  
 適用されるファイルおよびフォルダのセキュリティ [273](#)  
 デフォルトUNIXユーザへのHyper-VおよびSQL Serverドメイン アカウント マッピング [405](#)

## こ

### 交換

ネーム マッピング, コマンド [169](#)

### 更新

CIFSサーバでのGPOに対する実行方法 [121](#)  
 GPO失敗の対応 [121](#)  
 GPO設定の手動 [122](#)  
 ローカル データベースのドメイン ユーザおよびドメイン グループのオブジェクト [238](#)

### 構成

監査の計画 [443](#)

### SVM設定

クラスタを対象としたFPolicy外部エンジンの認証方式を選択する際の制限事項 [482](#)

### 構成, サブネット

CIFSサーバを作成する前に収集する情報 [39](#)

### 構成タイプ

FPolicy, 定義 [470](#)

### 考慮事項

BranchCacheのハッシュ ストアを選択する場合 [347](#)  
 BUILTINグループとローカル管理者アカウントを使用する場合 [221](#)  
 CIFSサーバでのSMB共有の命名 [177](#)  
 Hyper-V over SMB構成 [395](#)  
 Hyper-V over SMB構成を使用したりリモートVSS [398](#)  
 Hyper-V over SMB構成をリバートする場合 [417](#)  
 ODXを使用する場合 [371](#)  
 SMBアクセスのエクスポート ポリシーをリバートする場合 [215](#)  
 SMB自動ノード リファラール [374](#)  
 SQL Server over SMB構成 [397](#)  
 アグリゲート スペース, 監査を有効にする際のステージング ボリューム [435](#)  
 オフライン ファイルを導入する場合 [316](#)  
 監査設定 [435](#)

サポートしないバージョンのData ONTAPへリバートする場合のダイナミック アクセス制御 [207](#)  
 セキュリティトレースを作成する場合 [291](#)  
 セキュリティ ポリシー ジョブの変更時 [287](#)  
 リバート, ローカル ユーザとグループがある場合 [220](#)

### コピー オフロード

Hyper-V over SMBおよびSQL Server over SMB構成での使用方法 [390](#)  
 ODXを使用する場合の考慮事項 [371](#)  
 仕組み [369](#)  
 ユースケース [372](#)  
 次も参照: ODX

### コマンド

NTFS DACLのACEの管理 [288](#)  
 NTFS SACLのACEの管理 [288](#)  
 NTFSセキュリティ記述子の管理 [288](#)  
 SVMの監査の変更 [462](#)  
 管理、検索パス [336](#)  
 セキュリティ ポリシー ジョブの管理 [290](#)  
 セキュリティ ポリシー タスクの管理 [289](#)  
 セキュリティ ポリシーの管理 [289](#)  
 ネーム マッピングの管理用 [169](#)  
 ボリュームやqtreeでoplockを有効または無効にするための [112](#)

### コメント

マニュアルに関するフィードバックの送信方法 [512](#)

### コントローラ

CIFSサーバの優先ドメインの追加 [133](#)  
 コマンド、優先ドメインコントローラの管理用 [134](#)

### コンピュータ アカウント

Active Directory, CIFSサーバの代わりに作成するかどうかを選択する方法 [26, 36](#)  
 Active Directory, SVMの設定と管理 (CIFSライセンスなし) [26](#)  
 Active Directory, 管理の概要 [27](#)  
 Active Directoryで検出されたLDAPサーバおよびドメイン コントローラに関する情報の表示 [32](#)  
 Active Directoryの削除, SVM [30](#)  
 Active Directoryの作成 (CIFSライセンスなし) [27](#)  
 Active Directoryの優先ドメイン コントローラに関する情報の表示 [35](#)  
 Active Directory用のLDAPサーバおよびドメイン コントローラのリセットと再検出 [33](#)  
 Active Directory用のドメイン コントローラ接続の管理の概要 [32](#)  
 Active Directory用の優先ドメイン コントローラの追加または削除 [34](#)  
 CIFSサーバのパスワードの変更またはリセット [130](#)  
 Hyper-V over SMBソリューションのデフォルトUNIX ユーザへのマッピングの確認 [405](#)  
 SVM, Active Directoryに関する情報の表示 [30](#)  
 SVM, Active Directoryのパスワードの変更またはリセット [31](#)  
 SVMが関連付けられているActive Directoryドメインの変更 [28](#)  
 コンピュータ アカウント パスワード  
 CIFSサーバの変更の概要 [130](#)  
 自動変更の設定, CIFSサーバ [130](#)  
 自動変更の無効化, CIFSサーバ [131](#)  
 コンピュータの管理MMC



- 共有でのオフライン ファイル サポートの設定に使用 [318](#)
- コンポーネント
  - 共有パスのロックの処理に関するData ONTAPとWindowsの違い [303](#)

## さ

- サーバ
  - CIFS上のダイナミック アクセス制御でサポートされる機能とサポートされない機能 [201](#)
  - CIFSセットアップの前提条件 [37](#)
  - CIFSでのLDAP over SSL/TLSの有効化 [99](#)
  - CIFSのNetBIOSエイリアスのリストの表示 [136](#)
  - CIFSの管理用コマンド [142](#)
  - LDAPおよびドメイン コントローラのリセットと再検出 [132](#)
  - 検出されたLDAPおよびドメイン コントローラに関する情報の表示 [132](#)
- サーバ, CIFS
  - オプションの一覧 [71](#)
  - 設定の概要 [36](#)
- サーバ キー
  - BranchCacheの設定の指定 [348](#)
  - BranchCacheの変更 [357](#)
- サーバの設定, CIFS
  - 計画の概要 [38](#)
- サーバのセットアップ
  - CIFSについて確認しておく項目 [50](#)
- 再検出
  - Active Directory LDAPサーバおよびドメイン コントローラ [33](#)
  - LDAPサーバおよびドメイン コントローラ [132](#)
  - マルチドメイン ネーム マッピングの検索に使用する信頼できるドメイン [173](#)
- 最低限の認証セキュリティレベル
  - CIFSサーバの設定 [84](#)
  - LMCompatibilityLevel設定 [84](#)
- 削除
  - Active Directoryコンピュータ アカウント用の優先ドメイン コントローラ [34](#)
  - BranchCache設定, 動作 [367](#)
  - CIFSサーバ, コマンド [142](#)
  - CIFSサーバ用NetBIOSエイリアス, コマンド [142](#)
  - SMB共有, コマンド [190](#)
  - SVMのActive Directoryコンピュータ アカウント [30](#)
  - 監査設定 [462](#)
  - 既存のSMB共有からの共有プロパティ, コマンド [190](#)
  - 既存のSMB共有に対する共有プロパティ [187](#)
  - コマンド、優先ドメインコントローラ [134](#)
  - ストレージレベルのアクセス保護 [163](#)
  - すべてのセキュリティトレース レコード [299](#)
  - セキュリティトレース フィルタ [298](#)
  - セキュリティトレース レコード [298](#)
  - ネーム マッピング, コマンド [169](#)
  - マルチドメイン ネーム マッピングの検索に使用する信頼できるドメイン [174](#)
  - ローカル グループ [237](#)
  - ローカル グループからのユーザの [235](#)
  - ローカルまたはドメインのグループの権限 [240](#)
  - ローカル ユーザ アカウント [231](#)

## 作成

- %uを使用したホーム ディレクトリの設定 [333](#)
- %wと%dを使用したホーム ディレクトリの設定 [331](#)
- Active Directoryコンピュータ アカウント(CIFSライセンスなし) [27](#)
- BranchCacheが有効なSMB共有 [352](#)
- CIFSサーバ [65](#)
- CIFSサーバ, 概要 [36](#)
- CIFSサーバ, コマンド [142](#)
- CIFSサーバのSMB共有 [180](#)
- CIFSサーバ用のLIF [61](#)
- CIFSサーバをホストするためのSVM [59](#)
- FPolicyイベント [498](#)
- FPolicy外部エンジン [497](#)
- FPolicy構成 [496](#)
- FPolicyスコープ [500](#)
- FPolicyポリシー [499](#)
- Hyper-V over SMBまたはSQL Server over SMB用のData ONTAPの設定, 概要 [403](#)
- Hyper-VおよびSQL Server over SMB構成用の継続的可用性を備えた共有 [411](#)
- SMB共有, コマンド [190](#)
- SMB共有, 必要な情報 [179](#)
- SMB共有のACL [191](#)
- SMB共有のシンボリック リンク マッピング [343](#)
- 継続的可用性を備えた共有用のNTFSデータ ボリューム [410](#)
- セキュリティトレース フィルタ [293](#)
- ネームマッピング [168](#)
- ファイルおよびディレクトリ イベントの監査設定 [448](#)
- ファイルとディレクトリの監査設定 [448](#)
- フォースグループ設定を使用したSMB共有 [186](#)
- ローカル グループ [232](#)
- ローカル ユーザ アカウント [226](#)
- サブネット構成
  - CIFSサーバを作成する前に収集する情報 [39](#)
- サポート
  - SMBとCIFSサービスでのIPv6 [144](#)
- サポートされない機能
  - Windows [37](#)
- サポートするバージョン
  - BranchCacheの設定の変更 [355](#)
- サポート対象
  - GPO [116](#)
  - ローカル権限 [220](#)
- サポート対象のバージョン
  - BranchCacheの設定 [348](#)
  - FlexVolを備えたSVMのSMB [105](#)
  - Infinite Volumeを備えたSVMのSMB [105](#)

