clustered Data ONTAP® 8.3

ファイル アクセス管理ガイド（NFS）

2015年6月 | 215-10728_A0
ng-gpso-jp-documents@netapp.com

8.3.1用に更新

NetApp®

目次

ファイル アクセスを設定する際の考慮事項 10
Data ONTAPでサポートされるファイル プロトコル 10
Data ONTAPによるファイル アクセスの制御方法 10
認証ベースの制限 10
ファイルベースの制限 11
ファイル アクセス管理のためのLIF設定要件 11
FlexVolを備えたSVMでネームスペースとボリューム ジャンクションがファイル アクセスに与える影響 11
FlexVolを備えたSVMのネームスペースとは 11
ボリューム ジャンクションの使用に関するルール 12
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 12
一般的なNASネームスペース アーキテクチャとは 12
NASネームスペースでのデータ ボリュームの作成と管理 15
ジャンクション ポイントを指定したボリュームの作成 15
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 16
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 17
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 18
セキュリティ形式がデータ アクセスに与える影響 19
セキュリティ形式とその影響とは 19
セキュリティ形式を設定する場所とタイミング 20
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
Data ONTAPによるUNIXアクセス権の維持方法 21
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 22
セキュリティ形式の設定 22
SVMルート ボリュームでのセキュリティ形式の設定 23
FlexVolでのセキュリティ形式の設定 23
qtreeでのセキュリティ形式の設定 23
NFSとCIFSのファイルの命名規則について 24
ファイル名に使用できる文字 24
ファイル名での大文字と小文字の区別 24
Data ONTAPでのファイル名の作成方法 25
Data ONTAPでのUTF-16の追加文字を含むファイル名の処理方法 25
ハード マウントの使用 25
Data ONTAPでのNFSを使用したファイル アクセスのサポート方法 26
Data ONTAPによるNFSクライアント認証の処理 26
Data ONTAPでのネーム サービスの使用方法 26
Data ONTAPによるNFSクライアントからのCIFSファイル アクセスの許可方法 27

サポートされるNFSバージョンおよびクライアント 27
Data ONTAPでサポートされるNFSv4.0の機能 28
NFSv4のData ONTAPサポートの制限 28
NFSv4.1のData ONTAPサポート 29
Parallel NFSのData ONTAPサポート 29
Infinite VolumeでのNFSサポートに関する情報の参照先 29
FlexVolを備えたSVMでのUNIXセキュリティ形式データへのNFSアクセス プロセス 30
FlexVolを備えたSVMでのNTFSセキュリティ形式データへのNFSアクセス プロセス 30
NFSを使用したファイル アクセスの設定 32
SVMのプロトコルの変更 32
NFSサーバの作成 33
エクスポート ポリシーを使用したNFSアクセスの保護 34
エクスポート ポリシーがボリュームまたはqtreeへのクライアント アクセスを制御する仕組み 34
FlexVolを備えたSVMのデフォルト エクスポート ポリシー 34
エクスポート ルールの仕組み 35
リストにないセキュリティ タイプを使用するクライアントの処理方法 36
セキュリティ タイプによるクライアント アクセス レベルの決定方法 38
スーパーユーザ アクセス要求の処理方法 40
エクスポート ポリシーの作成 42
エクスポート ポリシーへのルールの追加 43
SVMへのネットグループのロード 46
ネットグループ定義のステータスの確認 47
エクスポート ルールのインデックス番号の設定 48
FlexVolへのエクスポート ポリシーの割り当て 49
qtreeへのエクスポート ポリシーの割り当て 50
qtreeからのエクスポート ポリシーの削除 51
qtreeファイル処理でのqtree IDの検証 51
FlexVolのエクスポート ポリシーの制限とネストされたジャンクション 52
エクスポートへのクライアント アクセスのチェック 52
NFSでのKerberos使用によるセキュリティ強化 53
Data ONTAPでのKerberosのサポート 53
NFSでのKerberos使用を設定するための要件 53
NFS Kerberosで許可される暗号化タイプの設定 56
NFSv4のユーザIDドメインの指定 57
NFS Kerberos realm設定の作成 58
NFS Kerberos設定の作成 59
ネーム サービスの設定 60
Data ONTAPのネーム サービス スイッチ設定の仕組み 60
ネーム サービス スイッチ テーブルの設定 62
LDAPの使用 63
SSL/TLS経由のLDAPを使用した通信の保護 63
新しいLDAPクライアント スキーマの作成 65

LDAPのRFC2307bisサポートの有効化 66
LDAPディレクトリ検索の設定オプション 67
LDAPクライアント設定の作成 69
LDAPディレクトリのホスト単位ネットグループ検索のパフォーマンス向上 70
SVMでのLDAPの有効化 72
LDAPを使用するためのSVMの設定 73
NISドメイン設定の作成 74
ローカルUNIXユーザおよびグループの設定 75
ローカルUNIXユーザの作成 75
ローカルUNIXグループへのユーザの追加 76
URIからのローカルUNIXユーザのロード 76
ローカルUNIXグループの作成 78
URIからのローカルUNIXグループのロード 78
ネーム マッピングの使用方法 80
ネーム マッピングの仕組み 81
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 81
ネーム マッピングの変換ルール 83
ネーム マッピングの作成 84
デフォルト ユーザの設定 85
IPv6経由のNFSのサポート 86
NFSでのIPv6の有効化 86
Windows NFSクライアント向けのアクセスの有効化 86
Infinite Volumeへのファイル アクセスの設定に関する情報の参照先 87
NFSを使用したファイル アクセスの管理 88
NFSv3の有効化と無効化 88
NFSv4.0の有効化と無効化 88
NFSv4.1の有効化と無効化 89
pNFSの有効化と無効化 89
NFSクライアントによるSVMのエクスポート表示の有効化 89
TCPおよびUDP経由のNFSアクセスの制御 91
非予約ポートからのNFS要求の制御 91
不明なUNIXユーザによるNTFSボリュームまたはqtreeへのNFSアクセスの処理 92
非予約ポートを使用してNFSエクスポートをマウントするクライアントに関する注意事項 93
ドメインの検証によるネットグループのより厳密なアクセス チェックの実行 93
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 94
NFSv3サービスで使用するポートの変更 95
NFSサーバの管理用コマンド 97
ネーム サービスに関する問題のトラブルシューティング 97
ネーム サービス スイッチ エントリの管理用コマンド 100
ネーム マッピングの管理用コマンド 100
ローカルUNIXユーザの管理用コマンド 101

ローカルUNIXグループの管理用コマンド 101
ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限 102
ローカルUNIXユーザおよびグループに対する制限の管理 102
ローカル ネットグループの管理用コマンド 103
NISドメイン設定の管理用コマンド 103
LDAPクライアント設定の管理用コマンド 104
LDAP設定の管理用コマンド 104
LDAPクライアント スキーマ テンプレートの管理用コマンド 105
NFS Kerberosインターフェイス設定の管理用コマンド 105
NFS Kerberos Realm設定の管理用コマンド 106
エクスポート ポリシーの管理用コマンド 106
エクスポート ルールの管理用コマンド 106
clustered Data ONTAPでのエクスポートのフェンシングまたはフェンシング解除 107
NFSクレデンシャル キャッシュの設定 107
NFSクレデンシャル キャッシュの仕組み 108
NFSクレデンシャル キャッシュのTime-To-Liveを変更する理由 108
キャッシュされたNFSユーザ クレデンシャルのTTLの設定 109
エクスポート ポリシー キャッシュの管理 110
Data ONTAPでのエクスポート ポリシー キャッシュの使用方法 110
エクスポート ポリシー キャッシュのフラッシュ 111
エクスポート ポリシー ネットグループ キューおよびキャッシュの表示 112
クライアントIPアドレスがネットグループのメンバーかどうかのチェック 112
アクセス キャッシュの仕組み 113
アクセス キャッシュ パラメータの仕組み 114
アクセス キャッシュのパフォーマンスの最適化 114
ファイル ロックの管理 115
プロトコル間のファイル ロックについて 115
Data ONTAPによる読み取り専用ビットの処理方法 116
ロックに関する情報の表示 116
ロックの解除 118
NFSv4.1サーバ実装IDの変更 119
NFSv4 ACLの管理 119
NFSv4 ACLを有効化する利点 120
NFSv4 ACLの仕組み 120
NFSv4 ACLの変更の有効化と無効化 121
Data ONTAPでのNFSv4 ACLを使用したファイル削除の可否の判別方法 121
NFSv4 ACLの有効化と無効化 121
NFSv4ファイル委譲の管理 122
NFSv4ファイル委譲の仕組み 123
NFSv4読み取りファイル委譲の有効化と無効化 123
NFSv4書き込みファイル委譲の有効化と無効化 124
NFSv4ファイルおよびレコード ロックの設定 125
NFSv4ファイルおよびレコード ロックについて 125

NFSv4ロック リース期間の指定 125
NFSv4ロック猶予期間の指定 126
NFSv4リファーラルの仕組み 126
NFSv4リファーラルの有効化と無効化 127
NFS統計の表示 127
VMware vStorage over NFSのサポート 128
VMware vStorage over NFSの有効化と無効化 129
rquotaのサポートの有効化と無効化 130
TCP最大読み取りサイズおよび書き込みサイズの変更によるNFSv3のパフォーマンスの向上 130
NFSv3 TCP最大読み取りサイズおよび書き込みサイズの変更 131
NFSユーザに許可するグループID数の設定 132
NTFSセキュリティ形式のデータへのrootユーザ アクセスの制御 133
FlexVolを備えたSVMでのNASイベントの監査 135
監査の仕組み 135
監査の基本概念 135
Data ONTAP監査プロセスの仕組み 136
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 138
監査の要件と考慮事項 138
サポートされる監査イベント ログの形式 139
監査イベント ログの表示 139
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 140
監査できるSMBイベント 140
監査対象オブジェクトへの完全パスの決定 142
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 143
NTFS代替データ ストリームを監査する際の考慮事項 144
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 145
監査設定の計画 146
SVMでのファイルとディレクトリの監査設定の作成 150
監査設定の作成 150
SVMでの監査の有効化 152
監査設定の確認 152
ファイルおよびフォルダの監査ポリシーの設定 152
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 153
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 156
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 157
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 157
CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示 158
監査設定の管理 160
監査イベント ログの手動ローテーション 160
SVMでの監査の有効化と無効化 161
監査設定に関する情報の表示 162

監査設定を変更するコマンド 163
監査設定の削除 163
リバート時のプロセス 164
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 164
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 164
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） 165
FlexVolを備えたSVMでのFPolicyによるファイルの監視と管理 166
FPolicyの仕組み 166
FPolicyソリューションの2つの要素とは 166
同期通知および非同期通知とは 166
FPolicyの実装でクラスタ コンポーネントが果たす役割 167
FPolicyと外部FPolicyサーバとの連携 168
ノードと外部FPolicyサーバの間の通信プロセス 169
SVMネームスペースにおけるFPolicyサービスの仕組み 171
FPolicyの設定タイプ 171
ネイティブFPolicyの設定を作成する場合 172
外部FPolicyサーバを使用する設定を作成する状況 172
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 172
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 173
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 174
FPolicyの設定方法 174
FPolicyを設定するための要件 174
FPolicyを設定する際のベストプラクティスと推奨事項 175
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 175
FPolicyの設定手順とは 176
FPolicy構成の計画 177
FPolicy外部エンジンの設定の計画 177
FPolicyイベントの設定の計画 184
FPolicyポリシーの設定の計画 189
FPolicyスコープの設定の計画 194
FPolicyの設定の作成 197
FPolicy外部エンジンの作成 198
FPolicyポリシー イベントの作成 199
FPolicyポリシーの作成 199
FPolicyスコープの作成 201
FPolicyポリシーの有効化 201
FPolicyの設定の変更 202
FPolicy設定の変更用コマンド 202
FPolicyポリシーの有効化と無効化 203
FPolicyの設定に関する情報の表示 203

showコマンドの仕組み 204
FPolicyの設定に関する情報を表示するコマンド 204
FPolicyポリシーのステータスに関する情報の表示 204
有効なFPolicyポリシーに関する情報の表示 205
FPolicyサーバの接続の管理 206
外部FPolicyサーバへの接続 206
外部FPolicyサーバからの切断 207
外部FPolicyサーバへの接続に関する情報の表示 207
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 209
用語集 211
著作権に関する情報 221
商標に関する情報 222
マニュアルの更新について 223
索引 224

ファイル アクセスを設定する際の考慮事項

Data ONTAPでは、さまざまなプロトコルを使用したクライアントによるファイル アクセスを管理できます。ファイル アクセスを設定する場合には、理解しておく必要がある概念がいくつかあります。

Data ONTAPでサポートされるファイル プロトコル

Data ONTAPはNFSおよびCIFSプロトコルを使用したファイル アクセスをサポートしています。

クライアントは、接続に使用しているプロトコルの種類や必要な認証の種類に関係なく、Storage Virtual Machine（SVM）上のすべてのファイルにアクセスできます。

関連タスク

SVMのプロトコルの変更（32ページ）

Data ONTAPによるファイル アクセスの制御方法

Data ONTAPでは、指定された認証ベースおよびファイルベースの制限に従って、ファイル アクセスが制御されます。

クライアントがファイルにアクセスするためにストレージ システムに接続するとき、Data ONTAPは2つのタスクを実行する必要があります。

- 認証
  Data ONTAPは、信頼できるソースでIDを検証して、クライアントを認証する必要があります。また、クライアントの認証タイプは、エクスポート ポリシーの設定時にクライアントがデータにアクセスできるかどうかの判断に使用できる方法の1つです（CIFSの場合は省略可能）。
- 許可
  Data ONTAPは、ユーザのクレデンシャルとファイルまたはディレクトリに対して設定されているアクセス許可を比較し、提供するアクセスのタイプ（該当する場合）を決定して、ユーザを許可する必要があります。

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。CIFSまたはNFSを使用するストレージ システムのファイル アクセスを設定するには、Data ONTAPの導入環境に応じて、サービスを適切に設定する必要があります。

関連コンセプト

Data ONTAPでのネーム サービスの使用方法（26ページ）

認証ベースの制限

認証ベースの制限を使用すると、Storage Virtual Machine（SVM）に接続できるクライアント マシンおよびユーザを指定できます。

Data ONTAPは、UNIXサーバおよびWindowsサーバどちらのKerberos認証もサポートします。

関連コンセプト

NFSでのKerberos使用によるセキュリティ強化（53ページ）

ファイルベースの制限

ファイルベースの制限を使用すると、ファイルごとにアクセス可能なユーザを指定できます。

ユーザがファイルを作成すると、Data ONTAPでは、そのファイルに関するアクセス許可のリストが生成されます。このアクセス許可リストの形式はプロトコルにより異なりますが、読み取り / 書き込み権限などの一般的な権限は必ず含まれます。

あるユーザがファイルにアクセスしようとすると、Data ONTAPは許可リストを使用してアクセスを許可するかどうかを決定します。アクセスは、ユーザが実行している操作（読み取り / 書き込みなど）および以下の要素に基づいて、許可または拒否されます。

- ユーザ アカウント
- ユーザ グループまたはネットグループ
- クライアント プロトコル
- ファイル タイプ

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。

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

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

ストレージ環境のStorage Virtual Machine（SVM）上のファイルへのアクセスを正しく設定するためには、ネームスペースとボリューム ジャンクションおよびその仕組みについて理解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（15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。