## し

- 自己署名ルートCA証明書
  - ASCIIテキストへの変換, コピー [99](#)
  - SVMでのインストール [100](#)
  - コピーのエクスポート [99](#)
- システム アクセス制御リスト
  - 次を参照: SACL
- システム ヘルスモニタ
  - Hyper-V over SMBおよびSQL Server over SMB構成のノンストップ オペレーションのステータスの確認方法 [420](#)

## 事前計算

BranchCacheハッシュ [358](#)

## 事前定義

BUILTINローカル グループ [222](#)

## 実行

セキュリティトレース, 概要 [292](#)

## 自動キャッシュ

提供するためのBranchCacheの設定, すべてのSMB共有用 [348](#)

## 自動ノード リファラール

Hyper-VおよびSQL Server over SMB構成で無効になっていることの確認 [409](#)SMBで応答時間を改善する方法 [373](#)SMBのサポート [376](#)SMBの有効化と無効化 [377](#)SMBを使用する際の考慮事項と要件 [374](#)Windowsクライアントを使用した監視方法 [379](#)統計カウンタによるSMBの監視 [377](#)

## シャドウ コピー セット

定義 [387](#)

## ジャンクション

以前のバージョンでのフォルダのリストアに関する考慮事項 [326](#)使用に関するルール [15](#)定義 [15](#)ボリューム, SMBおよびNFSネームスペースでの使用方法 [16](#)

## ジャンクション ポイント

横断時のSMB共有の実行権限に関する要件の廃止 [178](#)指定されていないボリュームの作成 [151](#)指定したボリュームの作成 [150](#)ボリューム, ネームスペースを作成するための使用方法 [15](#)ボリュームに関する情報の表示 [153](#)

## 集約型アクセス ポリシー

CIFSサーバ オブジェクトで使用する際の考慮事項 [202](#)CIFSサーバのデータへの安全なアクセスの設定 [204](#)使用したSMBアクセスの保護の概要 [200](#)情報の表示 [127](#)設定方法および使用方法の参照先 [208](#)

## 集約型アクセス ポリシーのステージング イベント

SMB, 監査できる [438](#)

## 集約型アクセス ポリシーの設定セクション

GPO用, 何も表示されない場合の対応 [121](#)

## 集約型アクセス ポリシー ルール

情報の表示 [128](#)

## 従来のoplock

SMBクライアント パフォーマンスの向上 [110](#)

## 手動ローテーション

監査イベント ログ [459](#)

## 使用

[以前のバージョン]タブを使用したSnapshotコピーデータの表示および管理 [324](#)オプションによるCIFSサーバのカスタマイズ [71](#)

## 情報

マニュアルの品質向上に関するフィードバックの送信方法 [512](#)

## 情報を収集する

CIFSサーバ作成用 [49](#)IPspace, ブロードキャストドメイン, サブネット構成 [39](#)SVM設定 [42](#)クラスタ タイム サービスの設定 [38](#)SVM上のデータLIF作成用 [44](#)ネーム サービスの設定用 [46](#)

## 証明書

自己署名ルートCAのコピーのエクスポートと変換 [99](#)自己署名ルートのインストール, SVM上 [100](#)

## ジョブ

セキュリティ ポリシー ジョブの監視 [273](#), [286](#)セキュリティ ポリシーの管理用コマンド [290](#)セキュリティ ポリシーの変更時の考慮事項 [287](#)

## 署名

SMB統計の監視 [92](#)

## 処理

Data ONTAPの監査の仕組み [433](#)

## シンボリックリンク

次を参照: シンボリック リンク

## シンボリック リンク

DFSの自動通知を制御する方法 [79](#), [340](#)SMBアクセス用に設定する場合の制限 [340](#)SMB共有のマッピングの作成 [343](#)SMBクライアントからのUNIXへのアクセス方法 [339](#)UNIXのサポートの設定, SMB共有での [342](#)監査する際の考慮事項 [440](#)

## シンボリック リンクのマッピング

管理用コマンド [344](#)

## 信頼できるドメイン

検出, ユーザ名マッピング用のマルチドメイン検索での使用方法 [170](#)検出された対象に関する情報の表示 [173](#)再検出, マルチドメイン ネーム マッピングの検索に使用 [173](#)優先リスト内の信頼できるドメインの追加、削除、または置換 [174](#)優先リストに関する情報の表示 [175](#)リスト内の信頼できるドメインの追加、削除、または置換 [174](#)リストに関する情報の表示 [175](#)

## 信頼できる優先ドメイン

ユーザ名マッピング用のマルチドメイン検索での使用方法 [170](#)

## す

随意アクセス制御リスト [194](#)

次も参照: NTFSファイル権限

## 推奨事項

BranchCacheの設定 [347](#)FPolicyのセットアップ [474](#)Hyper-V over SMB構成 [399](#)SMB署名の設定 [89](#)SQL Server over SMB構成 [399](#)

## スーパーユーザ クレデンシャル

FPolicyの権限付きデータ アクセスのための付与とは [468](#)

## スコープ

FPolicyに関する情報を表示するコマンド [503](#)FPolicyの作成 [500](#)

- FPolicyのための設定の計画 493
- FPolicyの変更用コマンド 502
- FPolicy用に収集する設定情報 496
- ステージング ファイル
  - 監査向けの定義 432
  - ボリュームに関するスペースの問題のトラブルシューティング方法 464
- ステージング ボリューム
  - 監査向けの定義 432
  - 監査を有効にする際のアグリゲート スペースに関する考慮事項 435
  - スペースに関する問題のトラブルシューティング方法 464
- ストレージレベルのアクセス保護
  - CLIを使用したファイル セキュリティと監査ポリシーの管理の概要 257
  - DACL ACEの追加 265
  - mixedセキュリティ形式のボリュームの監査設定に関する情報の表示 255
  - mixedセキュリティ形式のボリュームのファイル セキュリティの設定に関する情報の表示 250
  - mixedまたはNTFSセキュリティ形式のボリュームでの監査設定に関する情報の表示 253, 457
  - NTFSセキュリティ形式のボリュームのファイル セキュリティ設定に関する情報の表示 247
  - SACL ACEの追加 278
  - アクセスを保護するために使用される仕組み 24
  - 削除 163
  - 使用のユースケース 156
  - 情報の表示の概要 246
  - 設定 157
  - 設定ワークフロー 156
  - 対象のセキュリティ記述子の作成 263, 276
  - タスクをセキュリティ ポリシーに追加する 269, 282
  - ファイルおよびフォルダへのアクセスの保護方法 154
  - ボリュームまたはqtreeのセキュリティ情報の表示 162
- スペースに関する問題
  - ステージング ボリュームのトラブルシューティング方法 464

## せ

- 制御チャネル
  - FPolicyでの使用方法 467
- 制限
  - SMBアクセス用にUNIXシンボリック リンクを設定する場合 340
  - ファイルおよびフォルダのセキュリティ設定でのCLIの使用 258
- 制限事項
  - MetroClusterおよびSVMディザスタリカバリを搭載したクラスタ対象FPolicy外部エンジンの認証方式の選択時 482
- セキュアなLDAP通信
  - CIFSサーバでのLDAP over SSL/TLSの有効化 99
- セキュリティ
  - CLIを使用してファイルおよびフォルダについて設定するユースケース 258
  - ストレージレベルのアクセス保護の削除 163

- ストレージレベルのアクセス保護の使用のユースケース 156
- ストレージレベルのアクセス保護の設定 157
- ストレージレベルのアクセス保護を使用した、ファイルおよびフォルダへのアクセスの保護方法 154
- セキュリティトレースの仕組み 290
- ダイナミック アクセス制御, 情報の表示 206
- 適用されるファイルおよびフォルダの確認 273
- ファイルおよびフォルダの設定でのCLIの使用に関する制限事項 258
- ファイルおよびフォルダへのアクセスを保護するために使用される3つのレベル 24
- セキュリティ記述子
  - DACL ACEの追加 265
  - NTFSの管理用コマンド 288
  - NTFSの作成 263, 276
  - SACL ACEの追加 278
  - ファイルおよびフォルダのセキュリティを適用するための使用方法 259
- セキュリティ形式
  - FlexVolでの設定 149
  - mixed形式のボリュームのファイル セキュリティ情報の表示 250
  - NTFSセキュリティ形式のボリュームのファイル セキュリティ情報の表示 247
  - qtreeでの設定 149
  - SVMルート ボリュームでの設定 149
  - UNIX, SMB経由でのUNIXファイル権限によるアクセス制御方法 199
  - UNIXセキュリティ形式のボリュームのファイル セキュリティ情報の表示 252
  - 共有を含んでいるボリュームまたはqtree 191
  - 継承の仕組み 21
  - 設定のタイミングと場所 21
  - 選択方法 21
  - データ, UNIX|に対するファイル セキュリティのSMBクライアントへの提供方法の管理 77
  - データ アクセスに対する影響の概要 20
  - ファイル権限に対する影響 20
- セキュリティ証明書
  - FPolicyのセキュリティ証明書, SVMのIDが保持されない設定でレプリケートされない 481
- セキュリティ設定
  - CIFSサーバ上での管理の概要 81
  - CIFSサーバ上のSVMディザスタリカバリ構成, 重要な考慮事項 81
  - CIFSサーバに関する情報の表示 81
  - CIFSサーバのKerberosの変更 83
  - クライアントが暗号化されたSMBセッションを使用して接続しているかどうかの確認 96
  - 必要な要素を使用してSMBセッションが接続されているかどうかの確認 91
- [セキュリティ]タブ
  - Windowsを使用したUNIXアクセス権の管理方法 78
- セキュリティトレース
  - 作成時の考慮事項 291
  - 監視されるアクセス チェックの種類 291
  - 結果, 解釈方法 299
  - 仕組み 290
  - 実行の概要 292