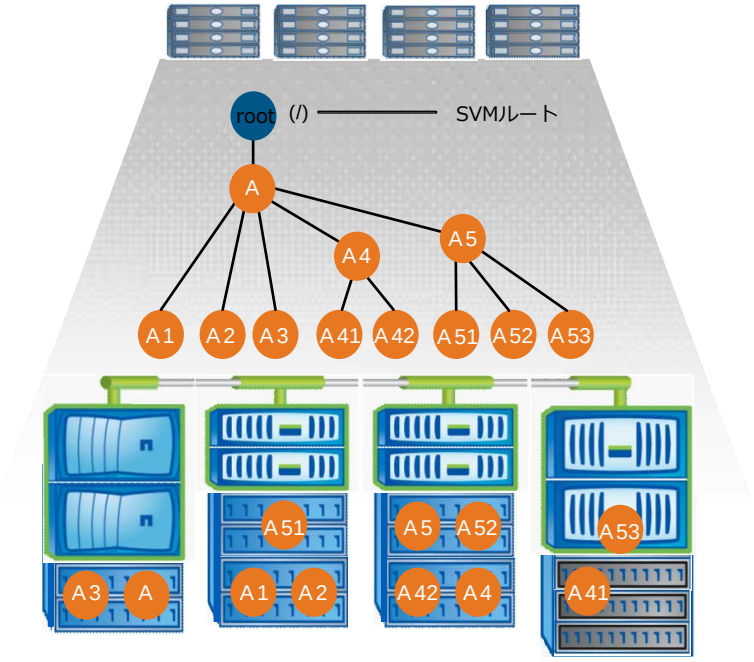
ネームスペース階層の最上位は常にルートボリュームであり、スラッシュ（/）で表します。ルートの下位のネームスペース アーキテクチャは以下の3つの基本カテゴリに分類されます。

- 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。

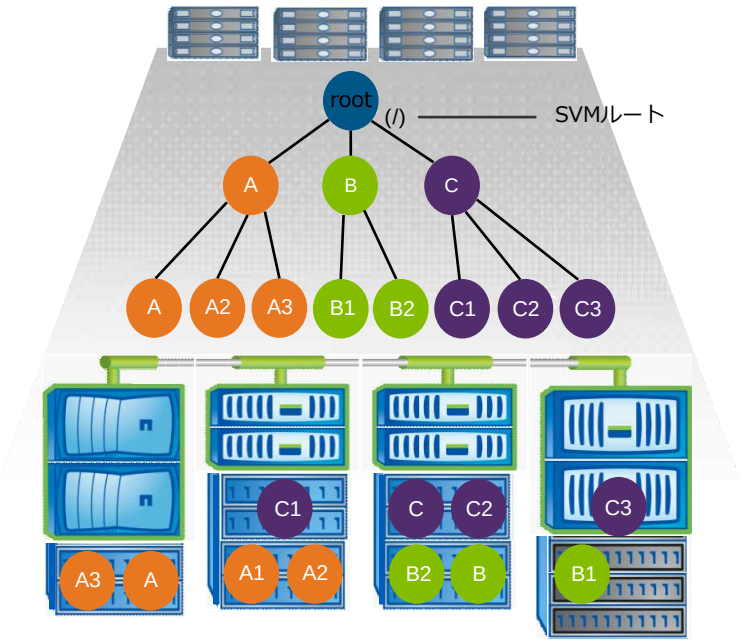


たとえば、上記のネームスペース アーキテクチャを使用する一般的なボリューム ジャンクション構成は、すべてのボリュームが単一の挿入ポイント(「data」という名前のディレクトリ)の下にジャンクションされる次のような構成になります。

```
                    Junction Junction
Vserver Volume Active Junction Path 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。

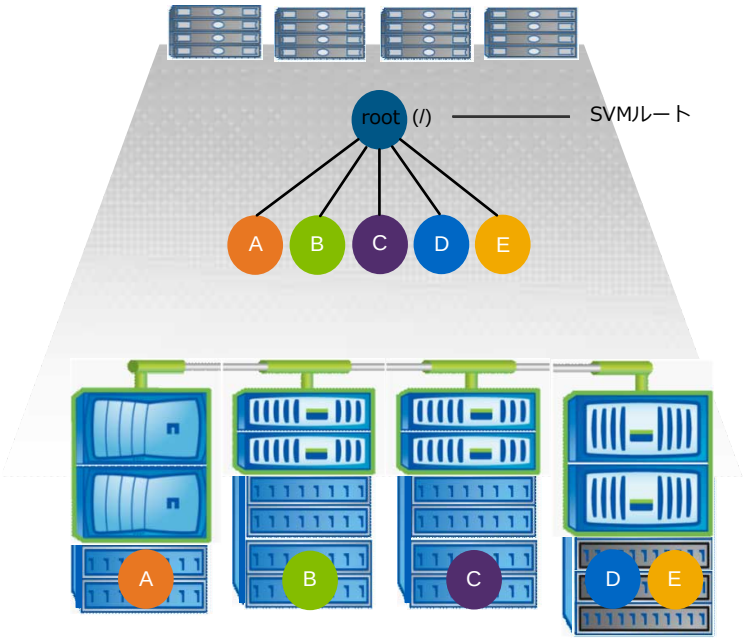


たとえば、上記のネームスペース アーキテクチャを使用する標準的なボリューム ジャンクション構成は、SVMのルートボリュームへの3つの挿入ポイントがある以下のような構成になります。挿入ポイントのうち2つは、それぞれ「data」、「projects」という名前のディレクトリです。もう1つの挿入ポイントは、「audit」という名前のジャンクション ボリュームです。

```
                    Junction Junction
Vserver Volume Active Junction Path 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。

```
                    Junction Junction
Vserver Volume Active Junction Path 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 - / -
```

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でネームスペースとボリューム ジャンクションがファイル アクセスに与える影響（11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

1. 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 *vserver_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 *vserver_name* -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
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   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はマウントされず、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 *vserver_name* -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 *vserver_name* -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
                  Junction                 Junction
Vserver   Volume     Active   Junction Path   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	**volume mount -vserver *vserver_name* -volume *volume_name* -junction-path *junction_path***

状況	入力するコマンド
ボリュームのアンマウント	**volume unmount -vserver *vserver_name* -volume *volume_name***

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 *vserver_name* -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
                  Junction                 Junction
Vserver   Volume     Active   Junction Path   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
                  Junction                 Junction
Vserver   Volume     Active   Junction Path   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	**volume show -vserver *vserver_name* -junction**
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	**volume show -vserver *vserver_name* -volume *volume_name* -instance**

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特定の情報	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。 **volume show -fields ?** b. -fieldsパラメータを使用して、必要な情報を表示します。 **volume show -vserver *vserver_name* -fields *fieldname*,...**

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
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   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 vserver,volume,aggregate,size,state,type,security-
style,junction-path,junction-parent,node
vserver 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
```

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qtree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。

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（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。

関連コンセプト

NFSv4 ACLの管理（119ページ）

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。

関連コンセプト

セキュリティ形式の設定（22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

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	• ファイルシステムがUNIX管理者によって管理されている。 • ユーザの大半がNFSクライアントである。 • 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。
NTFS	• ファイルシステムがWindows管理者によって管理されている。 • ユーザの大半がSMBクライアントである。 • 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。
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。

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。

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

セキュリティ形式がデータ アクセスに与える影響（19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`-security-style`パラメータを付加して、`volume 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 modify`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。

2. 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

NFSとCIFSのファイルの命名規則について

ファイルの命名規則は、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

ファイル名に使用できる文字

異なるオペレーティング システム上のクライアント間でファイルを共有する場合は、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を作成する場合は、ファイル名にはコロン（:）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。

ファイル名での大文字と小文字の区別

ファイル名について、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。

たとえば、CIFSクライアントがSpec.txtという名前のファイルを作成すると、この名前はCIFSクライアントとNFSクライアントの双方でSpec.txtと表示されます。ただし、CIFSクライアントがあとでspec.txtというファイルを作成しようとしても、CIFSクライアントに同じ名前がすでに存在しているため、その名前は許可されません。NFSユーザがあとでspec.txtという名前のファイルを作成すると、この名前はNFSクライアントとCIFSクライアントで次のように表示されます。

- 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、作成したとおりに両方のファイル名Spec.txtおよびspec.txtが表示されます。
- CIFSクライアントでは、Spec.txtおよびSpec~1.txtと表示されます。
  Data ONTAPによって、2つのファイル名を区別するために、Spec~1.txtというファイル名が作成されます。

Data ONTAPでのファイル名の作成方法

Data ONTAPでは、CIFS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に対して、2つのファイル名が作成され、保持されます。元の長いファイル名と8.3形式のファイル名です。

8文字のファイル名あるいは3文字の拡張子名の制限を越えるファイル名については、8.3形式ファイル名が次のように生成されます。

- ファイル名が6文字を越える場合は、元の名前が6文字に短縮されます。
- 切り捨て後に一意でなくなったファイル名にはチルダ（~）と1～5の数字が追加されます。
  同様の名前が6つ以上存在するため数字が足りなくなった場合には、元のファイル名とは無関係の一意のファイル名が作成されます。
- ファイルの拡張子が3文字に短縮されます。

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、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している場合は、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.html`になります。

Data ONTAPでのUTF-16の追加文字を含むファイル名の処理方法

UTF-16の追加文字を含むファイル名が環境で使用されている場合は、ストレージ システムでのファイルの命名時にエラーを回避するために、そのようなファイル名がData ONTAPでどのように処理されるかを理解しておく必要があります。

一般に、Windowsアプリケーションでは、Unicode文字データは16-bit Unicode Transformation Format（UTF-16）を使用して表現されます。UTF-16のBasic Multilingual Plane（BMP;基本多言語面）の文字は、単一の16ビット コード単位で表されます。それ以外の16個の追加面に含まれる文字は、*サロゲート ペア*と呼ばれる16ビット コード単位のペアで表されます。

ストレージ システムで作成するファイル名に追加文字が含まれている場合、その文字が有効か無効かにかかわらずData ONTAPはそのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

この問題を回避するために、ファイル名にはBMP文字のみを使用し、追加文字は使用しないようにしてください。

ハード マウントの使用

マウントの問題をトラブルシューティングする場合、正しい種類のマウントを使用していることを確認します。NFSは2つのマウント タイプをサポートしています。ソフト マウントとハード マウントです。信頼性を向上させるために、ハード マウントのみを使用してください。

ソフト マウントは使用しないでください（特に、NFSタイムアウトが頻繁に発生する場合）。タイムアウトによって競合状態が発生し、データが破損する可能性があります。

Data ONTAPでのNFSを使用したファイル アクセスのサポート方法

ストレージ システム上のボリュームまたはqtreeをエクスポートおよびエクスポート解除して、NFSクライアントがこれらにマウントできるようにしたりマウントできなくしたりすることができます。

Data ONTAPによるNFSクライアント認証の処理

NFSクライアントからStorage Virtual Machine（SVM）上のデータにアクセスするためには、NFSクライアントが正しく認証されている必要があります。Data ONTAPでは、UNIXクレデンシャルを設定されたネーム サービスに照らしてチェックすることで、そのクライアントを認証します。

NFSクライアントがSVMに接続すると、Data ONTAPは、SVMのネーム サービス設定に応じて複数のネーム サービスをチェックし、そのユーザのUNIXクレデンシャルを取得します。Data ONTAPでチェックできるのは、ローカルのUNIXアカウント、NISドメイン、およびLDAPドメインのクレデンシャルです。Data ONTAPがユーザを認証できるように、このうちの少なくとも1つを設定しておく必要があります。複数のネーム サービスと検索順序を指定できます。

UNIXのボリューム セキュリティ形式のみを使用するNFS環境の場合、この設定だけでNFSクライアントから接続するユーザが認証され、適切なファイル アクセスが提供されます。

ボリュームのセキュリティ形式がMixed、NTFS、またはUnifiedの場合、Data ONTAPがUNIXユーザをWindowsドメイン コントローラで認証するためにはCIFSユーザ名を取得する必要があります。そのためには、ローカルのUNIXアカウントまたはLDAPドメインを使用して個々のユーザをマッピングするか、代わりにデフォルトのCIFSユーザを使用します。Data ONTAPが検索するネーム サービスの種類と検索順序を指定するか、またはデフォルトのCIFSユーザを指定します。

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（19ページ）

Data ONTAPでのネーム サービスの使用方法

Data ONTAPは、ネーム サービスを使用してユーザやクライアントに関する情報を取得します。Data ONTAPは、この情報を使用して、ストレージ システム上のデータにアクセスしたりストレージ システムを管理したりするユーザの認証や、混在環境でのユーザ クレデンシャルのマッピングを行います。

ストレージ システムの設定時には、Data ONTAPが認証用のユーザ クレデンシャルを取得するために使用するネーム サービスを指定する必要があります。Data ONTAPでは、次のネーム サービスをサポートしています。

- ローカル ユーザ（file）
- 外部NISドメイン（NIS）
- 外部LDAPドメイン（LDAP）

ネットワーク情報を検索するソースやソースの検索順序に関するStorage Virtual Machine（SVM）の設定を行うには、`vserver services name-service ns-switch`コマンド ファミリーを使用します。これらのコマンドは、UNIXシステムの`/etc/nsswitch.conf`ファイルに相当する機能を提供します。

NFSクライアントがSVMに接続すると、Data ONTAPは指定されたネーム サービスをチェックして、ユーザのUNIXクレデンシャルを取得します。ネーム サービスが正しく設定されていてData ONTAPがUNIXクレデンシャルを取得できる場合、Data ONTAPはユーザの認証に成功します。

mixedセキュリティ形式の環境では、Data ONTAPによるユーザ クレデンシャルのマッピングが必要になる場合があります。Data ONTAPがユーザ クレデンシャルを適切にマッピングできるよう、ネーム サービスを適切に設定する必要があります。

Data ONTAPは、SVM管理者アカウントの認証にもネーム サービスを使用します。ネーム サービス スイッチを設定または変更する際にはこの点を念頭に置いて、SVM管理者アカウントの認証を誤って無効にしないようにする必要があります。SVM管理ユーザサービスの詳細については、『*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。

関連コンセプト

ネーム サービスの設定（60ページ）
ローカルUNIXユーザおよびグループの設定（75ページ）

関連タスク

LDAPを使用するためのSVMの設定（73ページ）
NISドメイン設定の作成（74ページ）

関連情報

ネットアップ テクニカル レポート4379:『Name Services Best Practice Guide Clustered Data ONTAP』

Data ONTAPによるNFSクライアントからのCIFSファイル アクセスの許可方法

Data ONTAPでは、NTFS（Windows NTファイルシステム）のセキュリティ セマンティクスを利用して、NTFS権限が設定されたファイルへのアクセス権が、NFSクライアント上のUNIXユーザにあるかどうかが判別されます。

Data ONTAPでは、ユーザのUNIX User ID（UID;UNIXユーザID）から変換されたCIFSクレデンシャルを使用して、ファイルに対するユーザのアクセス権の有無が確認されます。CIFSクレデンシャルは、通常はユーザのWindowsユーザ名であるプライマリSecurity Identifier（SID;セキュリティID）と、ユーザがメンバーとなっているWindowsグループに対応する1つ以上のグループSIDで構成されています。

Data ONTAPでUNIX UIDをCIFSクレデンシャルへ変換するときに要する時間は、数十ミリ秒から数百ミリ秒です。これは、この変換処理にドメイン コントローラへの問い合わせも含まれるためです。Data ONTAPではUIDがCIFSクレデンシャルにマッピングされます。このマッピングはクレデンシャル キャッシュ内に入力されるので、変換によって発生する照合時間が短縮されます。

サポートされるNFSバージョンおよびクライアント

ネットワークでNFSを使用する前に、Data ONTAPでサポートされるNFSのバージョンとクライアントを確認しておく必要があります。

Data ONTAPは、以下に示すNFSプロトコルのメジャーおよびマイナー バージョンをサポートしています。

- NFSv3

- NFSv4.0
- NFSv4.1
- pNFS

Data ONTAPがサポートするNFSクライアントの最新情報については、Interoperability Matrix（*mysupport.netapp.com/matrix*）を参照してください。

Data ONTAPでサポートされるNFSv4.0の機能

Data ONTAPは、SPKM3およびLIPKEYのセキュリティ機能を除き、NFSv4.0の必須機能をすべてサポートしています。

次のNFSV4の機能がサポートされます。

COMPOUND

クライアントは1回のRemote Procedure Call（RPC;リモート プロシージャ コール）要求で複数のファイル操作を要求できます。

ファイル委譲

サーバは一部の種類のクライアントにファイル制御を委任して読み取り / 書き込みアクセスを許可できます。

Pseudo-fs

NFSv4サーバでストレージ システムのマウント ポイントの決定に使用します。NFSv4にはマウント プロトコルはありません。

ロック

リースベースです。NFSv4には独立したNetwork Lock Manager（NLM;ネットワーク ロック マネージャ）またはNetwork Status Monitor（NSM;ネットワーク ステータス モニタ）プロトコルはありません。

NFSv4.0プロトコルの詳細については、RFC 3530を参照してください。

関連コンセプト

NFSv4ファイル委譲の管理（122ページ）
ファイル ロックの管理（115ページ）

関連タスク

NFSv4ファイルおよびレコード ロックの設定（125ページ）

NFSv4のData ONTAPサポートの制限

NFSv4のData ONTAPサポートにはいくつかの制限があることに注意してください。

- 委譲機能はすべてのクライアント タイプによってサポートされているわけではありません。
- LANG設定がUTF8以外のボリュームでは、ASCII以外の文字を使用した名前は、ストレージ システムで拒否されます。
- すべてのファイル ハンドルは永続的です。サーバは揮発性のファイル ハンドルを配布しません。
- 移行およびレプリケーションはサポートされません。
- NFSv4クライアントは、読み取り専用負荷共有ミラーでサポートされていません。

Data ONTAPは、NFSv4クライアントを直接読み取りおよび書き込みアクセスの負荷共有ミラーのソースにルーティングします。

- 名前付き属性はサポートされません。
- 次の属性を除くすべての推奨属性がサポートされています。
  - **archive**
  - **hidden**
  - **homogeneous**
  - **mimetype**
  - **quota_avail_hard**
  - **quota_avail_soft**
  - **quota_used**
  - **system**
  - **time_backup**

  注: Data ONTAPは**quota***属性をサポートしませんが、RQUOTA側のバンド プロトコルを通してユーザおよびグループ クォータをサポートします。

NFSv4.1のData ONTAPサポート

Data ONTAPは、NFSv4.1プロトコルをサポートし、NFSv4.1クライアントのアクセスを許可します。

デフォルトではNFSv4.1は無効になっています。これを有効にするには、Storage Virtual Machine（SVM）にNFSサーバを作成するときに`-v4.1`オプションを指定して有効（**enabled**）に設定します。

Data ONTAPは、NFSv4.1のディレクトリおよびファイル レベルの委譲をサポートしていません。

関連タスク

NFSv4.1の有効化と無効化（89ページ）

Parallel NFSのData ONTAPサポート

Data ONTAPは、Parallel NFS（pNFS;パラレルNFS）をサポートします。pNFSプロトコルは、クラスタの複数のノードに分散されたファイル セットのデータにクライアントが直接アクセスできるようにして、パフォーマンスを向上します。この機能により、クライアントはボリュームへの最適なパスを見つけることができます。

関連タスク

pNFSの有効化と無効化（89ページ）

Infinite VolumeでのNFSサポートに関する情報の参照先

Infinite VolumesでサポートされているNFSのバージョンと機能については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

FlexVolを備えたSVMでのUNIXセキュリティ形式データへのNFSアクセス プロセス

UNIXのセキュリティ形式へのNFSアクセスに使用するプロセスを理解しておくと、適切なセキュリティ設定を提供するファイル アクセスの構成を設計するときに役立ちます。

NFSクライアントがストレージ システムに接続してUNIXセキュリティ形式のデータへアクセスする場合、Data ONTAPは次の手順にしたがいます。

1. ユーザのUNIXクレデンシャルを取得します。
   Data ONTAPは、Storage Virtual Machine（SVM）の設定に応じて、ローカルのUNIXアカウント、NISサーバ、およびLDAPサーバをチェックします。
2. ユーザを許可します。
   Data ONTAPは、UNIX のデータ権限と照合してユーザのUNIXクレデンシャルをチェックし、ユーザに許可されているデータ アクセスのタイプを特定します（アクセス権限がある場合）。

このシナリオでは、CIFSクレデンシャルは必須要件ではないため、名前の照合は行われません。

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（19ページ）
ローカルUNIXユーザおよびグループの設定（75ページ）

FlexVolを備えたSVMでのNTFSセキュリティ形式データへのNFSアクセス プロセス

NTFSセキュリティ形式のデータへのNFSアクセスで使用されるプロセスを理解すると、ファイル アクセスの設定について設計するときに適切なセキュリティ設定を判断するのに役立ちます。

NTFSセキュリティ形式のデータにアクセスするためにNFSクライアントからストレージ システムに接続する場合のData ONTAPのプロセスは次のとおりです。

1. ユーザのUNIXクレデンシャルを取得します。
   Data ONTAPは、Storage Virtual Machine（SVM）の設定に応じて、ローカルのUNIXアカウント、NISサーバ、およびLDAPサーバをチェックします。
2. UNIXユーザをCIFS名にマップします。
   Data ONTAPは、SVMの設定に応じて、ローカル名のマッピング ルール、LDAPのマッピング ルール、およびデフォルトのCIFSユーザをチェックします。
3. Windowsドメイン コントローラへの接続を確立します。
   キャッシュされている接続を使用するか、DNSサーバを照会するか、または指定されている優先ドメイン コントローラを使用します。
4. ユーザを認証します。
   ドメイン コントローラに接続し、パススルー認証を実行します。
5. ユーザを許可します。
   Data ONTAPは、NTFS のデータ権限と照合してユーザのCIFSクレデンシャルをチェックし、ユーザに許可されているデータ アクセスのタイプを特定します（アクセス権限がある場合）。

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（19ページ）
ネーム マッピングの使用方法（80ページ）

ローカルUNIXユーザおよびグループの設定（75ページ）

NFSを使用したファイル アクセスの設定

クライアントがNFSを使用して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。環境の現在の設定によっては、さらにいくつかの追加手順があります。

クライアントがNFSを使用してSVMのファイルにアクセスできるようにするには、次の作業を行う必要があります。

1. SVMでNFSプロトコルを有効にします。
   NFSを使用したクライアントからのデータ アクセスを許可するようにSVMを設定する必要があります。
2. SVMでNFSサーバを作成します。
   NFSサーバは、SVM上の論理エンティティであり、SVMがNFS経由でファイルを提供できるようにします。NFSサーバを作成し、許可するNFSプロトコルのバージョンを指定する必要があります。
3. SVMでエクスポート ポリシーを設定します。
   エクスポート ポリシーを設定して、クライアントがボリュームとqtreeを使用できるようにする必要があります。
4. ネットワークおよびストレージの環境に応じて、適切なセキュリティおよびその他の設定を使用してNFSサーバを設定します。
   この手順には、Kerberos、LDAP、NIS、ネーム マッピング、ローカル ユーザの設定が含まれます。

注: NFSを使用したファイル アクセスをセットアップする前に、SVMを用意しておく必要があります。SVM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）*』を参照してください。

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	**vserver add-protocols -vserver *vserver_name* -protocols *protocol_name*[,*protocol_name*,...]**
プロトコルを無効にする	**vserver remove-protocols -vserver *vserver_name* -protocols *protocol_name*[,*protocol_name*,...]**

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
```

NFSサーバの作成

NFSサーバは、Storage Virtual Machine（SVM）へのアクセスをNFSクライアントに提供するために必要です。`vserver nfs create`コマンドを使用して、NFSサーバを作成できます。

開始する前に

NFSプロトコルを許可するようにSVMを設定しておく必要があります。

手順

1. `vserver nfs create`コマンドを使用して、NFSサーバを作成します。

例

次のコマンドは、NFSv3を無効、NFSv4.0を有効、NFSv4.0 ACLを有効にして、vs1という名前のSVM上にNFSサーバを作成します。

```
vs1::> vserver nfs create -vserver vs1 -v3 disabled -v4.0 enabled -
v4.0-acl enabled
```

関連参照情報

NFSサーバの管理用コマンド（97ページ）

エクスポート ポリシーを使用したNFSアクセスの保護

エクスポート ポリシーを使用することにより、ボリュームまたはqtreeへのNFSアクセスを特定のパラメータに一致するクライアントだけに制限することができます。

エクスポート ポリシーが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。

エクスポート ポリシーがボリュームまたはqtreeへのクライアント アクセスを制御する仕組み

エクスポート ポリシーには、各クライアント アクセス要求を処理する*エクスポート ルール*が1つ以上含まれています。この処理の結果によって、クライアント アクセスを許可するかどうか、およびアクセスのレベルが決定します。クライアントがデータにアクセスするには、エクスポート ルールを備えたエクスポート ポリシーがSVM上に存在する必要があります。

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にポリシーを1つ関連付けます。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を含む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、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ごとに新しいエクスポート ポリシーを作成する必要はありません。

クライアントが適用可能なエクスポート ルール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。

エクスポート ポリシーは、Data ONTAPが実行されているシステム上で動的に変更できます。

FlexVolを備えたSVMのデフォルト エクスポート ポリシー

FlexVolを備えたStorage Virtual Machine（SVM）には、ルールが含まれていないデフォルトのエクスポート ポリシーが用意されています。SVM上のデータにクライアントからアクセスできるようにするには、ルールを備えたエクスポート ポリシーを用意する必要があり、SVM内の各FlexVolにエクスポート ポリシーを関連付ける必要があります。

FlexVolを備えたSVMを作成すると、そのSVMのルート ボリュームに対して`default`というデフォルトのエクスポート ポリシーがストレージ システムによって自動的に作成されます。SVM上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポート ポリシーのルールを1つ以上作成する必要があります。または、ルールを備えたカスタムのエクスポート ポリシーを作成することもできます。デフォルトのエクスポート ポリシーは、変更および名前変更は可能ですが、削除することはできません。

FlexVolを備えたSVM内にFlexVolを作成すると、作成されたボリュームには、SVMのルート ボリュームのデフォルトのエクスポート ポリシーが関連付けられます。デフォルトでは、SVMに作成した各ボリュームには、ルート ボリュームのデフォルトのエクスポート ポリシーが関連付けられます。SVM内のすべてのボリュームでデフォルトのエクスポート ポリシーを使用することも、ボリュームごとに独自のエクスポート ポリシーを作成することもできます。また、複数のボリュームに同じエクスポート ポリシーを関連付けることもできます。

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。ポリシー内のエクスポート ルールの順序を変更するには、ルール インデックス番号を変更します。

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。

リストにないセキュリティ タイプを使用するクライアントの処理方法

エクスポート ルールのアクセス パラメータで指定されていないセキュリティ タイプを使用しているクライアントが現れた場合は、クライアント アクセスを拒否するか、アクセス パラメータでオプション**none**を使用してクライアントを匿名ユーザIDにマッピングすることができます。

クライアントは、別のセキュリティ タイプで認証されているか、まったく認証されていない（セキュリティ タイプAUTH_NONE）場合に、アクセス パラメータで指定されていないセキュリティ タイプを使用しているとみなされます。デフォルトでは、そのクライアントはそのレベルへのアクセスを自動的に拒否されます。ただし、アクセス パラメータにオプション**none**を追加できます。追加すると、リストにないセキュリティ タイプを使用するクライアントは、拒否されずに匿名ユーザIDにマッピングされます。`-anon`パラメータでは、このようなクライアントに割り当てられるユーザIDを指定します。`-anon`パラメータに指定するユーザIDは、匿名ユーザに適していると判断したアクセス権が設定されている有効なユーザである必要があります。

`-anon`パラメータに指定できる値の範囲は、**`0`**～**`65535`**です。

-anonに割り当てられたユーザID	**クライアント アクセス要求の処理結果**
`0` - **`65533`**	クライアント アクセス要求は匿名ユーザIDにマッピングされ、このユーザに対して設定されたアクセス権に応じてアクセスできるようになります。
`65534`	クライアント アクセス要求はユーザnobodyにマッピングされ、このユーザに対して設定されたアクセス権に応じてアクセスできるようになります。この値がデフォルトです。

-anonに割り当てられたユーザID	クライアント アクセス要求の処理結果
65535	クライアントからのアクセス要求は、このID にマッピングされ、セキュリティタイプAUTH_NONEをクライアントが使用している場合、すべて拒否されます。 ユーザID が0のクライアントからのアクセス要求は、このID にマッピングされ、他のセキュリティタイプをクライアントが使用している場合、拒否されます。

オプション**none**を使用する場合は、最初に読み取り専用パラメータが処理される点に注意することが重要です。リストにないセキュリティ タイプを使用するクライアントのエクスポート ルールを設定する際は、次のガイドラインを考慮してください。

読み取り専用にnoneが指定されている	読み取り / 書き込みにnoneが指定されている	リストにないセキュリティ タイプを使用するクライアントのアクセス結果
いいえ	いいえ	拒否
いいえ	はい	最初に読み取り専用が処理されるため、拒否
はい	いいえ	匿名として読み取り専用
はい	はい	匿名として読み取り / 書き込み

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` **`sys,none`**
- `-rwrule` **`any`**
- `-anon` **`70`**

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。

クライアント#3は、IPアドレスが10.1.16.234で、NFSv3プロトコルを使用してアクセス要求を送信し、認証は行われていません（セキュリティ タイプAUTH_NONE）。

3つすべてのクライアントで、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では、読み取り専用アクセスが、AUTH_SYSで認証された、自身のユーザIDを持つクライアントに許可されています。また、読み取り専用パラメータでは、ユーザIDが70の匿名ユーザとしての読み取り専用アクセスが、他のセキュリティ タイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスがすべてのセキュリティ タイプに許可されていますが、この場合は、読み取り専用ルールですでにフィルタされているクライアントにのみ適用されます。

したがって、クライアント#1とクライアント#3は、ユーザIDが70の匿名ユーザとしてのみ読み取り / 書き込みアクセス権を取得します。クライアント#2は、自身のユーザIDで読み取り / 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` **`sys,none`**
- `-rwrule` **`none`**
- `-anon` **`70`**

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。

クライアント#3は、IPアドレスが10.1.16.234で、NFSv3プロトコルを使用してアクセス要求を送信し、認証は行われていません（セキュリティ タイプAUTH_NONE）。

3つすべてのクライアントで、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では、読み取り専用アクセスが、AUTH_SYSで認証された、自身のユーザIDを持つクライアントに許可されています。また、読み取り専用パラメータでは、ユーザIDが70の匿名ユーザとしての読み取り専用アクセスが、他のセキュリティ タイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、匿名ユーザとしてのみ読み取り / 書き込みアクセスが許可されています。

したがって、クライアント#1とクライアント#3は、ユーザIDが70の匿名ユーザとしてのみ読み取り / 書き込みアクセス権を取得します。クライアント#2は、自身のユーザIDで読み取り専用アクセス権を取得しますが、読み取り / 書き込みアクセスは拒否されます。

セキュリティ タイプによるクライアント アクセス レベルの決定方法

クライアントの認証に使用されるセキュリティ タイプは、エクスポート ルールで特別な役割を果たします。クライアントがボリュームまたはqtreeにアクセスする際のレベルがセキュリティ タイプによってどのように決定されるかについて理解しておく必要があります。