ファイルおよびディレクトリのアクセスの検証または  
トラブルシューティングの概要 [290](#)

セキュリティトレースの結果  
表示 [295](#)

セキュリティトレース フィルタ  
削除 [298](#)  
作成 [293](#)  
表示 [295](#)  
変更 [297](#)

セキュリティトレース レコード  
削除 [298](#)  
すべて削除 [299](#)

セキュリティ ポリシー  
FlexVolを備えたSVMへの適用 [272, 285](#)  
管理用コマンド [289](#)  
作成 [268, 281](#)  
ジョブの監視 [273, 286](#)  
タスクを追加する [269, 282](#)

セキュリティ ポリシー ジョブ  
管理時の考慮事項 [287](#)  
管理用コマンド [290](#)

セキュリティ ポリシー タスク  
管理用コマンド [289](#)

セキュリティ レベル  
CIFSサーバのLMCompatibilityLevelの設定 [84](#)  
CIFSサーバの最低限の認証の設定 [84](#)

セッション  
SMBに関する情報の表示 [306, 425](#)  
SMBを介して接続しているユーザのタイプに関する  
情報の表示 [104](#)

接続  
FPolicy外部エンジンのSSL認証を使用する際の追  
加情報 [481](#)  
外部FPolicyサーバ [506](#)

接続クレデンシャル  
FPolicy, 権限付きデータ アクセス チャンネルでの使  
用方法 [467](#)

絶対シンボリック リンク  
SMB共有用の作成 [343](#)  
SMBクライアントからのUNIXへのアクセス方法  
[339](#)

切断  
外部FPolicyサーバから [506](#)

設定  
%uを使用したホーム ディレクトリ [333](#)  
%wと%dを使用したホーム ディレクトリ [331](#)  
CIFSサーバ, 概要 [36](#)  
CIFSサーバオプション [71, 75](#)  
CIFSサーバ作成前のタイム サービス [52](#)  
CIFSサーバのBranchCache [348](#)  
Data ONTAP CLIを使用したNTFSファイル権限, 方  
法 [199](#)  
SVM用のDNSサービス [63](#)  
FlexVolでのセキュリティ形式 [149](#)  
FPolicy [496](#)  
LDAP over SSL/TLS, タスク [98](#)  
NFSの監査 [455](#)  
NTFSファイルおよびフォルダに対する監査ポリシ  
ー, タスク [275](#)  
NTFSファイルおよびフォルダに対するファイル セ  
キュリティ, タスク [261](#)  
qtreeでのセキュリティ形式 [149](#)

SMB共有でのUNIXシンボリック リンク サポート  
[342](#)

SMB共有でのオフライン ファイル サポート [317](#)

SMB共有のACL [191](#)

SMBメタデータ キャッシュ エントリの有効期間 [301](#)

SVM上のNISまたはLDAPネーム サービス [68](#)

SVMでの動的DNS [65](#)

SVM(CIFSライセンスなし)のActive Directoryコン  
ピュータ アカウント [26](#)

SVMルート ボリュームでのセキュリティ形式 [149](#)

VSSシャドウ コピーのディレクトリ階層 [413](#)

Windowsの[セキュリティ]タブを使用した監査ポリシ  
ー [451](#)

Windowsの[セキュリティ]タブを使用した詳細な  
NTFSファイルやフォルダの権限 [196](#)

Windowsの[セキュリティ]タブを使用した標準の  
NTFSファイル権限 [194](#)

移動プロファイル [320](#)

コンピュータの管理MMCを使用した共有でのオフ  
ライン ファイル サポート [318](#)

デフォルトのUNIXユーザ [101](#)

ファイルおよびディレクトリ イベントの監査 [448](#)

フォルダ リダイレクト [321](#)

ホーム ディレクトリ, 追加 [336](#)

設定要件  
LIFファイル アクセス管理 [19](#)

設定ワークフロー  
ストレージレベルのアクセス保護 [156](#)

セットアップ  
CIFSサーバ, 概要 [36](#)  
CIFSサーバについて確認しておく項目 [50](#)  
CIFSサーバの前提条件 [37](#)  
LDAP over SSL/TLS, タスク [98](#)

前提条件  
BranchCacheの設定 [348](#)  
CIFSサーバのセットアップ [37](#)

## そ

相対シンボリック リンク  
SMB共有用の作成 [343](#)  
SMBクライアントからのUNIXへのアクセス方法  
[339](#)

挿入  
ネーム マッピング, コマンド [169](#)

## た

代替データ ストリーム  
NTFSによるファイルを監査する際の考慮事項 [441](#)

ダイナミック アクセス制御  
CIFSサーバ オブジェクトで使用する際の考慮事項  
[202](#)  
mixed形式のボリュームのセキュリティ, 情報の表  
示 [206](#)  
NTFS形式のボリュームのセキュリティ, 情報の表  
示 [206](#)  
サポートされる機能とサポートされない機能 [201](#)  
サポートしないバージョンのData ONTAPへリパト  
する場合の考慮事項 [207](#)  
集約型アクセス ポリシーの設定 [204](#)  
使用したSMBアクセスの保護の概要 [200](#)



- 設定方法および使用方法の参照先 [208](#)
- 無効な場合のダイナミック アクセス制御ACEを含むACLの管理 [204](#)
- 有効化と無効化 [203](#)
- タイム サービス
  - CIFSサーバ作成前の設定 [52](#)
  - クラスタの設定用に収集する情報 [38](#)
- タスク
  - 監査とファイル セキュリティ ポリシーを追加する [269](#), [282](#)
  - セキュリティ ポリシーの管理用コマンド [289](#)
- ち
- 置換
  - マルチドメイン ネーム マッピングの検索に使用する信頼できるドメイン [174](#)
- つ
- 追加
  - Active Directoryコンピュータ アカウント用の優先ドメイン コントローラ [34](#)
  - BranchCache SMB共有プロパティ [353](#)
  - CIFSサーバの優先ドメイン コントローラ [133](#)
  - CIFSサーバ用NetBIOSエイリアス, コマンド [142](#)
  - SQL Serverインストーラのユーザ アカウントへのSeSecurityPrivilege権限 [412](#)
  - 既存のSMB共有に対する共有プロパティ [187](#)
  - 既存のSMB共有への共有プロパティ, コマンド [190](#)
  - コマンド、優先ドメインコントローラ [134](#)
  - セキュリティ記述子に対するDACL ACE [265](#)
  - セキュリティ記述子に対するSACL ACE [278](#)
  - タスクをセキュリティ ポリシーに [269](#), [282](#)
  - ホーム ディレクトリ共有 [328](#)
  - ホーム ディレクトリ検索パス [330](#)
  - マルチドメイン ネーム マッピングの検索に使用する信頼できるドメイン [174](#)
  - ローカル グループへのユーザの [235](#)
  - ローカルまたはドメインのグループに対する権限 [239](#)
  - ローカルまたはドメインのユーザに対する権限 [239](#)
- て
- 提案
  - マニュアルに関するフィードバックの送信方法 [512](#)
- 定義
  - FPolicy [465](#)
  - SMB共有 [175](#)
  - ローカル権限 [220](#)
  - ローカル ユーザとグループ [216](#)
- SVMディザスタリカバリ
  - CIFSサーバのセキュリティ設定に関する重要な考慮事項 [81](#)
- ディザスタリカバリ
  - SVM, 設定でのCIFSサーバのセキュリティ設定に関する重要な考慮事項 [81](#)
  - SVMのIDが保持されない設定でFPolicyのセキュリティ証明書がレプリケートされない [481](#)
- SVMディザスタリカバリの設定
  - クラスタを対象としたFPolicy外部エンジンの認証方式を選択する際の制限事項 [482](#)
- 停止
  - CIFSサーバ [139](#)
  - CIFSサーバ, コマンド [142](#)
- ディレクトリ
  - 指定したユーザのホーム ディレクトリ パスに関する情報の表示 [337](#)
  - ホーム, 共有での一意なユーザ名の要件 [330](#)
- ディレクトリ イベント
  - 監査設定の作成 [448](#)
- ディレクトリ構造
  - リモートVSSで使用, 例 [388](#)
- ディレクトリのトラバース チェック
  - ユーザとグループに対するバイパスの禁止 [245](#)
- ディレクトリ名
  - clustered Data ONTAPで作成される仕組み [147](#)
  - NFSとSMBでの命名規則 [147](#)
  - 使用できる文字 [147](#)
  - マルチプロトコル環境で共有を作成する際の大文字と小文字の区別 [178](#)
  - マルチプロトコル環境での大文字と小文字の区別 [147](#)
- データLIF
  - FPolicy通信での制御チャネルの使用法 [467](#)
  - FPolicyによる移行とフェイルオーバーの処理方法 [469](#)
  - FPolicyの実装での役割 [466](#)
  - Hyper-V over SMBおよびSQL Server over SMB構成の要件 [393](#)
  - 複数でSMB署名の要求を変更する場合の考慮事項 [89](#)
- データ アクセス
  - セキュリティ形式による影響の概要 [20](#)
- データ アクセス チャネル
  - FPolicyでの権限付きの使用法 [467](#)
  - 権限付きでのFPolicy接続クレデンシャルの使用法 [467](#)
- データ ストリーム
  - NTFS代替によるファイルを監査する際の考慮事項 [441](#)
- データ ボリューム
  - NTFS, 継続的可用性を備えた共有用の作成 [410](#)
- 適用
  - NTFSファイルおよびフォルダに対する監査ポリシー, タスク [275](#)
  - NTFSファイルおよびフォルダに対するファイル セキュリティ, タスク [261](#)
- 適用されるセキュリティ
  - ファイルおよびフォルダの確認 [273](#)
- デスティネーションでローカル ユーザまたはグループ
  - を使用するファイルとディレクトリのポリシーを適用する際の考慮事項
  - SVMディザスタリカバリ [81](#), [260](#)
- デフォルトのUNIXユーザ
  - Hyper-VおよびSQL Serverドメイン アカウント マッピングの確認 [405](#)
  - 設定 [101](#)
- デフォルトの管理共有
  - 説明 [176](#)
- デフォルトの権限
  - 事前定義のBUILTINグループ [222](#)

## と

## 透過的なフェイルオーバー

監視プロトコルによって強化する仕組み 385

## 同期

FPolicyアプリケーション 466

FPolicy通知、定義 465

通信、権限付きデータ アクセス チャンネルの使用  
方法 467

## 統計

BranchCacheの表示 359

BranchCacheハッシュの表示 313

SMB署名の監視 92

SMBとCIFSの表示 313

SMBの表示 420

カウンタによるSMB自動ノードリファラルのアク  
ティビティの監視 377

監査の表示 313

使用可能なカウンタとオブジェクトの確認 311, 418

## 統合タスク

監査向けの定義 432

## 動作モード

BranchCacheの設定の変更 355

## 動的DNS

CIFSサーバを別のドメインに移動する前のSVM上  
の変更 140

SVMでの設定 65

## トークン

ODX 369

## 匿名ユーザ

CIFSのアクセス制限の設定 76

## ドメイン

SVMのActive Directoryへの参加 141

検出された信頼できる項目に関する情報の表示  
173

信頼できる優先リスト内の信頼できるドメインの追  
加、削除、または置換 174

信頼できる優先リストに関する情報の表示 175

信頼の再検出、マルチドメイン ネーム マッピングの  
検索に使用 173

## ドメイン、ブロードキャスト

CIFSサーバを作成する前に収集する情報 39

## ドメイン アカウント

CIFSサーバのパスワードの変更またはリセット 130

SQL Server over SMBソリューションのデフォルト

UNIXユーザへのマッピングの確認 405

## ドメイン コントローラ

Active Directoryのリセットと再検出 33

SMB, サポート対象 37

検出されたActive Directoryに関する情報の表示  
32

検出された対象に関する情報の表示 132

優先ドメインコントローラの管理用コマンド 134

優先に関する情報の表示、Active Directoryコンピュ  
ータアカウント 35

優先の追加 133

優先の追加または削除、Active Directoryコンピュ  
ータアカウント用 34

## ドメイン コントローラ接続

Active Directoryコンピュータ アカウント用、管理の  
概要 32

## トラバースするディレクトリ

ユーザとグループに対するバイパスの禁止 245

## トラバース チェックのバイパス

許可、SeChangeNotifyPrivilege権限の追加 244

設定についての情報 242

## トラブルシューティング

監査イベント ログ ボリュームのスペースに関する  
問題 463

ステージング ボリュームのスペースに関する問題  
464

## トレース

監視されるセキュリティ アクセス チェックの種類  
291

セキュリティ、結果の表示 295

セキュリティ、仕組み 290

セキュリティの結果の解釈方法 299

セキュリティの実行の概要 292

## トレース フィルタ

削除 298

作成 293

表示 295

変更 297

## トレース レコード

すべて削除 299

セキュリティの削除 298

## な

## 名前

clustered Data ONTAPでファイルとディレクトリが作  
成される仕組み 147

ファイルやディレクトリに使用できる文字 147

## 名前変更

ローカル グループ 233

ローカル ユーザ アカウント 227

## に

## 認証

Kerberos 22

KerberosおよびNTLMのサポート 22

NTLM 23

SMBアクセスの保護において果たす役割 22

SSLによるFPolicy外部エンジン接続を使用する際  
の追加情報 481

ローカル ユーザ、仕組み 218

ローカル ユーザおよびローカル グループを使用  
216

## 認証セキュリティレベル

CIFSサーバの最低限の設定 84

LMCompatibilityLevel設定 84

## ね

## ネイティブFPolicyサーバ

設定タイプの定義 470

## ネイティブFPolicyの設定

どのような場合に作成するか 471

## ネーム サービス

SVMでの設定 68

設定用に収集する情報 46

## ネーム サービス スイッチ

設定用に収集する情報 [46](#)

ネームスペース

- SVMにおけるFPolicyサービスの仕組み [470](#)
- NASアクセスでのボリューム ジャンクションの使用  
方法 [16](#)
- NASでのデータ ボリュームの作成と管理の概要  
[150](#)
- NAS内のボリュームのマウントまたはアンマウント  
[152](#)
- NASの一般的なアーキテクチャ [16](#)
- SMBアクセスに与える影響 [15](#)
- 定義 [15](#)

ネームマッピング

- UNIXユーザからWindowsユーザへのマルチドメイン検索 [170](#)
- 管理用コマンド [169](#)
- 作成 [168](#)

ネーム マッピング

- SMBアクセスでの使用方法 [23](#)
- 検索用、マルチドメインの設定の概要 [170](#)
- 作成の概要 [167](#)
- 仕組み [23](#)
- 信頼できるドメインの優先リスト内の信頼できるドメインの追加、削除、または置換 [174](#)
- デフォルトUNIXユーザへのHyper-VおよびSQL Serverドメイン アカウント マッピングの確認 [405](#)
- 変換ルール [167](#)
- マルチドメイン検索に使用される検出された信頼できるドメインに関する情報の表示 [173](#)
- マルチドメイン検索に使用する信頼できるドメインの再検出 [173](#)
- マルチドメイン検索の有効化と無効化 [172](#)
- マルチドメインの検索に使用する信頼できるドメインの優先リストに関する情報の表示 [175](#)

ネットワーク

- Hyper-V over SMBおよびSQL Server over SMB構成の要件 [393](#)

## の

ノード

- FPolicy対応の通信プロセス [468](#)
- Hyper-VおよびSQL Server over SMB構成のLIFステータスの確認 [424](#)
- フェイルオーバー時のFPolicyによる外部通信の実行方法 [469](#)

ノード リファラール

- SMB自動のサポート [376](#)
- SMB自動を使用する際の考慮事項と要件 [374](#)
- SMBでクライアントの応答時間を改善する方法 [373](#)

ノンストップ オペレーション

- Hyper-V over SMB, CIFSサーバとボリューム設定の要件 [393](#)
- Hyper-V over SMB, 概念 [383](#)
- Hyper-V over SMB, システム ヘルスモニタを使用したステータスの確認方法 [420](#)
- Hyper-V over SMB, 定義 [382](#)
- Hyper-V over SMBおよびSQL Server over SMB, SMBの機能がサポートする仕組み [385](#)
- Hyper-V over SMBおよびSQL Server over SMB構成の要件 [392](#)
- Hyper-V over SMB構成の要件と考慮事項 [395](#)