有効なアクセス レベルには、次の3つがあります。

1. 読み取り専用
2. 読み取り / 書き込み
3. スーパーユーザ（ユーザIDが0のクライアントの場合）

セキュリティ タイプに基づくアクセス レベルはこの順序で評価されるため、エクスポート ルールでアクセス レベル パラメータを作成するときは、次のルールに従う必要があります。

クライアントに必要なアクセス レベル	クライアントのセキュリティ タイプと一致する必要があるアクセス パラメータ
標準ユーザの読み取り専用	読み取り専用（`-rorule`）
標準ユーザの読み取り / 書き込み	読み取り専用（`-rorule`）および読み取り / 書き込み（`-rwrule`）
スーパーユーザの読み取り専用	読み取り専用（`-rorule`）および`-superuser`

クライアントに必要なアクセス レベル	クライアントのセキュリティ タイプと一致する必要があるアクセス パラメータ
スーパーユーザの読み取り / 書き込み	読み取り専用（`-rorule`）、読み取り / 書き込み（`-rwrule`）、および`-superuser`

次に、3つそれぞれのアクセス パラメータで有効なセキュリティ タイプを示します。

- **any**
- **none**
- **never**
  このセキュリティ タイプは、`-superuser`パラメータには使用できません。
- **krb5**
- **krb5i**
- **ntlm**
- **sys**

クライアントのセキュリティ タイプを3つそれぞれのアクセス パラメータと照合したときの結果としては、次の3つが想定されます。

クライアントのセキュリティ タイプ	結果
アクセス パラメータで指定されたタイプと一致する。	クライアントは、自身のユーザIDでそのレベルのアクセス権を取得します。
指定されたタイプと一致しないが、アクセス パラメータにオプション**none**が指定されている。	クライアントは、そのレベルのアクセス権を、`-anon`パラメータで指定されているユーザIDの匿名ユーザとして取得します。
指定されたタイプと一致せず、アクセス パラメータにオプション**none**が指定されていない。	クライアントは、そのレベルのアクセス権を取得できません。 これは、`-superuser`パラメータには適用されません。このパラメータには、指定しなくても常に**none**が指定されるためです。

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` **sys,krb5**
- `-superuser` **krb5**

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが0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、ユーザIDが0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。

クライアント#3は、IPアドレスが10.1.16.234、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、認証は行われていません（AUTH_NONE）。

3つすべてのクライアントで、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では、セキュリティ タイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスが、AUTH_SYSまたはKerberos v5で認証された、独自のユーザIDを持つクライアントに許可されています。スーパーユーザ パラメータでは、スーパーユーザ アクセスが、Kerberos v5で認証された、ユーザIDが0のクライアントに許可されています。

したがって、クライアント#1は、3つすべてのアクセス パラメータに一致するため、スーパーユーザの読み取り / 書き込みアクセス権を取得します。クライアント#2は、読み取り / 書き込みアクセス権を取得しますが、スーパーユーザ アクセス権は取得できません。クライアント#3は、読み取り専用アクセス権を取得しますが、スーパーユーザ アクセス権は取得できません。

スーパーユーザ アクセス要求の処理方法

エクスポート ポリシーを設定する際には、ユーザIDが0のクライアント（スーパーユーザ）からアクセス要求を受け取った場合のストレージ システムの処理を検討し、それに応じてエクスポート ルールを設定する必要があります。

UNIXでは、ユーザIDが0のユーザはスーパーユーザ（通常はroot）と呼ばれ、システムに対して無制限のアクセス権を持ちます。スーパーユーザ権限の使用は、システムやデータのセキュリティ侵害などのいくつかの理由により、リスクを伴う可能性があります。

デフォルトでは、ユーザIDが0のクライアントは匿名ユーザにマッピングされます。ただし、エクスポート ルールで`-superuser`パラメータを指定すると、ユーザIDが0のクライアントの処理方法をセキュリティ タイプに応じて決定することができます。次に、`-superuser`パラメータで有効なオプションを示します。

- **any**
- **none**
  これは、`-superuser`パラメータを指定しない場合のデフォルト設定です。
- **krb5**
- **ntlm**
- **sys**

ユーザIDが0のクライアントは、`-superuser`パラメータの設定に応じて2通りの方法で処理されます。

-superuserパラメータとクライアントのセキュリティ タイプ	**結果**
Match	クライアントは、ユーザID 0でスーパーユーザ アクセス権を取得します。
一致しない	クライアントは、-anonパラメータで指定されているユーザIDの匿名ユーザとしてアクセスし、そのユーザに割り当てられたアクセス権を取得します。 読み取り専用パラメータまたは読み取り / 書き込みパラメータでオプション**none**が指定されているかどうかは関係ありません。

クライアントがNTFSセキュリティ形式のボリュームへのアクセスでユーザID 0を使用し、-superuserパラメータが**none**に設定されている場合、Data ONTAPは匿名ユーザのネーム マッピングを使用して適切なクレデンシャルを取得します。

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`**
- `-anon` **`127`**

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが746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、ユーザIDが0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。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、スーパーユーザ アクセス権を取得できません。`-superuser`パラメータが指定されていないため、代わりに匿名にマッピングされます。つまり、デフォルトで**none**が設定され、ユーザID 0は自動的に匿名にマッピングされます。また、クライアント#2はセキュリティ タイプが読み取り / 書き込みパラメータと一致しなかったため、読み取り専用アクセス権のみを取得します。

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`**
- `-superuser` **`krb5`**
- `-anon` **`0`**

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが0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、ユーザIDが0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。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。

このエクスポート ルールでは、ユーザIDが0のクライアントにスーパーユーザ アクセスが許可されています。クライアント#1は、ユーザIDが一致し、読み取り専用パラメータと-superuserパラメータのセキュリティ タイプにも一致するため、スーパーユーザ アクセス権を取得します。クライアント#2は、セキュリティ タイプが読み取り / 書き込みパラメータとも-superuserパラメータとも一致しないため、読み取り / 書き込みアクセス権もスーパーユーザ アクセス権も取得できません。代わりに、クライアント#2は匿名ユーザ（この場合はユーザIDが0）にマッピングされます。

エクスポート ポリシーの作成

エクスポート ルールを作成する前に、それらを保持するエクスポート ポリシーを作成する必要があります。`vserver export-policy create`コマンドを使用して、エクスポート ポリシーを作成できます。

手順

1. エクスポート ポリシーを作成するには、次のコマンドを入力します。

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   `-vserver` *`vserver_name`*には、Storage Virtual Machine（SVM）名を指定します。

   `-policyname` *`policy_name`*には、新しいエクスポート ポリシーの名前を指定します。ポリシー名に指定できる文字数は最大256文字です。

2. 次の操作のいずれかを実行して、エクスポート ポリシーをボリュームまたはqtreeに割り当てます。

エクスポート ポリシーの割り当て先	入力するコマンド
ボリューム	**`volume modify -vserver` *`vserver_name`* `-volume` *`volume_name`* `-policy` *`export_policy_name`***
qtree	**`volume qtree modify -vserver` *`vserver_name`* `-volume` *`volume_name`* `-qtree` *`qtree_name`* `-export-policy` *`export_policy_name`***

例

次のコマンドは、vs1という名前のSVM上にrs1という名前のエクスポート ポリシーを作成します。

```
vs1::> vserver export-policy create -vserver vs1 -policyname rs1
```

関連タスク

エクスポートへのクライアント アクセスのチェック（52ページ）

関連参照情報

エクスポート ポリシーの管理用コマンド（106ページ）

エクスポート ポリシーへのルールの追加

`vserver export-policy rule create`コマンドを使用して、エクスポート ポリシーのエクスポート ルールを作成することができます。これにより、データへのクライアント アクセスを定義できます。

開始する前に

エクスポート ルールを追加するエクスポート ポリシーを用意しておく必要があります。

手順

1. エクスポート ルールを作成します。

   `vserver export-policy rule create -vserver` *`virtual_server_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol {any|nfs3|nfs|cifs|nfs4|flexcache},... -clientmatch` *`text`* `-rorule {any|none|never|krb5|ntlm|sys},... -rwrule {any|none|never|krb5|ntlm|sys},... -anon` *`user_ID`* `-superuser {any|none|krb5|ntlm|sys},... -allow-suid {true|false} -allow-dev {true|false}`

   `-vserver` *`vserver_name`*では、Storage Virtual Machine（SVM）名を指定します。

   `-policyname` *`policy_name`*で、ルールを追加する既存のエクスポート ポリシーの名前を指定します。

   `-ruleindex` *`integer`*で、ルールのインデックス番号を指定します。ルールは、インデックス番号のリストの順序に従って、インデックス番号が小さいものから順番に評価されます。たとえば、インデックス番号が1のルールは、インデックス番号が2のルールよりも先に評価されます。

   `-protocol` {**any**|**nfs3**|**nfs**|**cifs**|**nfs4**|**flexcache**}で、エクスポート ルールを適用するアクセス プロトコルを指定します。カンマ区切りの形式を使用して、1つのエクスポート ルールに対して複数のアクセス プロトコルを指定できます。プロトコルとして**any**を指定する場合、他のプロトコルは指定しないでください。アクセス プロトコルを指定しない場合は、デフォルト値である**any**が使用されます。

   `-clientmatch` *`text`*で、ルールを適用するクライアントを指定します。次のいずれかの形式で指定できます。

クライアントを照合する形式	例
先頭に「.」という 文字が付いたドメイン名	**`.example.com`**
ホスト名	**`host1`**
IPv4アドレス	**`10.1.12.24`**
サブネット マスクをビット数で表したIPv4アドレス	**`10.1.12.10/4`**
IPv4アドレスとネットワーク マスク	**`10.1.16.0/255.255.255.0`**
ピリオド区切りの形式のIPv6アドレス	**`::1.2.3.4`**
サブネット マスクをビット数で表したIPv6アドレス	**`ff::00/32`**
ネットグループ名の前に@文字を付けた単一ネットグループ	**`@netgroup1`**

   注: 10.1.12.10-10.1.12.70のように、IPアドレスの範囲を入力することはできません。この形式のエントリはテキスト文字列と解釈され、ホスト名として扱われます。ff::12/ff::00のように、IPv6アドレスとネットワーク マスクを入力することはできません。

エクスポート ルールの個々のIPアドレスを指定してクライアント アクセスを細かく管理する際には、動的（DHCPなど）または一時的（IPv6など）に割り当てられているIPアドレスを指定しないでください。これらのアドレスを指定した場合、IPアドレスが変更されるとクライアントはアクセス権を失います。

一部のクライアント照合形式では、Data ONTAPがデータSVMのDNS設定を使用してDNSルックアップを実行します。エクスポート ポリシー ルールの照合エラーによるクライアント データ アクセスの問題を回避するためには、データSVMのDNS設定が適切に機能することと、DNSサーバにNFSクライアントの正しいエントリが設定されていることが重要です。

`-rorule` {**any**|**none**|**never**|**krb5**|**krb5i**|**ntlm**|**sys**|}は、指定したセキュリティ タイプで認証するクライアントに読み取り専用アクセスを許可します。

`-rwrule` {**any**|**none**|**never**|**krb5**|**krb5i**|**ntlm**|**sys**|}は、指定したセキュリティ タイプで認証するクライアントに読み取り / 書き込みアクセスを許可します。

注: クライアントに特定のセキュリティタイプの読み取り / 書き込みアクセスが許可されるのは、エクスポート ルールでそのセキュリティ タイプに対しても読み取り専用アクセスが許可されている場合にかぎります。読み取り専用パラメータに読み取り / 書き込みパラメータよりも限定的なセキュリティ タイプを指定した場合、クライアントに対して読み取り / 書き込みアクセスが許可されない可能性があります。

1つのルールに対して複数のセキュリティ タイプをカンマで区切って指定できます。セキュリティ タイプとして**any**または**never**を指定する場合、他のセキュリティ タイプは指定しないでください。指定できる有効なセキュリティ タイプは次のとおりです。

- **any**
  一致するクライアントに対して、セキュリティ タイプに関係なく、データへのアクセスを許可します。
- **none**
  単独で指定した場合、どのセキュリティ タイプのクライアントにも匿名アクセスが許可されます。他のセキュリティ タイプと一緒に指定した場合、指定したセキュリティ タイプのクライアントにアクセスが許可され、それ以外のセキュリティ タイプのクライアントには匿名アクセスが許可されます。
- **never**
  一致するクライアントに対して、セキュリティ タイプに関係なく、データへのアクセスを禁止します。
- **krb5**
  一致するクライアントのうち、Kerberos 5で認証されたクライアントに対して、データへのアクセスを許可します。
- **krb5i**
  一致するクライアントのうち、Kerberos 5iで認証されたクライアントに対して、データへのアクセスを許可します。
- **ntlm**
  一致するクライアントのうち、CIFS NTLMで認証されたクライアントに対して、データへのアクセスを許可します。
- **sys**
  一致するクライアントのうち、NFS AUTH_SYSで認証されたクライアントに対して、データへのアクセスを許可します。

`-anon` *`user_ID`*で、ユーザIDが0（ゼロ）で到着するクライアント要求にマップされるUNIXユーザIDまたはユーザ名を指定します。このユーザIDは通常、ユーザ名rootと関連付けられています。デフォルト値は65534です。通常、NFSクライアントは65534というユーザIDをユーザ名nobodyに関連付けます。clustered Data ONTAPでは、このユーザIDがpcuserというユーザに関

連付けられています。ユーザIDが0のクライアントからのアクセスをすべて無効にするには、値65535を指定します。

`-superuser` {**any**|**none**|**krb5**|**krb5i**|**ntlm**|**sys**|}で、クライアントにスーパーユーザ アクセスを許可する条件となるセキュリティ タイプを指定します。

注: 特定のセキュリティ タイプに対するスーパーユーザ アクセスは、エクスポート ルールでそのセキュリティ タイプに対する読み取り専用アクセスも許可した場合にのみ許可されます。読み取り専用パラメータでスーパーユーザ パラメータよりも限定的なセキュリティ タイプを指定した場合、クライアントに対してスーパーユーザ アクセスが許可されない可能性があります。

`-allow-suid` {**true**|**false**}で、set user ID（SUID）およびset group ID（SGID）へのアクセスを許可するかどうかを指定します。このパラメータが**true**に設定されている場合、クライアントはファイル、ディレクトリ、およびボリュームのSUIDやSGIDを変更できます。このパラメータが**false**に設定されている場合、クライアントはディレクトリおよびボリュームのSUIDやSGIDを変更できますが、ファイルのSUIDやSGIDは変更できません。デフォルトは**true**です。

`-allow-dev` {**true**|**false**}で、デバイスの作成を許可するかどうかを指定します。デフォルトは**true**です。

例

次に、rs1というエクスポート ポリシーでvs1というSVMに対するエクスポート ルールを作成するコマンドの例を示します。このルールのインデックス番号は1です。このルールでは、すべてのクライアントを対象に、すべてのNFSアクセスを許可します。読み取り専用アクセスをすべてのクライアントに許可し、読み取り / 書き込みアクセスについては、Kerberos認証を使用するクライアントにのみ許可しています。UNIXユーザIDが0（ゼロ）のクライアントは、ユーザID 65534（通常はユーザ名nobody）にマッピングされます。このルールは、SUIDおよびSGIDの変更を有効にしていますが、デバイスの作成は有効にしていません。

```
vs1::> vserver export-policy rule create -vserver vs1
-policyname rs1 -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0
-rorule any -rwrule krb5 -anon 65534 -allow-suid true -allow-dev
false
```