- Hyper-VおよびSQL Server over SMB, ヘルスモニタステータスの表示 [421](#)
- Hyper-VおよびSQL Server over SMB機能を提供するプロトコル [383](#)
- Hyper-VおよびSQL Server over SMBのCIFSサーバ オプションの確認 [408](#)
- Hyper-VおよびSQL Server over SMBの設定時のネットワークおよびデータLIF要件 [393](#)
- Hyper-VまたはSQL Server over SMB構成計画タスクの概要 [400](#)
- SQL Server over SMB, CIFSサーバとボリューム構成の要件 [394](#)
- SQL Server over SMB, 概念 [383](#)
- SQL Server over SMB, システム ヘルスモニタを使用したステータスの確認方法 [420](#)
- SQL Server over SMB, 定義 [382](#)
- SQL Server over SMB構成の要件と考慮事項 [397](#)
- SQL Serverのインストールに使用するユーザ アカウントへのSeSecurityPrivilege権限の追加 [412](#)
- サポートされるSMB 3.0の機能 [107](#)
- 設定が可能であることの確認の概要 [420](#)

## は

バージョン

- サポートされるBranchCache [345](#)

ハードリンク

- 監査する際の考慮事項 [440](#)

パス

- 監査対象オブジェクトでの決定 [440](#)
- 検索の管理用コマンド [336](#)

パス コンポーネント

- 共有のロックの処理に関するData ONTAPとWindowsの違い [303](#)

パススルー リード

- FPolicy, HSMのユーザビリティ向上方法 [472](#)
- FPolicy, アップグレードおよびリバートに関する考慮事項 [474](#)
- FPolicy, 有効になっている場合の読み取り要求の処理方法 [473](#)
- FPolicyの接続のステータスに関する情報の表示 [508](#)
- FPolicyポリシーの作成 [499](#)

パスワード

- CIFSサーバのコンピュータ アカウントの変更の概要 [130](#)
- CIFSサーバのドメイン アカウントの変更 [130](#)
- CIFSサーバのドメイン アカウントのリセット [130](#)
- SVM, Active Directoryコンピュータ アカウントの変更またはリセット [31](#)
- コンピュータ アカウント, 自動変更の設定, CIFSサーバ [130](#)
- コンピュータ アカウント, 自動変更の無効化, CIFSサーバ [131](#)
- ローカル ユーザに対する複雑さの要件の有効化と無効化 [82](#)
- ローカル ユーザのアカウントの変更 [229](#)
- ローカル ユーザの要件 [222](#)

パスワードの複雑さ

- ローカル ユーザに対する要件の有効化と無効化 [82](#)

パスワードの複雑さの要件

- ローカル ユーザに対する有効化と無効化 [82](#)
- バックアップ
  - Hyper-V over SMB共有でのVSSシャドウ コピーの有効化と無効化 [416](#)
  - 共有ベースのバックアップを実行するためのリモートVSSの使用 [387](#)
  - リモートVSS対応, Hyper-V over SMB構成とともに使用する場合の考慮事項 [398](#)
- ハッシュ
  - BranchCacheでの事前計算 [358](#)
  - BranchCacheハッシュ ストアからのフラッシュ [359](#)
  - Data ONTAPでBranchCacheが無効になる理由 [346](#)
- ハッシュ ストア
  - BranchCacheの最大サイズの設定 [348](#)
  - BranchCacheの場所を選択する際の考慮事項 [347](#)
- ハッシュ ストア ディレクトリの最大サイズ
  - BranchCacheの設定の変更 [355](#)
- ハッシュ ストア ディレクトリのパス
  - BranchCacheの設定の変更 [355](#)
- ハッシュ ストアのパス
  - BranchCacheの設定の指定 [348](#)
- ハッシュ ストアのボリュームサイズ
  - BranchCacheの設定の増加 [355](#)
- パフォーマンス
  - ODXによるリモート コピーのパフォーマンスの向上 [368](#)
  - oplockによるSMBクライアント パフォーマンスの向上 [110](#)
  - SMB署名 への影響 [88](#)
  - SMBの自動ノード リファラールでクライアントを改善する方法 [373](#)
- パブリック アクセス
  - ユーザのホーム ディレクトリへの有効化と無効化 [337](#)

## ひ

- ビット
  - Data ONTAPによる読み取り専用の処理方法 [302](#)
- 非同期
  - FPolicyアプリケーション [466](#)
  - FPolicy通知, 定義 [465](#)
- 表示
  - Active Directoryコンピュータ アカウントの優先ドメイン コントローラに関する情報 [35](#)
  - BranchCache設定に関する情報 [356](#)
  - BranchCache統計 [359](#)
  - BranchCacheハッシュの統計 [313](#)
  - CIFSサーバ, コマンド [142](#)
  - CIFSサーバに適用されているGPO設定およびActive Directoryで定義されているGPO設定に関する情報 [122](#)
  - CIFSサーバに適用されているかActive Directoryで定義されている集約型アクセス ポリシー [127](#)
  - CIFSサーバに適用されているかActive Directoryで定義されている集約型アクセス ポリシー ルール [128](#)
  - CIFSサーバに適用されている制限されたグループ およびActive Directoryで定義されている制限されたグループのGPOに関する詳細 [125](#)
  - CIFSサーバのセキュリティ設定情報 [81](#)
  - CIFSとSMBの統計 [313](#)
  - Data ONTAP CLIを使用したFlexVolのNTFS監査情報 [253, 457](#)
  - FlexVolのNFsv4監査情報 [255](#)
  - FlexVolの監査ポリシーの情報, 概要 [246](#)
  - FPolicy設定に関する情報 [503](#)
  - FPolicyの設定, showコマンドの仕組み [503](#)
  - FPolicyの設定情報, コマンド [503](#)
  - FPolicyパススルー リード接続のステータスに関する情報 [508](#)
  - FPolicyポリシーのステータスに関する情報 [504](#)
  - Hyper-V over SMBのヘルスマニタ ステータス [421](#)
  - IPv6 SMBセッション情報 [146](#)
  - Microsoft管理コンソールでのローカル ユーザとローカル グループ [219](#)
  - mixedセキュリティ形式のボリュームのファイル セキュリティ情報 [250](#)
  - NetBIOS over TCPの情報 [142](#)
  - NTFSおよびmixedセキュリティ形式のボリュームのダイナミック アクセス制御セキュリティの情報 [206](#)
  - NTFSセキュリティ形式のボリュームのファイル セキュリティ情報 [247](#)
  - SMBが開いているファイルに関する情報 [305](#)
  - SMB共有, コマンド [190](#)
  - SMBセッション情報 [305, 306, 425](#)
  - SMBセッションで開いているファイルの情報 [308, 428](#)
  - SMBセッションを介して接続しているユーザのタイプに関する情報 [104](#)
  - SMB統計 [420](#)
  - SMB統計情報 [305](#)
  - SQL Server over SMBのヘルスマニタ ステータス [421](#)
  - SVMのActive Directoryコンピュータ アカウントに関する情報 [30](#)
  - UNIXセキュリティ形式のボリュームのファイル セキュリティ情報 [252](#)
  - Windowsの[セキュリティ]タブを使用した監査ポリシーの情報 [455](#)
  - 外部FPolicyサーバへの接続に関する情報 [506](#)
  - 監査イベント ログ [436](#)
  - 監査設定に関する情報 [461](#)
  - 監査の統計 [313](#)
  - 既存のSMB共有の共有プロパティ, コマンド [190](#)
  - 継続的可用性を備えた保護に関する情報 [306, 425](#)
  - 権限の上書き [242](#)
  - 検出されたActive DirectoryのLDAPサーバおよびドメイン コントローラに関する情報 [32](#)
  - 検出されたLDAPおよびドメイン コントローラ サーバに関する情報 [132](#)
  - 検出された信頼できるドメインに関する情報 [173](#)
  - 検出された信頼できるドメインの順序に関する情報 [173](#)
  - コマンド、優先ドメインコントローラ [134](#)
  - 従来のoplockの状態およびoplockリリースの状態 [113](#)
  - 信頼できるドメインの優先リストに関する情報 [175](#)
  - セキュリティトレースの結果 [295](#)
  - セキュリティトレース フィルタ [295](#)
  - 定義および適用されているBranchCache GPOに関する情報 [362](#)
  - ネーム マッピング, コマンド [169](#)
  - 開いているSMBファイルの情報 [308, 428](#)