次に、expol2というエクスポート ポリシーでvs2というSVMに対するエクスポート ルールを作成するコマンドの例を示します。このルールのインデックス番号は21です。このルールは、クライアントをネットグループdev_netgroup_mainのメンバーと照合します。すべてのNFSアクセスを許可します。AUTH_SYSによって認証されたクライアントの読み取り専用アクセスを許可し、読み取り / 書き込みアクセスについてはKerberos認証を要求します。UNIXユーザIDが0（ゼロ）のクライアントは、ユーザID 65534（通常はユーザ名nobody）にマッピングされます。このルールは、SUIDおよびSGIDの変更を有効にしていますが、デバイスの作成は有効にしていません。

```
vs1::> vserver export-policy rule create -vserver vs2
-policyname expol2 -ruleindex 21 -protocol nfs -clientmatch
@dev_netgroup_main -rorule sys -rwrule krb5 -anon 65534
-allow-suid true -allow-dev false
```

関連タスク

エクスポートへのクライアント アクセスのチェック（52ページ）

関連参照情報

エクスポート ルールの管理用コマンド（106ページ）

SVMへのネットグループのロード

エクスポート ポリシー ルールでクライアントの照合に使用できる方法の1つに、ネットグループに含まれるホストを使用する方法があります。外部ネーム サーバに格納されているネットグループを使用する（`vserver services name-service netgroup load`）代わりに、URIを使用してネットグループをStorage Virtual Machine（SVM）にロードすることもできます。

タスク概要

Data ONTAPは、ローカル ネットグループ ファイルを対象としたホスト単位のネットグループ検索をサポートしています。ネットグループ ファイルをロードすると、ホスト単位のネットグループ検索を有効にするためにnetgroup.byhostマップがData ONTAPによって自動的に作成されます。これにより、エクスポート ポリシー ルールを処理してクライアント アクセスを評価する際のローカル ネットグループ検索にかかる時間が大幅に短縮されます。

手順

1. URIを使用してネットグループをSVMにロードします。

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   `-vserver` *`vserver_name`*では、SVM名を指定します。

   `-source` {**`ftp`**|**`http`**|**`ftps`**|**`https`**}://*`uri`*では、ロードに使用するURIを指定します。

   ファイルは、NISの設定に使用されたのと同じネットグループ テキスト ファイル形式に従っている必要があります。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。Data ONTAPは、ファイルをロードする前にファイル形式をチェックします。エラーがあった場合は、ファイルに対して必要な修正内容を示す警告メッセージがコンソールに表示されます。修正しなかった場合、クライアント アクセスに問題が生じる可能性があります。

   ネットグループにIPv6アドレスを指定する際には、RFC 5952の規定に従って各アドレスを短縮する必要があります。

   ネットグループ ファイル内のホスト名に含まれるアルファベットは、すべて小文字にする必要があります。

   サポートされる最大ファイル サイズは5MBです。

   ネットグループでサポートされる最大ネスト レベルは1,000です。

   ネットグループ ファイルにホスト名を定義する際には、プライマリDNSホスト名のみを使用する必要があります。エクスポートへのアクセスに関する問題を避けるために、ホスト名の定義にはDNS CNAMEやラウンド ロビン レコードを使用しないでください。

   フォワードおよびリバースDNSルックアップの一貫性を確保するために、ネットグループ内のすべてのホストにフォワード（A）およびリバース（PTR）の両方のDNSレコードがある必要があります。また、あるクライアントのIPアドレスに複数のPTRレコードがある場合は、それらすべてのホスト名がネットグループのメンバーで、対応するAレコードが定義されている必要があります。

   ネットグループ ファイル内の3要素のドメイン部は、Data ONTAPでサポートされていないため空にしておきます。

   ネットグループ ファイルのロードとnetgroup.byhostマップの構築には、少し時間がかかる場合があります。

   ネットグループの更新が必要な場合は、ネットグループ ファイルを編集し、更新されたファイルをSVMにロードすることができます。

例

次のコマンドは、HTTPのURL `http://intranet/downloads/corp-netgroup`を使用して、ネットグループ定義をvs1というSVMにロードします。

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

関連タスク

ネットグループ定義のステータスの確認（47ページ）
クライアントIPアドレスがネットグループのメンバーかどうかのチェック（112ページ）
ドメインの検証によるネットグループのより厳密なアクセス チェックの実行（93ページ）

関連参照情報

ローカル ネットグループの管理用コマンド（103ページ）

関連情報

IETF RFC 5952:『A Recommendation for IPv6 Address Text Representation』

ネットグループ定義のステータスの確認

ネットグループをStorage Virtual Machine（SVM）にロードしたあと、`vserver services name-service netgroup status`コマンドを使用してネットグループ定義の状態を確認できます。これにより、ネットグループの定義がSVMの基盤となるすべてのノードで一貫しているかどうかを確認することができます。

手順

1. 権限レベルをadvancedに設定します。

   `set -privilege advanced`

2. ネットグループの定義の状態を確認します。

   `vserver services name-service netgroup status`

   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
   - ネットグループの定義のロード時間
   - ネットグループの定義のハッシュ値

   より詳細な表示でその他の情報を表示できます。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。

3. admin権限レベルに戻ります。

   `set -privilege admin`

例

次に、すべてのSVMのネットグループの状態を表示するコマンドの例を示します。

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- ------------------- --------------------------------
vs1
          node1           9/20/2006 16:04:53  e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26  e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08  e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33  e6cb38ec1396a280c0d2b77e3a84eda2
```

関連タスク

SVMへのネットグループのロード（46ページ）

エクスポート ルールのインデックス番号の設定

`vserver export-policy rule setindex`コマンドを使用して、既存のエクスポート ルールのインデックス番号を手動で設定することができます。これにより、エクスポート ルールが処理される順序を変更できます。

タスク概要

新しいインデックス番号がすでに使用されている場合は、指定した位置にルールが挿入され、それに応じてリストの順序が調整されます。

手順

1. 指定したエクスポート ルールのインデックス番号を変更するには、次のコマンドを入力します。

   `vserver export-policy rule setindex -vserver` *`virtual_server_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-newruleindex` *`integer`*

   `-vserver` *`virtual_server_name`*では、Storage Virtual Machine（SVM）名を指定します。

   `-policyname` *`policy_name`*で、ポリシー名を指定します。

   `-ruleindex` *`integer`*で、エクスポート ルールの現在のインデックス番号を指定します。指定したインデックス番号が既存のエクスポート ポリシー ルールによってすでに使用されている場合、そのエクスポート ポリシー ルールおよびそれ以降のすべてのエクスポート ポリシー ルールのインデックス番号が1つ増やされます。

   `-newruleindex` *`integer`*で、エクスポート ルールの新しいインデックス番号を指定します。

例

次に、vs1というSVMのrs1というエクスポート ポリシーのインデックス番号を3から2に変更する例を示します。

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

FlexVolへのエクスポート ポリシーの割り当て

Storage Virtual Machine（SVM）内の各FlexVolには、ボリュームのデータにクライアントがアクセスできるように、エクスポート ルールを含むエクスポート ポリシーを関連付ける必要があります。

タスク概要

SVMを作成すると、Data ONTAPによって*default*というデフォルト エクスポート ポリシーがSVMに対して作成されます。SVMのボリュームには、この*default*エクスポート ポリシーが割り当てられます。デフォルト ポリシーの代わりに、別のカスタム エクスポート ポリシーを作成してボリュームに関連付けることができます。カスタム エクスポート ポリシーをボリュームに関連付ける前に、ボリュームのデータへの必要なアクセスを許可するエクスポート ルールを1つ以上作成し、そのエクスポート ルールを、ボリュームに関連付けるエクスポート ポリシーに割り当てる必要があります。

エクスポート ポリシーは、ボリュームの作成時、またはボリュームの作成後にいつでも、ボリュームに関連付けることができます。1個のボリュームに1つのエクスポート ポリシーを関連付けることができます。

手順

1. `volume create`コマンドまたは`volume modify`コマンドに`-policy`オプションを指定して実行し、エクスポート ポリシーをボリュームに関連付けます。

   例

   ```
   cluster::> volume create -vserver vs1 -volume vol1
   -aggregate aggr2 -state online -policy cifs_policy -security-style
   ntfs
   -junction-path /dept/marketing -size 250g -space-guarantee volume
   ```

   `volume create`コマンドと`volume modify`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 export-policy rule show`コマンドに`-policyname`オプションを指定して実行し、ボリュームに関連付けたエクスポート ポリシーのアクセス設定が適切であることを確認します。

   例

   ```
   cluster::> vserver export-policy rule show -policyname cifs_policy
   Virtual      Policy             Rule    Access   Client       RO
   Server       Name               Index   Protocol Match        Rule
   ------------ ------------------ ------  -------- ------------ ------
   vs1          cifs_policy        1       cifs      0.0.0.0/0    any
   ```

   `vserver export-policy rule show`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。

   このコマンドにより、エクスポート ポリシーに適用されるルールの一覧を含む、エクスポート ポリシーの概要が表示されます。Data ONTAPでは、各ルールにルール インデックス番号が割り当てられます。ルール インデックス番号を確認したあと、その番号を使用して、指定したエクスポート ルールの詳細情報を表示できます。

3. `vserver export-policy rule show`コマンドに`-policyname`、`-vserver`、`-ruleindex`の各オプションを指定して実行し、エクスポート ポリシーに適用されるルールが正しく設定されていることを確認します。

例

```
cluster::> vserver export-policy rule show -policyname cifs_policy -
vserver vs1 -ruleindex 1
                             Virtual Server: vs1
                                Policy Name: cifs_policy
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 0
                  Superuser Security Flavors: any
                Honor SetUID Bits In SETATTR: true
                   Allow Creation of Devices: true
```

qtreeへのエクスポート ポリシーの割り当て

ボリューム全体をエクスポートする代わりに、ボリュームの特定のqtreeをエクスポートしてクライアントから直接アクセスできるようにすることもできます。qtreeをエクスポートするには、qtreeにエクスポート ポリシーを割り当てます。エクスポート ポリシーの割り当ては、新しいqtreeの作成時に行うことも、既存のqtreeを変更して行うこともできます。

開始する前に

エクスポート ポリシーが存在している必要があります。

タスク概要

作成時に指定しなかった場合、qtreeでは格納先ボリュームの親のエクスポート ポリシーがデフォルトで使用されます。

手順

1. 次のいずれかを実行します。

エクスポート ポリシーの割り当て先	入力するコマンド
新しいqtree	**volume qtree create -vserver *vserver_name* -qtree-path /vol/*volume_name*/*qtree_name* -export-policy *export_policy_name***
既存のqtree	**volume qtree modify -vserver *vserver_name* -qtree-path /vol/*volume_name*/*qtree_name* -export-policy *export_policy_name***

2. 次のコマンドを入力して、エクスポート ポリシーが正しく割り当てられたことを確認します。

   volume qtree show -qtree *qtree_name* -fields export-policy

例

次のコマンドは、SVM vs1上のボリュームvol_engにdev1という新規qtreeを作成し、このqtreeにエクスポート ポリシーdev1_exportを割り当てます。

```
vs1::> volume qtree create -vserver vs1 -qtree-path /vol/vol_eng/
dev1 -export-policy dev1_export
```

次のコマンドは、SVM vs1上のボリュームvol_engにあるdev2という既存のqtreeを変更し、このqtreeにエクスポート ポリシーdev2_exportを割り当てます。

```
vs1::> volume qtree modify -vserver vs1 -qtree-path /vol/vol_eng/
dev2 -export-policy dev2_export
```

qtreeからのエクスポート ポリシーの削除

qtreeに割り当てられている特定のエクスポート ポリシーが不要になった場合は、代わりに格納先ボリュームのエクスポート ポリシーを継承するようにqtreeを変更することで、そのエクスポート ポリシーを削除できます。この操作を行うには、`volume qtree modify`コマンドで`-export-policy`パラメータと空の名前文字列(""")を指定します。

タスク概要

qtreeエクスポートをサポートしていない8.2.1より前のData ONTAPリリースへのダウングレードを行うには、この作業を実行して、qtreeに割り当てられているすべてのエクスポート ポリシーを削除する必要があります。

手順

1. qtreeからエクスポート ポリシーを削除するには、次のコマンドを入力します。

   volume qtree modify -vserver *vserver_name* -qtree-path /vol/*volume_name*/*qtree_name* -export-policy ""

2. 次のコマンドを入力して、qtreeが適切に変更されたことを確認します。

   volume qtree show -qtree *qtree_name* -fields export-policy

qtreeファイル処理でのqtree IDの検証

Data ONTAPでは、オプションでqtree IDのオプションの検証を実行できます。この検証により、クライアントのファイル処理要求で有効なqtree IDが使用されていることが確認され、クライアントが同じqtree内でのみファイルを移動できるようになります。この検証は、`-validate-qtree-export`パラメータを変更することで有効または無効にすることができます。このパラメータはデフォルトで有効になっています。

タスク概要

このパラメータは、Storage Virtual Machine(SVM)上にある1つ以上のqtreeにエクスポート ポリシーを直接割り当てている場合にのみ機能します。

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。

qtree ID検証	入力するコマンド
有効にする	**vserver nfs modify -vserver *vserver_name* -validate-qtree-export enabled**
無効にする	**vserver nfs modify -vserver *vserver_name* -validate-qtree-export disabled**

3. admin権限レベルに戻ります。

   set -privilege admin

FlexVolのエクスポート ポリシーの制限とネストされたジャンクション

上位レベルのジャンクションでネストされたジャンクションよりも制限が厳しいエクスポート ポリシーを設定した場合は、下位レベルのジャンクションへのアクセスに失敗する可能性があります。

上位レベルのジャンクションには下位レベルのジャンクションよりも制限が厳しくないエクスポート ポリシーを設定するようにしてください。

エクスポートへのクライアント アクセスのチェック

エクスポート ポリシーを導入してエクスポートへのクライアント アクセスを管理する場合、エクスポート ポリシーをテストして想定どおりに動作するかどうかを確認できます。エクスポート ポリシーを導入後にクライアントでアクセスの問題が発生した場合は、エクスポート ポリシーをテストして問題のトラブルシューティングを実施できます。これらの目的でのエクスポート ポリシーのテストは、`vserver export-policy check-access`コマンドで実行できます。

タスク概要

特定の認証方式とファイル アクセス プロトコルを使用した、特定のクライアントによる特定のボリュームまたはqtreeエクスポートへのアクセスをチェックできます。

手順

1. `vserver export-policy check-access`コマンドを使用して、エクスポートへのクライアント アクセスをチェックします。

   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. 出力内容を確認して、エクスポート ポリシーが意図したとおりに機能してクライアント アクセスが想定どおりに動作しているかどうかを判断します。具体的には、ボリュームまたはqtreeによって使用されたエクスポート ポリシーと、クライアントに許可されたアクセスのタイプを確認します。

3. 必要に応じて、エクスポート ポリシー ルールを設定しなおします。

例

次のコマンドは、IPアドレスが1.2.3.4のNFSv3クライアントによるボリュームflex_vol上のqtree qt1への読み取り / 書き込みアクセスをチェックします。コマンド出力には、qtreeがエクスポート ポリシー*primarynames*を使用していること、アクセスが拒否されたことが示されています。

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip 1.2.3.4 -volume
flex_vol -authentication-method sys -protocol nfs3 -access-type read-write -qtree qt1
                                    Policy    Policy     Rule
Path                          Policy     Owner     Owner Type Index  Access
----------------------------- ---------- --------- ---------- ------ ----------
/                             default    vs1_root  volume          1 read
/dir1                         default    vs1_root  volume          1 read
/dir1/dir2                    default    vs1_root  volume          1 read
/dir1/dir2/flex1              data       flex_vol  volume         10 read
/dir1/dir2/flex1/qt1          primarynames
                                         qt1       qtree           0 denied
5 entries were displayed.
```

関連タスク

エクスポート ポリシーの作成（42ページ）
エクスポート ポリシーへのルールの追加（43ページ）

関連参照情報

エクスポート ポリシーの管理用コマンド（106ページ）

エクスポート ルールの管理用コマンド（106ページ）

NFSでのKerberos使用によるセキュリティ強化

Kerberosを使用してStorage Virtual Machine（SVM）とNFSクライアント間の認証を強化すると、セキュアなNFS通信を実現することができます。NFSにKerberosを設定すると、NFSクライアントとストレージ システム間の通信の整合性とセキュリティが向上します。

Data ONTAPでのKerberosのサポート

バージョン3以降のNFSはgeneric security services for RPC（RPCSEC_GSS）をサポートしており、Kerberos 5を使用できます。Kerberosは、クライアント / サーバ アプリケーションに対して強力でセキュアな認証を提供し、サーバに対してユーザおよびプロセスのIDの検証機能を提供します。Data ONTAP環境では、KerberosでStorage Virtual Machine（SVM）とNFSクライアント間の認証を実行できます。

Data ONTAP 8.3以降では、次に示す追加のKerberos機能がサポートされます。

- 整合性チェック機能を備えたKerberos 5認証（krb5i）
  Krb5iでは、チェックサムを使用して、クライアントとサーバとの間で転送される各NFSメッセージの整合性を検証します。これは、セキュリティ上の理由（データが改ざんされていないことの保証など）とデータ整合性に関する理由（信頼性の低いネットワーク経由のNFS使用時のデータ破損の防止など）の両方で有用です。
- 128ビットおよび256ビットのAES暗号化
  Advanced Encryption Standard（AES）は電子データを保護するための暗号化アルゴリズムです。Data ONTAPでは、セキュリティ強化のために、128ビット キーによるAES（AES-128）と256ビット キーによるAES（AES-256）がKerberosでサポートされるようになりました。
- SVMレベルのKerberos Realm設定
  SVM管理者は、Kerberos Realm設定をSVMレベルで作成できるようになりました。つまり、SVM管理者は、Kerberos Realm設定に関してクラスタ管理者に頼る必要がなくなり、個別のKerberos Realm設定をマルチテナンシー環境で作成することができます。

NFSでのKerberos使用を設定するための要件

NFSでKerberosを使用するための設定をシステムで行う前に、ネットワークおよびストレージの環境のいくつかの項目について、適切に設定されていることを確認する必要があります。

注: 環境を設定する手順は、クライアントで使用しているオペレーティング システム、ドメイン コントローラ、Kerberos、DNSなどのバージョンや種類によって異なります。このドキュメントでは、それらのすべてについては説明していません。詳細については、それぞれのコンポーネントの対応するドキュメントを参照してください。

Windows Server 2008 R2のActive DirectoryおよびLinuxホストを使用する環境でのclustered Data ONTAPとKerberos 5およびNFSv3 / NFSv4の設定方法に関する詳しい例については、テクニカル レポート4073を参照してください。

次の項目について事前に設定しておく必要があります。

ネットワーク環境の要件

- Kerberos
  KerberosをKey Distribution Center（KDC;キー配布センター）で設定しておく必要があります（たとえば、Windows Active DirectoryベースのKerberosまたはは MIT Kerberos）。
  NFSサーバでは、マシン プリンシパルの主要コンポーネントとして「nfs」を使用する必要があります。

- ディレクトリ サービス
  Active DirectoryやOpenLDAPなど、セキュアなディレクトリ サービスを環境に導入し、SSL/TLS経由のLDAPの使用を設定する必要があります。
- NTP
  タイム サーバでNTPを実行している必要があります。これは、時刻のずれによるKerberos認証の失敗を回避するために必要です。
- ドメイン名解決（DNS）
  それぞれのUNIXクライアントおよびStorage Virtual Machine（SVM）LIFについて、KDCの前方参照ゾーンと逆引き参照ゾーンに適切なサービス レコード（SRV）が登録されている必要があります。すべてのコンポーネントをDNSで正しく解決できなければなりません。
- ユーザ アカウント
  各クライアントについて、Kerberos Realmのユーザ アカウントが必要です。NFSサーバでは、マシン プリンシパルの主要コンポーネントとして「nfs」を使用する必要があります。

NFSクライアントの要件

- NFS
  NFSv3またはNFSv4を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。
  クライアントでRFC1964およびRFC2203がサポートされている必要があります。
- Kerberos
  以下の詳細も含めて、Kerberos認証を使用するように各クライアントが適切に設定されている必要があります。
  - TGS通信に対して暗号化を有効にする。
    AES-256が最も強固なセキュリティ。
  - TGT通信に対して最も安全な暗号化タイプを有効にする。
  - Kerberos Realmとドメインを正しく設定する。
  - GSSを有効にする。

  マシンのクレデンシャルを使用する場合:
  - `-n`パラメータを指定して`gssd`を実行しない。
  - rootユーザとして`kinit`を実行しない。
- 各クライアントのオペレーティング システムが、最新バージョンに更新されている必要があります。
  これにより、KerberosでのAES暗号化について最高の互換性と信頼性が確保されます。
- DNS
  DNSを使用して名前が正しく解決されるように各クライアントが適切に設定されている必要があります。
- NTP
  各クライアントがNTPサーバと同期されている必要があります。
- ホストとドメインの情報
  各クライアントの`/etc/hosts`ファイルと`/etc/resolv.conf`ファイルに、正しいホスト名とDNSの情報が格納されている必要があります。
- keytabファイル

各クライアントについて、KDCのkeytabファイルが必要です。Realmは大文字で指定する必要があります。最高レベルのセキュリティを得るために、暗号化タイプをAES-256にする必要があります。

- オプション：パフォーマンスを最大限に高めるには、ローカル エリア ネットワークとの通信用とストレージ ネットワークとの通信用に、少なくとも2つのネットワーク インターフェイスを設定します。

ストレージ システムの要件

- NFSライセンス
  ストレージ システムに有効なNFSライセンスがインストールされている必要があります。
- CIFSライセンス
  CIFSライセンスはオプションです。マルチプロトコルのネーム マッピングを使用する環境で、Windowsクレデンシャルのチェックを行う場合にのみ必要になります。純粋なUNIXのみの環境では必要ありません。
- SVM
  システムでSVMを少なくとも1つ設定しておく必要があります。
- SVMでのDNS
  それぞれのSVMでDNSを設定しておく必要があります。
- NFSサーバ
  SVMでNFSを設定しておく必要があります。
- AES暗号化
  最高レベルのセキュリティを得るために、KerberosでAES-256暗号化のみを許可するようにNFSサーバを設定する必要があります。
- CIFSサーバ
  マルチプロトコル環境の場合は、SVMでCIFSを設定しておく必要があります。CIFSサーバはマルチプロトコルのネーム マッピングに必要です。
- ボリューム
  SVMで使用するルート ボリュームと少なくとも1つのデータ ボリュームを設定しておく必要があります。
- ルート ボリューム
  SVMのルート ボリュームを次のように設定しておく必要があります。

名前	設定
セキュリティ形式	UNIX
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIXアクセス権	777

  ルート ボリュームとは異なり、データ ボリュームのセキュリティ形式は任意に設定してかまいません。
- UNIXグループ
  SVMで次のUNIXグループを設定しておく必要があります。

グループ名	グループID
daemon	1

グループ名	グループID
root	0
pcuser	65534（SVMを作成するとData ONTAPで自動的に作成されます）

- UNIXユーザ
  SVMで次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザID	プライマリ グループID	コメント
nfs	500	0	GSS INITフェーズで必要 NFSクライアント ユーザのSPNの最初のコンポーネントがユーザとして使用されます。
pcuser	65534	65534	NFSとCIFSのマルチプロトコルで必要 SVMを作成すると、Data ONTAPで自動的に作成されてpcuserグループに追加されます。
root	0	0	マウントに必要

  NFSクライアント ユーザのSPNに対するKerberos-UNIXネーム マッピングがある場合は、nfsユーザは必要ありません。

- エクスポート ポリシーとエクスポート ルール
  ルートおよびデータ ボリュームとqtreeに対するエクスポート ポリシーと必要なエクスポート ルールを設定しておく必要があります。SVMのすべてのボリュームへのアクセスにKerberosを使用する場合は、ルート ボリュームのエクスポート ルール オプションである**-rorule**、**-rwrule**、および**-superuser**を**krb5**または**krb5i**に設定できます。

- Kerberos-UNIXネーム マッピング
  NFSクライアント ユーザのSPNによって識別されたユーザにroot権限を割り当てる場合は、rootへのネーム マッピングを作成する必要があります。

関連情報

ネットアップ テクニカル レポート4073:『Secure Unified Authentication for NFS Kerberos, NFSv4, and LDAP in Clustered Data ONTAP』
NetApp Interoperability Matrix Tool
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

NFS Kerberosで許可される暗号化タイプの設定

Data ONTAPがデフォルトでサポートしている暗号化タイプは、DES、3DES、AES-128、およびAES-256です。特定の環境のセキュリティ要件に合わせて各Storage Virtual Machine（SVM）で許可する暗号化タイプを設定するには、`vserver nfs modify`コマンドと`-permitted-enc-types`パラメータを使用します。

タスク概要

クライアントの互換性を最大にするために、Data ONTAPはデフォルトでセキュリティの弱いDES暗号化とより強いAES暗号化の両方をサポートしています。そのため、たとえば、セキュリティの強化が必要で環境でサポートされている場合は、この手順を使用して、DESと3DESを無効にしてクライアントでAES暗号化のみが使用されるようにすることができます。

- SVMでAESを完全に（AES-128とAES-256の両方を）有効化または無効化するには、SVMのすべてのLIFでKerberos設定を無効にする必要があるため、システムの停止が伴います。この変更を行う前に、NFSクライアントがSVMのAES暗号化に依存していないことを確認します。
- DESや3DESの有効化または無効化は、LIFでのKerberos設定の変更を一切必要としません。

手順

1. 許可される暗号化タイプを必要に応じて有効または無効にします。

有効または無効にする対象	手順

DESまたは3DES	**a.** SVMのNFS Kerberosで許可する暗号化タイプを設定します。
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	複数の暗号化タイプを指定する場合はカンマで区切ります。
	b. 変更が正常に行われたことを確認します。
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`

AES-128またはAES-256	**a.** Kerberosが有効になっているSVMとLIFを特定します。
	`vserver nfs kerberos interface show`
	b. NFS Kerberosで許可する暗号化タイプを変更するSVM上のすべてのLIFでKerberosを無効にします。
	`vserver nfs kerberos interface disable -lif lif_name`
	c. SVMのNFS Kerberosで許可する暗号化タイプを設定します。
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	複数の暗号化タイプを指定する場合はカンマで区切ります。
	d. 変更が正常に行われたことを確認します。
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	e. SVM上のすべてのLIFでKerberosを再び有効にします。
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	f. すべてのLIFでKerberosが有効になっていることを確認します。
	`vserver nfs kerberos interface show`

NFSv4のユーザIDドメインの指定

ユーザIDドメインを指定するには、`-v4-id-domain`オプションを設定します。

タスク概要

NFSv4ユーザIDのマッピングにデフォルトで使用されるドメインは、NISドメインが設定されている場合はNISドメインになります。NISドメインが設定されていない場合はDNSドメインが使用されます。たとえば、複数のユーザIDドメインがあると、ユーザIDドメインの設定が必要になる場合があります。ドメイン名は、ドメイン コントローラのドメインの設定と一致する必要があります。これは、NFSv3の場合は必要ありません。

手順

1. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
   ```

NFS Kerberos realm設定の作成

NFSクライアント アクセスでKerberos認証を使用する場合は、既存のKerberos Realmを使用するようにStorage Virtual Machine（SVM）をまず設定する必要があります。Kerberos Realmを使用するようにSVMを設定するには、`vserver nfs kerberos realm create`コマンドを使用します。

開始する前に

認証の問題を回避するために、クラスタ管理者はストレージ システム、クライアント、およびKDCサーバ上でNTPを設定しておく必要があります。クライアントとサーバとの間の時差（クロック スキュー）が認証エラーの一般的な理由です。

タスク概要

クラスタ管理者は、任意のSVMでKerberos Realmの作成、変更、および削除を行うことができます。SVM管理者は、自らのSVMでのみKerberos Realmの作成、変更、および削除を行うことができます。

手順

1. `vserver nfs kerberos-realm create`コマンドを使用して、Kerberos Realmを設定します。

例

次のコマンドは、Microsoft Active Directoryサーバを KDCサーバとして使用するNFS Kerberos Realm設定をSVM vs1で作成します。Kerberos RealmはAUTH.EXAMPLE.COMです。Active Directoryサーバの名前はad-1で、IPアドレスは10.10.8.14です。許容されるクロック スキューは300秒（デフォルト）です。KDCサーバのIPアドレスは10.10.8.14で、ポート番号は88（デフォルト）です。「Microsoft Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-
port 88 -kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

次のコマンドは、MIT KDCを使用するNFS Kerberos Realm設定をSVM vs1で作成します。Kerberos RealmはSECURITY.EXAMPLE.COMです。許容されるクロック スキューは300秒です。KDCサーバのIPアドレスは10.10.9.1で、ポート番号は88です。KDCベンダーはUNIXベンダーを示すOtherです。管理サーバのIPアドレスは10.10.9.1で、ポート番号は749（デフォルト）です。パスワード サーバのIPアドレスは10.10.9.1で、ポート番号は464（デフォルト）です。「UNIX Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip
10.10.9.1 -adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment
"UNIX Kerberos config"
```

関連参照情報

NFS Kerberos Realm設定の管理用コマンド（106ページ）

NFS Kerberos設定の作成

`vserver nfs kerberos interface enable`コマンドを使用すると、Storage Virtual Machine（SVM）でKerberosを有効にしてKerberos設定を作成できます。これにより、SVMで、NFSのKerberosセキュリティ サービスを使用できます。

タスク概要

最大のパフォーマンスを得るためには、SVMに少なくとも2つのLIFが必要です。1つはNFS Kerberosトラフィックの Service Principal Name（SPN;サービス プリンシパル名）用、もう1つはKerberos以外のトラフィック用です。

注: SVMでpNFSとKerberosを併用する場合は、SVM上のすべてのLIFでKerberosを有効にする必要があります。

Active Directory KDCを使用する場合、使用されるSPNの最初の15文字はRealmまたはドメイン内のSVM間で一意である必要があります。

NFS Kerberos設定を作成すると、Data ONTAPによって次のチェックがSPNに対して行われます。

- 2つの異なるSVMが同じIPspaceにあって同じKDCアカウントを使用している場合、Data ONTAPはそのような設定は許可しません。
- 2つの異なるSVMが異なるIPspaceにあって同じKDCアカウントを使用している場合、Data ONTAPは、追加のチェックを内部で実行するとともに外部のKDCによっても実行し、KDCアカウントがSVM間で共有されている場合にはそのような設定を回避します。

手順

1. NFS Kerberos設定を作成します。

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   Kerberos Realmの異なるOUでSPNを作成する必要がある場合は、オプションの`-ou`パラメータを指定できます。

   Data ONTAPでKerberosインターフェイスを有効にするには、KDCからSPNのシークレット キーを取得する必要があります。このキーは、次の2つの方法のどちらかを使用して取得できます。

状況または条件	コマンドで指定するパラメータ
KDCからキーを直接取得するためのKDC管理者のクレデンシャルがある	`-admin-username` *`kdc_admin_username`*
KDC管理者のクレデンシャルはないが、キーが含まれている、KDCのkeytabファイルはある	`-keytab-uri` {ftp|http}://*`uri`*

   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

次の例は、vs1というSVMのNFS Kerberos設定を、OU lab2ou内のSPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COMを使用して、論理インターフェイスves03-d1に対して作成します。