- ファイル セキュリティの情報, 概要 [246](#)
  - ボリューム マウント ポイントとジャンクション ポイントに関する情報 [153](#)
  - ボリュームまたはqtreeのストレージレベルのアクセス保護のファイル セキュリティ情報 [162](#)
  - 有効なFPolicyポリシーに関する情報 [505](#)
  - ユーザのホーム ディレクトリ パスに関する情報 [337](#)
  - ローカル グループに関する情報 [234](#)
  - ローカル グループのメンバー [236](#)
  - ローカル ユーザ アカウントに関する情報 [230](#)
  - ローカル ユーザのグループ メンバーシップ [230](#)
  - ロックに関する情報 [303](#)
  - 標準のエンジン
    - FPolicyポリシーで使用する場合のFPolicyスコープの要件 [492](#)
  - 開いているSMBファイル
    - 情報の表示 [305](#), [308](#), [428](#)
  - 開いているファイル
    - SMBに関する情報の表示 [308](#), [428](#)
- ## ふ
- ファイル
    - SMB共有でのオフラインのサポートの設定 [317](#)
    - オフラインで使用するファイルのキャッシュに関する概要 [315](#)
    - オフライン ファイルを使用するための要件 [316](#)
    - オフラインを導入する際の考慮事項 [316](#)
    - ステージングを含むボリュームに関するスペースの問題のトラブルシューティング方法 [464](#)
  - ファイル アクセス
    - 管理のためのLIF設定要件 [19](#)
  - ファイル アクセス イベント
    - 監視するためのFPolicyの使用 [465](#)
  - ファイル イベント
    - 監査設定の作成 [448](#)
  - ファイルおよびフォルダ アクセス
    - NFSおよびSMBの監査の概要 [432](#)
    - 保護するために使用される3つのレベルのセキュリティの仕組み [24](#)
  - ファイルおよびフォルダのアクセス イベント
    - SMB, 監査できる [438](#)
  - ファイルおよびフォルダのセキュリティ
    - CLIを使用して設定するユースケース [258](#)
    - セキュリティ記述子の使用方法 [259](#)
    - 設定でのCLIの使用に関する制限事項 [258](#)
  - ファイル監査ポリシー
    - 設定の概要 [450](#)
  - ファイル形式
    - XMLまたはEVTXによる監査イベント ログの表示 [436](#)
  - ファイル権限
    - NTFS, Windowsの[セキュリティ]タブを使用した詳細なファイルやフォルダの権限の設定 [196](#)
    - NTFS, Windowsの[セキュリティ]タブを使用した標準のファイルやフォルダの権限の設定 [194](#)
    - NTFSの設定方法, Data ONTAP CLIを使用 [199](#)
    - UNIX, SMB経由でアクセス制御を行う場合 [199](#)
    - 使用したSMBアクセスの保護の概要 [193](#)
    - セキュリティ形式による影響 [20](#)
  - ファイル処理
    - NFSv3 FPolicyイベントでサポートされるフィルタとの組み合わせ [487](#)
    - NFSv4 FPolicyイベントでサポートされるファイル処理とフィルタの組み合わせ [487](#)
    - SMB FPolicyイベントでサポートされるファイル処理とフィルタの組み合わせ [486](#)
  - ファイル セキュリティ
    - mixedセキュリティ形式のボリュームについての表示 [250](#)
    - NTFSセキュリティ記述子の作成 [263](#), [276](#)
    - NTFSファイルおよびフォルダに対する設定および適用タスク [261](#)
    - UNIXセキュリティ形式のボリュームについての表示 [252](#)
    - 情報, NTFSセキュリティ形式のボリュームについての表示 [247](#)
    - 情報の表示の概要 [246](#)
    - ストレージレベルのアクセス保護を使用するボリュームまたはqtreeに関する情報の表示 [162](#)
    - 適用される内容の確認 [273](#)
  - ファイル セキュリティ ポリシー
    - 作成 [268](#), [281](#)
    - ジョブの監視 [273](#), [286](#)
    - タスクを追加する [269](#), [282](#)
  - ファイル操作
    - セキュリティトレースの結果の表示 [295](#)
  - ファイルとディレクトリの監査
    - SVMでの設定の作成 [448](#)
  - ファイルとディレクトリのポリシー
    - SVMディザスタリカバリ デスティネーションに適用する際のローカル ユーザおよびグループの考慮事項 [260](#)
  - ファイルとフォルダ
    - 詳細なNTFSファイル権限の設定, Windowsの[セキュリティ]タブの使用 [196](#)
    - 標準のNTFSファイル権限の設定, Windowsの[セキュリティ]タブの使用 [194](#)
  - ファイルとフォルダのリカバリ
    - 以前のバージョン [323](#)
  - ファイルのキャッシュ
    - オフライン ファイルによるオフラインでの使用に関する概要 [315](#)
  - ファイル名
    - clustered Data ONTAPで作成される仕組み [147](#)
    - NFSとSMBでの命名規則 [147](#)
    - 使用できる文字 [147](#)
    - マルチプロトコル環境での大文字と小文字の区別 [147](#)
  - ファイル名変換
    - FlexVolでのSMBの文字マッピングの設定 [164](#)
    - NFSからSMBへの文字マッピングを管理するコマンド [166](#)
  - ファイルレベルとフォルダレベルのセキュリティ
    - アクセスを保護するために使用される仕組み [24](#)
  - ファイル ロック
    - 解除 [305](#)
    - 管理の概要 [302](#)
    - 情報の表示 [303](#)
    - プロトコル間, 説明 [302](#)
  - フィードバック
    - マニュアルに関するコメントの送信方法 [512](#)
  - フィルタ

NFSv3 FPolicyイベントでサポートされるファイル処理との組み合わせ [487](#)  
 NFSv4 FPolicyイベントでサポートされるファイル処理とフィルタの組み合わせ [487](#)  
 SMB FPolicyイベントでサポートされるファイル処理とフィルタの組み合わせ [486](#)  
 セキュリティトレースの作成 [293](#)  
 セキュリティトレースの表示 [295](#)

フェイルオーバー  
   ノードでのFPolicyによる外部通信の処理方法 [469](#)

フォースグループ  
   共有設定, 機能 [185](#)

フォースグループ設定  
   使用したSMB共有の作成 [186](#)

フォルダ監査ポリシー  
   設定の概要 [450](#)

フォルダ セキュリティ  
   適用される内容の確認 [273](#)

フォルダ リダイレクト  
   CIFSサーバへのデータの格納に関する概要 [320](#)  
   使用するための要件 [321](#)  
   設定 [321](#)

ブロードキャストドメイン  
   CIFSサーバが配置されるSVMを含むIPspace用に作成 [56](#), [58](#)  
   CIFSサーバのセットアップ, 新しいブロードキャストドメインに追加できるポートの確認 [53](#)  
   CIFSサーバを作成する前に収集する情報 [39](#)  
   既存, CIFSサーバのセットアップ用の新しいブロードキャストドメインへの追加前のポートの削除 [55](#)

プロトコル  
   BranchCacheのサポート要件 [345](#)  
   FPolicyで監視可能 [465](#)  
   Hyper-VおよびSQL Server over SMBのノンストップオペレーション機能の提供 [383](#)  
   監視の仕組み [386](#)  
   ファイルのロック, 説明 [302](#)  
   SVMの変更 [138](#)

プロファイル  
   移動の設定 [320](#)  
   移動プロファイルにユーザ プロファイルを格納する利点 [319](#)  
   移動プロファイルを使用するための要件 [320](#)

## へ

ベストプラクティス  
   FPolicyのセットアップ [474](#)

変換  
   自己署名ルートCA証明書のコピーをASCIIテキストへ [99](#)

変換タスク  
   監査向けの定義 [432](#)

変更  
   BranchCache構成 [355](#)  
   CIFSサーバ, コマンド [142](#)  
   CIFSサーバのKerberosセキュリティ設定 [83](#)  
   CIFSサーバ マシン アカウント用パスワード, コマンド [142](#)  
   FPolicyの設定用コマンド [502](#)  
   SMB共有, コマンド [190](#)

SVMコンピュータ アカウントが関連付けられているActive Directoryドメイン [28](#)  
 SVMのActive Directoryコンピュータ アカウントのパスワード [31](#)  
 監査設定, コマンド [462](#)  
 継続的な可用性を確保するための既存の共有 [414](#)  
 セキュリティトレース フィルタ [297](#)  
 ネーム マッピング パターン, コマンド [169](#)  
 SVMのプロトコル [138](#)  
 ローカル グループの説明 [233](#)  
 ローカル ユーザ アカウント [227](#)  
 ローカル ユーザのアカウント パスワード [229](#)  
 ローカル ユーザのフルネームや説明 [227](#)

## ほ

ポート  
   CIFSサーバのセットアップ用の新しいブロードキャストドメインへの追加前の既存のブロードキャストドメインからの削除 [55](#)

ホーム ディレクトリ  
   %uを使用した設定の作成 [333](#)  
   %wと%dを使用した設定の作成 [331](#)  
   clustered Data ONTAPにおける動的SMBの仕組み [327](#)  
   Windows管理者アクセスの有効化と無効化 [337](#)  
   アップグレード後に静的共有名が受ける影響 [330](#)  
   管理の概要 [327](#)  
   共有の一意なユーザ名の要件 [330](#)  
   検索パスの追加 [330](#)  
   指定したユーザのホーム ディレクトリ パスに関する情報の表示 [337](#)  
   その他のユーザ アクセス(パブリック アクセス)の有効化と無効化 [337](#)  
   追加の設定 [336](#)

ホーム ディレクトリ共有  
   追加 [328](#)

保存されないID  
   SVMのディザスタリカバリ構成でのCIFSサーバ セキュリティ設定に関する重要な考慮事項 [81](#)