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver
vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou
"ou=lab2ou"
```

関連参照情報

NFS Kerberosインターフェイス設定の管理用コマンド（105ページ）

ネーム サービスの設定

ストレージ システムの構成によっては、クライアントに適切なアクセスを提供するためにData ONTAPがホスト、ユーザ、グループ、またはネットグループ情報を検索できる必要があります。Data ONTAPがローカルまたは外部のネーム サービスにアクセスしてこれらの情報を取得できるように、ネーム サービスを設定する必要があります。

Data ONTAPのネーム サービス スイッチ設定の仕組み

Data ONTAPでは、UNIXシステムの`/etc/nsswitch.conf`ファイルに相当するテーブルにネーム サービス設定情報が格納されます。このテーブルを環境に応じて適切に設定するためには、その機能とData ONTAPでテーブルがどのように使用されるかを理解しておく必要があります。

ネーム サービス スイッチ テーブルは、Data ONTAPが特定の種類のネーム サービス情報を取得する際にどのネーム サービス ソースをどの順番で参照するかを決定します。ネーム サービス スイッチ テーブルは、Storage Virtual Machine（SVM）ごとに作成および保存されます。

データベース タイプ

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
hosts	ホスト名のIPアドレスへの変換	files、dns
group	ユーザ グループ情報の検索	files、nis、ldap
passwd	ユーザ情報の検索	files、nis、ldap
netgroup	ネットグループ情報の検索	files、nis、ldap
namemap	ユーザ名のマッピング	files、ldap

ソース タイプ

ソース タイプによって、該当する情報を取得するために使用するネーム サービス ソースが決まります。

ソース タイプ	情報の検索先	使用するコマンド

files	ローカルのソース ファイル	`vserver services name-service unix-user`
		`vserver services name-service unix-group`
		`vserver services name-service netgroup`
		`vserver services name-service dns hosts`

nis	SVMのNISドメイン設定で指定された外部のNISサーバ	`vserver services name-service nis-domain`
ldap	SVMのLDAPクライアント設定で指定された外部のLDAPサーバ	`vserver services name-service ldap`
dns	SVMのDNS設定で指定された外部のDNSサーバ	`vserver services name-service dns`

データ アクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、NIS認証またはLDAP認証が失敗した場合に備え、**files**でローカル ユーザも設定しておく必要があります。

外部ソースへのアクセスに使用されるプロトコル

Data ONTAPでは、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部のネーム サービス ソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例では、SVM svm_1のネーム サービス スイッチ情報を表示しています。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files
svm_1           passwd         files
svm_1           netgroup       nis,
                               files
```

ホストのIPアドレス検索では、最初にローカルのソース ファイルが参照され、結果が返されない場合は、次にDNSサーバが照会されます。

ユーザまたはグループ情報の検索では、ローカルのソース ファイルだけが参照され、結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、最初に外部のNISサーバが参照され、結果が返されない場合は、次にローカルのネットグループ ファイルが照会されます。

このSVMのテーブルには、ネーム マッピング用のネーム サービス エントリは含まれていません。そのため、デフォルトの設定に従ってローカルのソース ファイルだけが参照されます。

関連コンセプト

Data ONTAPでのネーム サービスの使用方法（26ページ）

関連情報

ネットアップ テクニカル レポート4379:『Name Services Best Practice Guide Clustered Data ONTAP』

ネーム サービス スイッチ テーブルの設定

Data ONTAPがローカルまたは外部のネーム サービスに問い合わせてホスト、ユーザ、またはグループ情報を取得できるようにするには、ネーム サービス スイッチ テーブルを正しく設定する必要があります。

開始する前に

現在の環境に合わせて、ホスト、ユーザ、グループ、ネットグループ、およびネーム マッピングで使用するネーム サービスを決定しておく必要があります。

ネットグループの使用を計画している場合、ネットグループ内に指定されているすべてのIPv6アドレスは、RFC 5952の既定に沿って短縮されている必要があります。

手順

1. ネーム サービス スイッチ テーブルに必要なエントリを追加します。

   vserver services name-service ns-switch create -vserver *vserver_name* -database *database_name* -sources *source_names*

2. ネーム サービス スイッチ テーブルに想定されるエントリが適切な順序で格納されていることを確認します。

   vserver services name-service ns-switch show -vserver *vserver_name*

   修正が必要な場合は、`vserver services name-service ns-switch modify`または`vserver services name-service ns-switch delete`コマンドを使用します。

例

次の例は、SVM vs1のネーム サービス スイッチ テーブルに新しいエントリを作成し、ローカル ネットグループ ファイル、外部NISサーバ、および外部LDAPサーバを使用して（この順序で）ネットグループ情報を検索するように設定します。

```
cluster::> vserver services name-service ns-switch create -vserver
vs1 -database netgroup -sources files,nis,ldap
```

終了後の操作

SVMに対して指定したネーム サービスを設定する必要があります。ネーム サービスを指定してもその設定を行っていない場合は、ストレージ システムへのクライアント アクセスが想定どおりに機能しない可能性があります。

関連タスク

ネーム サービスに関する問題のトラブルシューティング（97ページ）

関連参照情報

ネーム サービス スイッチ エントリの管理用コマンド（100ページ）

関連情報

ネットアップ テクニカル レポート4379:『Name Services Best Practice Guide Clustered Data ONTAP』
IETF RFC 5952:『A Recommendation for IPv6 Address Text Representation』

LDAPの使用

LDAPサーバを使用すると、ユーザ情報を一元的に管理できます。ユーザ データベースを環境内のLDAPサーバに格納している場合、既存のLDAPデータベース内のユーザ情報を検索するようにストレージ システムを設定できます。

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）TSL/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ベースの 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。

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 *vserver_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 *vserver_name*

SSL/TLS経由のLDAPの有効化

Storage Virtual Machine（SVM）でLDAPサーバに対するセキュアな通信を使用するには、SVMのLDAPクライアントを変更して、SSL/TLS経由のLDAPを有効にする必要があります。

開始する前に

LDAPサーバの自己署名ルートCA証明書をSVMにインストールしておく必要があります。

手順

1. LDAPサーバとのセキュアなLDAP通信を許可するようにLDAPクライアントを設定します。
   vserver services name-service ldap client modify -vserver *vserver_name* -client-config *ldap_client_config_name* -use-start-tls true
2. SSL/TLS経由のLDAPの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 services name-service ldap client show -vserver *vserver_name*

新しいLDAPクライアント スキーマの作成

Data ONTAPには、3つのLDAPスキーマが用意されています。UNIXとの互換性に対応するActive Directory Services用、UNIXとの互換性に対応するActive Directory Identity Management用、およ

びRFC-2307 LDAPとの互換性用の3つです。環境で使用するLDAPスキーマがこれらと異なる場合は、Data ONTAP用の新しいLDAPクライアント スキーマを作成する必要があります。

タスク概要

Data ONTAPに用意されているデフォルトのLDAPスキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、そのコピーを必要に応じて変更します。

手順

1. 既存のLDAPクライアント スキーマ テンプレートを表示して、コピーするスキーマを特定します。

   ```
   vserver services name-service ldap client schema show
   ```

2. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

3. 既存のLDAPクライアント スキーマのコピーを作成します。

   ```
   vserver services name-service ldap client schema copy -vserver
   vserver_name -schema existing_schema_name -new-schema-name
   new_schema_name
   ```

4. `vserver services name-service ldap client schema modify`コマンドを使用して、新しいスキーマを変更し、環境に合わせてカスタマイズします。

   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。

5. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

関連タスク

LDAPのRFC2307bisサポートの有効化（66ページ）

関連参照情報

LDAPクライアント スキーマ テンプレートの管理用コマンド（105ページ）

LDAPのRFC2307bisサポートの有効化

LDAPを使用し、ネストされたグループ メンバーシップを使用する機能が追加で必要な場合は、Data ONTAPを設定してLDAPのRFC2307bisサポートを有効にすることができます。

開始する前に

デフォルトのLDAPクライアント スキーマのうち、使用するいずれか1つのコピーを作成しておく必要があります。

タスク概要

LDAPクライアント スキーマでは、グループ オブジェクトがmemberUid属性を使用します。この属性には、グループに属するユーザの名前を複数指定できます。RFC2307bis対応のLDAPクライアント スキーマでは、グループ オブジェクトがuniqueMember属性を使用します。この属性には、LDAPディレクトリ内の別のオブジェクトの完全なDistinguished Name（DN;識別名）を指定できます。これにより、グループに他のグループをメンバーとして追加できるため、ネストされたグループを使用することができます。

ユーザは、ネストされたグループを含めて256を超えるグループのメンバーになることはできません。Data ONTAPは256を超えたグループをすべて無視します。

デフォルトでは、RFC2307bisサポートは無効になっています。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. コピーしたRFC2307 LDAPクライアント スキーマを変更して、RFC2307bisサポートを有効にします。

   ```
   vserver services name-service ldap client schema modify -vserver
   vserver_name -schema schema-name -enable-rfc2307bis true
   ```

3. LDAPサーバでサポートされているオブジェクト クラスに一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver
   vserver-name -schema schema_name -group-of-unique-names-object-class
   object_class
   ```

4. LDAPサーバでサポートされている属性名に一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver
   vserver-name -schema schema_name -unique-member-attribute attribute_name
   ```

5. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

関連タスク

LDAPクライアント設定の作成（69ページ）
新しいLDAPクライアント スキーマの作成（65ページ）

関連参照情報

LDAPクライアント設定の管理用コマンド（104ページ）

LDAPディレクトリ検索の設定オプション

環境に応じて最も適切な方法でLDAPサーバに接続するようにLDAPクライアントを構成することで、ユーザ、グループ、およびネットグループ情報を含め、LDAPディレクトリ検索を最適化することができます。デフォルトのLDAPベースおよびスコープ検索値で十分な状況や、カスタム値のほうが適切な場合に指定すべきパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報のLDAPクライアント検索オプションは、LDAPクエリの失敗、ひいてはストレージ システムへのクライアント アクセスの失敗を回避するのに役立ちます。また、検索をできるだけ効率的にしてクライアントのパフォーマンスに関する問題を回避するのにも役立ちます。

デフォルトのベースおよびスコープ検索値

LDAPベースは、LDAPクライアントがLDAPクエリを実行するために使用するデフォルトのベースDNです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベースDNを使用して行われます。デフォルトの設定は、LDAPディレクトリが比較的小さくてすべての関連エントリが同じDN内にある場合に適しています。

カスタムのベースDNを指定しない場合、デフォルト値は**root**で、各クエリでディレクトリ全体が検索されます。LDAPクエリが成功する可能性は最大になりますが、非効率的であるため、大きなLDAPディレクトリではパフォーマンスの大幅な低下につながる可能性があります。

LDAPベース スコープは、LDAPクライアントがLDAPクエリを実行するために使用するデフォルトのベース スコープです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベース スコープを使用して行われます。ベース スコープに基づいて、LDAPクエリによる検索範囲を名前

付きエントリのみ、DNの1レベル下にあるエントリ、またはDNの下にあるサブツリー全体のどれにするかが決まります。

カスタムのベース スコープを指定しない場合、デフォルト値は**subtree**で、各クエリでDNの下にあるサブツリー全体が検索されます。LDAPクエリが成功する可能性は最大になりますが、非効率的であるため、大きなLDAPディレクトリではパフォーマンスの大幅な低下につながる可能性があります。

カスタムのベースおよびスコープ検索値

必要に応じて、ユーザ、グループ、およびネットグループ検索で、別々のベースおよびスコープ値を指定できます。クエリの検索ベースおよびスコープをこのようにして制限すると、検索対象がLDAPディレクトリのサブセクションに限定されるため、パフォーマンスが大幅に向上します。

カスタムのベースおよびスコープ値を指定した場合、ユーザ、グループ、およびネットグループ検索に対するデフォルトの検索ベースおよびスコープは無視されます。カスタムのベースおよびスコープ値を指定するパラメータは、advanced権限レベルで使用できます。

LDAPクライアント パラメータ	カスタム値の指定対象
`-base-dn`	すべてのLDAP検索のベースDN
`-base-scope`	すべてのLDAP検索のベース スコープ
`-user-dn`	すべてのLDAPユーザ検索のベースDN このパラメータはユーザ名マッピング検索にも適用されます。
`-user-scope`	すべてのLDAPユーザ検索のベース スコープ このパラメータはユーザ名マッピング検索にも適用されます。
`-group-dn`	すべてのLDAPグループ検索のベースDN
`-group-scope`	すべてのLDAPグループ検索のベース スコープ
`-netgroup-dn`	すべてのLDAPネットグループ検索のベースDN
`-netgroup-scope`	すべてのLDAPネットグループ検索のベース スコープ

複数のカスタム ベースDN値

LDAPディレクトリの構成が複雑な場合は、LDAPディレクトリの複数の部分で特定の情報を検索するために、複数のベースDNの指定が必要になることがあります。ユーザ、グループ、およびネットグループに複数のDNパラメータを指定するには、各パラメータをセミコロンで区切り、DN検索リスト全体を二重引用符（"）で囲みます。DNにセミコロンが含まれる場合、DN内のセミコロンの直前にエスケープ文字（\）を追加する必要があります。

スコープは、対応するパラメータに対して指定したDNリスト全体に適用されることに注意してください。たとえば、ユーザ スコープに対して3つの異なるユーザDNのリストとサブツリーを指定した場合、指定した3つのDNのそれぞれでサブツリー全体が検索されます。

関連タスク

LDAPクライアント設定の作成（69ページ）

関連参照情報

LDAPクライアント設定の管理用コマンド（104ページ）

LDAPクライアント設定の作成

Data ONTAPが環境内の外部LDAPサーバにアクセスしてLDAPディレクトリに格納された情報を検索できるようにするには、最初にストレージ システムにLDAPクライアントをセットアップする必要があります。このLDAPクライアント設定を作成するには、`vserver services name-service ldap client create`コマンドを使用します。

手順

1. LDAPクライアント設定を作成します。

   vserver services name-service ldap client create -vserver *vserver_name* -client-config *client_config_name* {-servers *LDAP_server_list* | -ad-domain *ad_domain* -preferred-ad-servers *preferred_ad_server_list* -bind-as-cifs-server {true|false}} -schema *schema* -port *port* -query-timeout *integer* -min-bind-level {anonymous|simple|sasl} -bind-dn *LDAP_DN* -bind-password *password* -base-dn *LDAP_DN* -base-scope {base|onelevel|subtree}

   `-vserver` *vserver_name*には、LDAPクライアント設定を作成するSVMの名前を指定します。

   `-client-config` *client_config_name*には、新しいLDAPクライアント設定の名前を指定します。SVMがデフォルト以外のIPspaceにある場合は、クラスタ管理者によって作成されたLDAPクライアント設定を割り当てることができません。

   `-servers` *LDAP_server_list*には、1つ以上のLDAPサーバのIPアドレスをカンマで区切って指定します。

   `-ad-domain` *ad_domain*では、Active Directoryドメインを指定します。

   `-preferred-ad-servers` *preferred_ad_server_list*には、1つ以上の優先されるActive Directoryサーバ のIPアドレスをカンマで区切って指定します。

   `-bind-as-cifs-server` {**true**|**false**}は、SVMのCIFSクレデンシャルを使用してバインドするかどうかを指定します。デフォルトは**false**です。このパラメータを**true**に設定する場合は、まず、CIFSライセンスをインストールし、CIFSサーバを作成する必要があります。

   `-schema` *schema*には、使用するスキーマ テンプレートを指定します。用意されているデフォルト スキーマのいずれかを使用するか、デフォルト スキーマ（読み取り専用です）をコピーし、そのコピーを変更して独自のスキーマを作成します。