ポリシー  
   FPolicy, 収集する設定情報 [493](#)  
   FPolicyに関する情報を表示するコマンド [503](#)  
   FPolicyによる複数のFPolicyの処理方法 [468](#)  
   FPolicyのための設定の計画 [488](#)  
   FPolicyの変更用コマンド [502](#)  
   FPolicyの有効化 [501](#)  
   FPolicyの有効化と無効化 [502](#)  
   FPolicyポリシーのステータスに関する情報の表示 [504](#)  
   エクスポートをリポートする際の考慮事項, SMBアクセス [215](#)  
   ジョブの監視, ファイルセキュリティおよび監査 [273](#), [286](#)  
   セキュリティ, FlexVolを備えたSVMへの適用 [272](#), [285](#)  
   セキュリティ, タスクの管理用コマンド [289](#)  
   セキュリティの管理用コマンド [289](#)  
   セキュリティの作成 [268](#), [281](#)  
   適用される監査の確認 [286](#)  
   ファイルおよびフォルダ監査設定の概要 [450](#)  
   有効なFPolicyに関する情報の表示 [505](#)

## ボリューム

FlexVolでのNFSからSMBへの文字マッピングを管理するコマンド [166](#)  
 FlexVolでのSMBファイル名の変換のための文字マッピングの設定 [164](#)  
 FlexVolでのセキュリティ形式の設定 [149](#)  
 FlexVolの監査ポリシーの情報の表示の概要 [246](#)  
 FlexVolのストレージレベルのアクセス保護に関する情報の表示の概要 [246](#)  
 Hyper-V over SMBの要件 [393](#)  
 Hyper-VおよびSQL Server over SMB構成を作成する際に収集する情報 [400](#)  
 InfiniteのSMBサポートに関する情報の参照先 [70](#)  
 mixedセキュリティ形式でのストレージレベルのアクセス保護の監査設定に関する情報の表示 [255](#)  
 mixedセキュリティ形式でのストレージレベルのアクセス保護のファイル セキュリティの設定に関する情報の表示 [250](#)  
 mixedセキュリティ形式でのファイル セキュリティ情報の表示 [250](#)  
 NASネームスペースでの作成と管理の概要 [150](#)  
 NASネームスペースに対するボリュームのマウントまたはアンマウント [152](#)  
 NTFS, 継続的可用性を備えた共有用の作成 [410](#)  
 NTFSおよびmixedセキュリティ形式でのダイナミック アクセス制御セキュリティ情報の表示 [206](#)  
 NTFSセキュリティ形式でのストレージレベルのアクセス保護のファイル セキュリティ設定に関する情報の表示 [247](#)  
 NTFSセキュリティ形式でのファイル セキュリティ情報の表示 [247](#)  
 NTFSまたはmixedセキュリティ形式のストレージレベルのアクセス保護の監査設定に関する情報の表示 [253](#), [457](#)  
 oplockを有効または無効にするためのコマンド [112](#)  
 oplockを有効または無効にできるタイミング [112](#)  
 SQL Server over SMBの要件 [394](#)  
 UNIXセキュリティ形式でのファイル セキュリティ情報の表示 [252](#)  
 ジャンクション ポイントを指定した作成 [150](#)  
 ジャンクション ポイントを指定しない作成 [151](#)  
 ジャンクション ポイントを使用したネームスペースの作成方法 [15](#)  
 ステージングで監査を有効にする際のアグリゲートスペースに関する考慮事項 [435](#)  
 ステージングに関するスペースの問題のトラブルシューティング方法 [464](#)  
 ストレージレベルのアクセス保護セキュリティのファイル セキュリティ情報の表示 [162](#)  
 ストレージレベルのアクセス保護の削除 [163](#)  
 ストレージレベルのアクセス保護の設定 [157](#)  
 ストレージレベルのアクセス保護を使用した、ファイルおよびフォルダへのアクセスの保護方法 [154](#)  
 ファイル セキュリティに関する情報の表示の概要 [246](#)  
 マウント ポイントとジャンクション ポイントに関する情報の表示 [153](#)  
 ルートへのアクセス時のSMB共有の実行権限に関する要件の廃止 [178](#)

## ボリューム ジャンクション

SMBアクセスに与える影響 [15](#)  
 SMBおよびNFSネームスペースでの使用方法 [16](#)

使用に関するルール [15](#)

定義 [15](#)

## ボリュームのルート

アクセス時のSMB共有の実行権限に関する要件の廃止 [178](#)

## ま

## マウント

NASネームスペースのボリューム [152](#)

## マッピング

シンボリック リンクの作成, SMB共有 [343](#)  
 ルートへのWindows Administratorsグループ [103](#)

## マニュアル

フィードバックの送信方法 [512](#)  
 変更に関する自動通知の受信方法 [512](#)

## マルチドメイン検索

ネーム マッピング, 設定の概要 [170](#)

## マルチドメイン ネーム マッピングの検索

検出された信頼できるドメインに関する情報の表示 [173](#)  
 使用する信頼できるドメインの再検出 [173](#)  
 信頼できるドメインの優先リスト内の信頼できるドメインの追加、削除、または置換 [174](#)  
 信頼できるドメインの優先リストに関する情報の表示 [175](#)  
 設定の概要 [170](#)  
 有効化と無効化 [172](#)

## む

## 無効化

BranchCache [366](#)  
 BranchCache, 動作 [365](#)  
 BranchCacheハッシュ, 理由 [346](#)  
 CIFSサーバ上での受信SMBトラフィックのSMB暗号化要求 [95](#)  
 CIFSサーバでKerberos通信に強固なセキュリティを設定するためのAES暗号化 [86](#)  
 FlexVolを備えたSVMでのSMB 2.x [108](#)  
 FlexVolを備えたSVMでのSMB 3.0 [109](#)  
 FPolicyポリシー [502](#)  
 GPOサポート [120](#)  
 ODX [373](#)  
 SMBアクセスに関するエクスポート ポリシー [210](#)  
 SMBアクセスに関するローカル ユーザ認証 [225](#)  
 SMB共有でのアクセススペースの列挙 [380](#)  
 SMB自動ノード リファラール [377](#)  
 SMB署名要求 [90](#)  
 VSSシャドウ コピー [416](#)  
 Windowsゲスト ユーザ アカウント [102](#)  
 SVMでの監査 [459](#)  
 ダイナミック アクセス制御 [203](#)  
 マルチドメイン ネーム マッピングの検索 [172](#)  
 ローカル ユーザ アカウント [227](#), [229](#)  
 ローカル ユーザとグループ [224](#)  
 ローカル ユーザに対するパスワードの複雑さの要件 [82](#)

## め

## メタデータのキャッシング

- SMB 1.0共有の設定の概要 300
- SMBでの仕組み 300
- SMBの有効化 301
- SMBの有効期間の設定 301

## も

## 文字マッピング

- FlexVolでのSMBファイル名の変換の有効化 164
- SMBファイル名変換の情報を作成、変更、削除、表示するコマンド 166

## ゆ

## 有効化

- BranchCache 366
  - CIFSサーバ上での受信SMBトラフィックのSMB暗号化要求 95
  - CIFSサーバでKerberos通信に強固なセキュリティを設定するためのAES暗号化 86
  - CIFSサーバでのLDAP over SSL/TLS 99
  - FlexVolを備えたSVMでのSMB 2.x 108
  - FlexVolを備えたSVMでのSMB 3.0 109
  - FPolicyポリシー 501, 502
  - GPOサポート 120
  - ODX 373
  - SMBアクセスに関するエクスポート ポリシー 210
  - SMBアクセスに関するローカル ユーザ認証 225
  - SMB共有でのアクセススペースの列挙 380
  - SMB自動ノード リファラル 377
  - SMB署名要求 90
  - SMBメタデータのキャッシング 301
  - SMB用のクラスタでのIPv6 146
  - VSSシャドウ コピー 416
  - Windowsゲスト ユーザ アカウント 102
  - SVMでの監査 459
  - SVMでの監査 450
  - すべてのSMB共有でのBranchCache自動キャッシング 348
  - ダイナミック アクセス制御 203
  - マルチドメイン ネーム マッピングの検索 172
  - ローカル ユーザ アカウント 227, 229
  - ローカル ユーザとグループ 224
  - ローカル ユーザに対するパスワードの複雑さの要件 82
- 有効なセキュリティ形式
- UNIX, SMB経由でのUNIXファイル権限によるアクセス制御方法 199
- ユーザ
- CIFSサーバの削除, ローカルのオブジェクトに対する影響 219
  - ディレクトリのトラバース チェックのバイパスの禁止 245
  - デフォルトUNIXの設定 101
  - ローカル, 認証の仕組み 218
  - ローカル, ローカル グループ メンバーシップに関する情報の表示 230
  - ローカル アカウントの削除 231
  - ローカル アカウントの作成 226

- ローカル アカウントの変更, 名前の変更, 有効化, 無効化 227
- ローカル アカウントの有効化と無効化 229
- ローカルがある場合のリバートに関する考慮事項 220
- ローカル データベースでのドメイン オブジェクトの名前の更新 238
- ローカルに関する情報の表示 230
- ローカルのアカウント パスワードの変更 229
- ローカルのアクセストークンの構成方法 218
- ローカルの場合のパスワードの要件 222
- ローカルまたはドメインに対する権限の追加 239
- ローカルまたはドメインの権限の削除 240
- ローカルまたはドメインの権限のリセット 241

## ユーザ アカウント

- ゲストUNIXアカウントの設定 102
- パスワードの変更 229
- ローカル, ローカル グループ メンバーシップに関する情報の表示 230
- ローカル アカウントの変更, 名前の変更, 有効化, 無効化 227
- ローカルに関する情報の表示 230
- ローカルの削除 231
- ローカルの作成 226
- ローカルの有効化と無効化 229

## ユーザ アクセストークン

- 構成方法 218

## ユーザとグループ

- Data ONTAPでのローカルの使用方法 216
- ローカル, 定義 216
- ローカル, 認証と許可に使用 216

## ユーザとグループ)

- WindowsとUNIX, SMB共有レベルACLの設定の使用の概要 191

## ユーザのタイプ

- SMBセッションを介した接続, 情報の表示 104

## ユーザのホーム ディレクトリ

- アクセスの有効化と無効化 337

## ユーザ マッピング

- デフォルトの設定の概要 100

## ユーザ名

- ホーム ディレクトリ共有での一意の要件 330
- マッピングの仕組み 23

## ユーザ名マッピング

- マルチドメイン検索で使用する信頼できる優先ドメイン 170

## ユースケース

- ODX 372
- ストレージレベルのアクセス保護の使用 156
- ファイルおよびフォルダのセキュリティ設定でのCLIの使用 258

## 優先度

- FPolicyによるFPolicyポリシーの処理方法 468

## 優先ドメイン コントローラ

- Active Directoryコンピュータ アカウント用の追加または削除 34
- 管理用コマンド 134
- 情報の表示, Active Directoryコンピュータ アカウント 35
- 追加 133



## よ

## 要件

- BranchCacheに対するData ONTAPのバージョン要件 [346](#)
- BranchCacheに対するWindowsホストのバージョン要件 [346](#)
- BranchCacheによるネットワーク プロトコルのサポート [345](#)
- BUILTINグループを使用する場合 [221](#)
- CIFSサーバ, Hyper-V over SMB構成用 [393](#)
- CIFSサーバ, SQL Server over SMB構成用 [394](#)
- CIFSサーバでのGPOの使用 [120](#)
- Data ONTAPとライセンス, Hyper-V over SMB構成 [392](#)
- Data ONTAPとライセンス, SQL Server over SMB構成 [392](#)
- FPolicyのセットアップ [473](#)
- FPolicyポリシーで標準のエンジンを使用する場合のFPolicyスコープの設定 [492](#)
- Hyper-V over SMB構成 [395](#)
- ODXを使用する場合 [370](#)
- SMB自動ノード リファール [374](#)
- SMBでのIPv6の使用 [143](#)
- SQL Server over SMB構成 [397](#)
- [以前のバージョン]の使用 [323](#)
- オフライン ファイルの使用 [316](#)
- 監査設定 [435](#)
- ネットワークおよびデータLIF, Hyper-V over SMB構成用 [393](#)
- ネットワークおよびデータLIF, SQL Server over SMB構成用 [393](#)
- フォルダ リダイレクトの使用 [321](#)
- ボリューム, Hyper-V over SMB構成 [393](#)
- ボリューム, SQL Server over SMB構成用 [394](#)

## 用語

SSL/TLS経由のLDAP [97](#)

## 読み取り専用ビット

Data ONTAPによる処理方法 [302](#)

## ら

## ライセンス

Hyper-V over SMBおよびSQL Server over SMB構成の要件 [392](#)

## り

## リストア

以前のバージョンでジャンクションがあるフォルダをリストアする場合の考慮事項 [326](#)

## リセット

- Active Directory LDAPサーバおよびドメイン コントローラ [33](#)
- CIFSサーバ マシン アカウント用パスワード, コマンド [142](#)
- LDAPサーバおよびドメイン コントローラ [132](#)
- SVMのActive Directoryコンピュータ アカウントのパスワード [31](#)
- ローカルまたはドメインのグループの権限 [241](#)
- ローカルまたはドメインのユーザの権限 [241](#)

## リセットと再検出

CIFSサーバ用サーバ, コマンド [142](#)

## リソース

KDC, SID圧縮のサポート [22](#)

## リダイレクト

フォルダ リダイレクトによるCIFSサーバへのデータの格納に関する概要 [320](#)

フォルダ リダイレクトを使用するための要件 [321](#)

## リバート

- BranchCacheの動作 [368](#)
- FPolicyパススルー リード機能に関する考慮事項 [474](#)
- 監査を有効にしたSVMがある場合のプロセス [463](#)
- ダイナミック アクセス制御をサポートしないバージョンのData ONTAPへ, 考慮事項 [207](#)
- ノンストップ オペレーション用に設定されたSQL Server over SMBの考慮事項 [417](#)

## リバートに関する考慮事項

Hyper-V over SMB構成 [417](#)

ローカル ユーザとグループが設定されている場合 [220](#)

## リファール

SMB自動ノードのサポート [376](#)

SMB自動ノードを使用する際の考慮事項と要件 [374](#)

## リモートVSS

- Hyper-V over SMB構成とともに使用する場合の考慮事項 [398](#)
- Hyper-V仮想マシンの共有ベースのバックアップに使用 [387](#)
- SnapManager for Hyper-Vを使用する場合のプロセス [389](#)
- 概念の定義 [387](#)
- 使用されるディレクトリ構造の例 [388](#)
- 定義 [387](#)
- バックアップ, SnapManager for Hyper-Vによる管理方法 [389](#)

## リモート オフィス

BranchCacheの設定に関する情報の参照先 [351](#)

## リンク

- SMBクライアントからのUNIXシンボリックへのアクセス方法 [339](#)
- UNIXシンボリックのサポートの設定, SMB共有での [342](#)
- UNIXシンボリックを設定する場合の制限, SMBアクセス用 [340](#)

## リンク マッピング

シンボリックの作成, SMB共有 [343](#)

## る

## ルートCA証明書

- ASCIIテキストへのコピーの変換, 自己署名 [99](#)
- SVMでのインストール [100](#)
- 自己署名のコピーのエクスポート [99](#)

## ルート ボリューム

- Hyper-V over SMB構成, NTFSセキュリティ形式の確認 [407](#)
- SQL Server over SMB構成, NTFSセキュリティ形式の確認 [407](#)
- SVMでのセキュリティ形式の設定 [149](#)

## ルール

エクスポート ポリシー, SMBアクセスの例 [213](#)

## れ

## 列挙

アクセスベース, Windowsクライアントからの有効化と無効化 [381](#)

## ろ

## ローカル管理者アカウント

使用時の考慮事項 [221](#)

## ローカル グループ

SVMでSnapMirrorを使用する際の考慮事項 [219](#)

削除 [237](#)

作成 [232](#)

作成する理由 [217](#)

事前定義のBUILTIN [222](#)

情報の表示 [234](#)

メンバーの一覧の表示 [236](#)

## ローカル権限

定義 [220](#)

割り当て方法 [221](#)

## ローカル ユーザ

アカウントの削除 [231](#)

アカウントの有効化と無効化 [229](#)

アカウント パスワードの変更 [229](#)

作成する理由 [217](#)

情報の表示 [230](#)

認証の仕組み [218](#)

パスワードの複雑さの要件の有効化と無効化 [82](#)

パスワードの要件 [222](#)

変更, 名前の変更, 有効化, 無効化 [227](#)

ローカル グループ メンバーシップに関する情報の表示 [230](#)

## ローカル ユーザとグループ

CIFSサーバの削除, 影響 [219](#)

Data ONTAPでの使用方法 [216](#)

Microsoft管理コンソールでの表示 [219](#)

作成する理由 [217](#)

設定されている場合のリポートに関する考慮事項 [220](#)

定義 [216](#)

認証と許可に使用 [216](#)

ファイルとディレクトリのポリシーを含む, SVMディザスタリカバリ デスティネーションに適用する際の考慮事項 [260](#)

有効化と無効化 [224](#)

用途 [216](#)

## ローカル ユーザとローカル グループ

ユーザ アクセストークンの構成方法 [218](#)

## ローカル ユーザ認証

SMBアクセスに関する有効化と無効化 [225](#)

## ローカル リンク

SMBクライアントからのUNIXシンボリック リンクへのアクセス方法 [339](#)

## ローテーション

監査イベント ログ, 手動 [459](#)

## ログ

監査ログの手動ローテーション [459](#)

## ログオンおよびログオフ イベント

SMB, 監査できる [438](#)

## ロック

解除 [305](#)

情報の表示 [303](#)

処理に関するData ONTAPとWindowsの違い, 共有パス コンポーネント [303](#)

## わ

## ワークシート

FPolicyイベントの設定に必要な情報の記録 [488](#)

FPolicy外部エンジンの設定に必要な情報の記録 [482](#)

FPolicyスコープの設定に必要な情報の記録 [496](#)

FPolicyポリシーの設定に必要な情報の記録 [493](#)

## ワークフロー

ストレージレベルのアクセス保護設定 [156](#)

## ワイドリンク

SMBクライアントからのUNIXシンボリック リンクへのアクセス方法 [339](#)

使用したSMBクライアント アクセスの設定の概要 [338](#)

## 割り当て

ローカル権限, 方法 [221](#)