   `-port` *port*には、LDAPサーバ ポートを指定します。デフォルトは**389**です。Start TLSを使用したLDAP接続の保護を予定している場合は、デフォルトのポート389を使用する必要があります。Start TLSはLDAPのデフォルト 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。ポートを変更した場合、Start TLSは失敗します。

   `-query-timeout` *integer*には、クエリ タイムアウト（秒）を指定します 指定できる値の範囲は0～10秒です。デフォルト値は**3**秒です

   `-min-bind-level` {**anonymous**|**simple**|**sasl**}は、最小バインド認証レベルを指定します。デフォルトは**anonymous**です。

   `-bind-dn` *LDAP_DN*には、バインド ユーザを指定します。Active Directoryサーバの場合は、アカウント（DOMAIN\user）またはプリンシパル（user@domain.com）の形式でユーザを指定します。それ以外の場合は、識別名（CN=user,DC=domain,DC=com）の形式でユーザを指定します。

   `-bind-password` *password*には、バインド パスワードを指定します。

   `-base-dn` *LDAP_DN*には、ベースDNを指定します。デフォルトは**""**（ルート）です。

   `-base-scope` {**base**|**onelevel**|**subtree**}は、ベース検索スコープを指定します。デフォルトは**subtree**です。

`-use-start-tls {true|false}`では、LDAP接続でStart TLSを使用するかどうかを指定します。LDAPサーバがStart TLSをサポートしている場合、**true**に設定すると、LDAPクライアントはサーバに対する暗号化されたTLS/SSL接続を使用します。デフォルトは**false**です。このオプションを使用するには、LDAPサーバの自己署名ルートCA証明書をインストールする必要があります。

2. LDAPクライアント設定が正常に作成されたことを確認します。

   vserver services name-service ldap client show -client-config client_config_name

例

次のコマンドでは、LDAPのActive Directoryサーバと連携するためにSVM vs1で「ldap1」という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -
vserver vs1 -client-config ldapclient1 –ad-domain
addomain.example.com -bind-as-cifs-server true -schema AD-SFU -port
389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-
servers 172.17.32.100
```

次のコマンドは、SVM vs1の「ldap1」というLDAPクライアント設定を変更し、Active Directoryドメインを指定してLDAPのActive Directoryサーバと連携させ、SVMのCIFSクレデンシャルを使用してこのサーバにバインドするようにします。

```
cluster1::> vserver services name-service ldap client modify -
vserver vs1 -client-config ldap1 -bind-as-cifs-server true -ad-
domain addomain.example.com
```

次のコマンドでは、ベースDNを指定することで、SVM vs1で「ldap1」という名前のLDAPクライアント設定を変更します。

```
cluster1::> vserver services name-service ldap client modify -
vserver vs1 -client-config ldap1 -base-dn
CN=Users,DC=addomain,DC=example,DC=com
```

関連コンセプト

LDAPディレクトリ検索の設定オプション（67ページ）

関連タスク

LDAPディレクトリのホスト単位ネットグループ検索のパフォーマンス向上（70ページ）

関連参照情報

LDAPクライアント設定の管理用コマンド（104ページ）

LDAPディレクトリのホスト単位ネットグループ検索のパフォーマンス向上

LDAP環境がホスト単位のネットグループ検索を許可するように設定されている場合は、この機能を使用するようにData ONTAPを設定し、ホスト単位のネットグループ検索を実行することができま

す。これにより、ネットグループ検索の処理速度を大幅に向上させ、ネットグループ検索時の遅延が原因のNFSクライアント アクセスの問題を削減することができます。

開始する前に

LDAPディレクトリに`netgroup.byhost`マップが含まれている必要があります。

DNSサーバに、NFSクライアントに対するフォワード（A）およびリバース（PTR）ルックアップ レコードの両方が含まれている必要があります。

ネットグループにIPv6アドレスを指定する際には、RFC 5952の規定に従って各アドレスを短縮する必要があります。

タスク概要

NISサーバは、`netgroup`、`netgroup.byuser`、および`netgroup.byhost`という3つのマップにネットグループ情報を格納します。`netgroup.byuser`マップと`netgroup.byhost`マップの目的は、ネットグループ検索の速度を向上することにあります。Data ONTAP 8.3以降では、NISサーバでホスト単位のネットグループ検索を実行でき、マウントの応答時間を短縮できます。

デフォルトでは、LDAPディレクトリにはNISサーバと違って`netgroup.byhost`マップがありません。ただし、サードパーティ ツールを利用してNISの`netgroup.byhost`マップをLDAPディレクトリにインポートすれば、高速なホスト単位のネットグループ検索を実行できるようになります。ホスト単位のネットグループ検索許可するようにLDAP環境を設定している場合は、Data ONTAP LDAP クライアントに`netgroup.byhost`マップ名、DN、および検索範囲を設定してより高速なホスト単位のネットグループ検索を実行できます。

ホスト単位のネットグループ検索の結果をより迅速に受け取ることで、Data ONTAPは、NFSクライアントがエクスポートへのアクセスを要求した場合により短時間でエクスポート ルールを処理できます。その結果、ネットグループ検索の遅延によってアクセスが遅延することが少なくなります。

手順

1. LDAPディレクトリにインポートしたNISの`netgroup.byhost`マップの完全な識別名（DN）を取得します。

   マップのDNは、インポートに使用したサードパーティ ツールによって異なります。最高のパフォーマンスを得るためには、正確なマップDNを指定してください。

2. 権限レベルをadvancedに設定します。

   `set -privilege advanced`

3. Storage Virtual Machine（SVM）のLDAPクライアント設定でホスト単位のネットグループ検索を有効にします。

   `vserver services name-service ldap client modify -vserver` *`vserver_name`* `-client-config` *`config_name`* `-is-netgroup-byhost-enabled true -netgroup-byhost-dn` *`netgroup-by-host_map_distinguished_name`* `-netgroup-byhost-scope` *`netgroup-by-host_search_scope`*

   `-is-netgroup-byhost-enabled` {**`true`**|**`false`**}は、LDAPディレクトリのホスト単位のネットグループ検索を有効または無効にします。デフォルトは**`false`**です。

   `-netgroup-byhost-dn` *`netgroup-by-host_map_distinguished_name`*では、LDAPディレクトリ内の`netgroup.byhost`マップの識別名を指定します。この指定により、ホスト単位のネットグループ検索のベースDNが上書きされます。このパラメータを指定しない場合、Data ONTAPは代わりにベースDNを使用します。

   `-netgroup-byhost-scope` {**`base`**|**`onelevel`**|**`subtree`**}では、ホスト単位のネットグループ検索の検索範囲を指定します。このパラメータを指定しない場合、デフォルトの**`subtree`**が使用されます。

LDAPクライアント設定がない場合は、`vserver services name-service ldap client create`コマンドを使用して新しいLDAPクライアント設定を作成する際に、これらのパラメータを指定してホスト単位のネットグループ検索を有効にします。

4. admin権限レベルに戻ります。

   `set -privilege admin`

例

次のコマンドは、「nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com」という`netgroup.byhost`マップとデフォルトの検索範囲である**`subtree`**を使用して、ホスト単位のネットグループ検索を有効にするように、「ldap_corp」という既存のLDAPクライアント設定を変更します。

```
cluster1::*> vserver services name-service ldap client modify -
vserver vs1 -client-config ldap_corp -is-netgroup-byhost-enabled
true -netgroup-byhost-dn
nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

終了後の操作

クライアント アクセスの問題が発生しないよう、`netgroup.byhost`とディレクトリ内の`netgroup`マップは常に同期されている必要があります。

関連タスク

LDAPクライアント設定の作成（69ページ）

関連情報

IETF RFC 5952:『A Recommendation for IPv6 Address Text Representation』

SVMでのLDAPの有効化

`vserver services name-service ldap create`コマンドを使用して、Storage Virtual Machine（SVM）でLDAPを有効にし、作成したLDAPクライアントを使用するように設定できます。これにより、SVMでLDAPをネーム マッピングに使用できます。

開始する前に

LDAPクライアント設定がSVM上に存在している必要があります。

手順

1. SVMでLDAPを有効にします。

   `vserver services name-service ldap create -vserver *vserver_name* -client-config *client_config_name* -client-enabled true`

   `-vserver` *`vserver_name`*には、SVM名を指定します。

   `-client-config` *`client_config_name`*には、クライアント設定の名前を指定します。

   `-client-enabled`は、LDAPクライアントを有効にするかどうかを指定します。デフォルトは**`true`**です。

例

次のコマンドは、「vs1」というSVMでLDAPを有効にし、「ldap1」という名前のLDAPクライアント設定を使用するように設定します。

```
cluster1::> vserver services name-service ldap create -vserver vs1 -
client-config ldap1 -client-enabled true
```

関連参照情報

LDAP設定の管理用コマンド（104ページ）

LDAPを使用するためのSVMの設定

環境内のLDAPサーバを使用してネットワーク情報を取得するようにStorage Virtual Machine（SVM）を設定できます。ネットワーク情報やネーム マッピングのソースを設定するには、SVMのネーム サービス設定を変更します。

手順

1. 次のいずれかを実行します。

SVMでLDAPを使用して検索する対象	入力するコマンド
ユーザ情報	**vserver services name-service ns-switch create -vserver *vserver_name* -database passwd -sources ldap,files**
グループ情報	**vserver services name-service ns-switch create -vserver *vserver_name* -database group -sources ldap,files**
ネットグループ情報	**vserver services name-service ns-switch create -vserver *vserver_name* -database netgroup -sources ldap,files**
ネーム マッピング情報	**vserver services name-service ns-switch create -vserver *vserver_name* -database namemap -sources ldap,files**

ネットグループ検索でLDAPを使用する計画の場合：

- フォワードおよびリバースDNSルックアップの一貫性を確保するために、ネットグループ内のすべてのホストにフォワード（A）およびリバース（PTR）の両方のDNSレコードがある必要があります。また、あるクライアントのIPアドレスに複数のPTRレコードがある場合は、それらすべてのホスト名がネットグループのメンバーで、対応するAレコードが定義されている必要があります。
- ネットグループ内に指定されているすべてのIPv6アドレスは、RFC 5952の既定に沿って短縮されている必要があります。

namemapでは、ネーム マッピング情報を検索するためのソースとその検索順序を指定します。UNIXのみの環境では、このエントリは必要ありません。ネーム マッピングは、UNIXとWindowsの両方を使用する混在環境でのみ必要になります。

データ アクセスとSVM管理者の両方の認証にLDAPを使用する場合も、LDAP認証が失敗した場合に備え、filesでローカル ユーザを設定しておく必要があります。

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。

関連コンセプト

Data ONTAPでのネーム サービスの使用方法（26ページ）
ネーム マッピングの使用方法（80ページ）

関連情報

IETF RFC 5952:『A Recommendation for IPv6 Address Text Representation』

NISドメイン設定の作成

Storage Virtual Machine（SVM）のセットアップ時にNISをネーム サービス オプションとして指定した場合は、SVMのNISドメイン設定を作成する必要があります。`vserver services name-service nis-domain create`コマンドを使用して、NISドメイン設定を作成できます。

タスク概要

複数のNISドメインを作成できます。ただし、使用できるのは、**active**に設定されているドメインだけです。

NISデータベースに`netgroup.byhost`マップが格納されている場合、Data ONTAPはこのマップを使用して検索を高速化できます。クライアント アクセスの問題が発生しないよう、`netgroup.byhost`とディレクトリ内の`netgroup`マップは常に同期されている必要があります。

手順

1. `vserver services nis-domain create`コマンドを使用して、NISドメイン設定を作成します。

   最大10台のNISサーバを指定できます。

   設定されているすべてのNISサーバが使用可能かつ到達可能である必要があります。設定したNISサーバのいずれかがあとになって永続的に使用不可能になった場合は、そのサーバを（`vserver services name-service nis-domain modify`コマンドを使用して）NISドメイン設定から削除して、発生しうるNIS機能の遅れを回避してください。

   ディレクトリ検索でのNISの使用を予定している場合、NISサーバ内のマップに1,024文字を超えるエントリを持たせることはできません。この上限に従っていないNISサーバを指定しないでください。そうしないと、NISエントリに依存したクライアント アクセスに失敗する可能性があります。

   ネットグループ検索でのNISの使用を予定している場合：

   - フォワードおよびリバースDNSルックアップの一貫性を確保するために、ネットグループ内のすべてのホストにフォワード（A）およびリバース（PTR）の両方のDNSレコードがある必要があります。また、あるクライアントのIPアドレスに複数のPTRレコードがある場合は、それらすべてのホスト名がネットグループのメンバーで、対応するAレコードが定義されている必要があります。
   - ネットグループ内に指定されているすべてのIPv6アドレスは、RFC 5952の既定に沿って短縮されている必要があります。

例

次のコマンドは、IPアドレス192.0.2.180のNISサーバを使用して、SVM vs1上でnisdomainというNISドメインのNISドメイン設定を作成してアクティブにします。

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -servers 192.0.2.180
```

関連参照情報

NISドメイン設定の管理用コマンド（103ページ）

関連情報

IETF RFC 5952:『A Recommendation for IPv6 Address Text Representation』

ローカルUNIXユーザおよびグループの設定

ローカルUNIXユーザおよびグループは、認証やネーム マッピングに使用できます。

ローカルUNIXユーザの作成

`vserver services name-service unix-user create`コマンドを使用すると、ローカルUNIXユーザを作成できます。ローカルUNIXユーザは、UNIXネーム サービス オプションとしてStorage Virtual Machine（SVM）上に作成するUNIXユーザであり、ネーム マッピングの処理で使用します。

タスク概要

クラスタ内のローカルUNIXユーザ数に対するデフォルトの上限値は32,768です。クラスタ管理者はこの制限を変更できます。

手順

1. ローカルUNIXユーザを作成します。

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-vserver` *`vserver_name`*には、SVM名を指定します。

   `-user` *`user_name`*には、ユーザ名を指定します。ユーザ名は64文字以内にする必要があります。

   `-id` *`integer`*には、ユーザIDを指定します。

   `-primary-gid` *`integer`*には、プライマリ グループIDを指定します。この操作ではユーザはグループには追加されません。ユーザを作成したあと、手動でユーザを適切なグループに追加する必要があります。

   `-full-name` *`full_name`*には、ユーザのフルネームを指定します。

例

次のコマンドは、johnmというローカルUNIXユーザ（フルネームは「John Miller」）をSVM vs1上に作成します。ユーザIDは123で、プライマリ グループIDは100です。

```
node::> vserver services name-service unix-user create -vserver vs1
-user johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

終了後の操作

希望するローカルUNIXグループにユーザを追加します。

関連コンセプト

ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限（102ページ）

関連タスク

ローカルUNIXユーザおよびグループに対する制限の管理（102ページ）

関連参照情報

ローカルUNIXユーザの管理用コマンド（101ページ）

ローカルUNIXグループへのユーザの追加

`vserver services name-service unix-group adduser`コマンドを使用すると、Storage Virtual Machine（SVM）のローカルのUNIXグループにユーザを追加できます。

タスク概要

クラスタ内のローカルUNIXグループおよびグループ メンバーの合計数に対するデフォルトの上限値は32,768です。クラスタ管理者はこの制限を変更できます。

手順

1. ローカルUNIXグループにユーザを追加します。

   `vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

   `-vserver` *`vserver_name`*には、SVM名を指定します。

   `-name` *`group_name`*で、ユーザを追加する UNIXグループの名前を指定します。

   `-username` *`user_name`*で、グループに追加するユーザの名前を指定します。

例

次に、vs1というSVMのengというローカルUNIXグループに、maxという名前のユーザを追加するコマンドの例を示します。

```
vs1::> vserver services name-service unix-group adduser -vserver
vs1 -name eng
-username max
```

関連コンセプト

ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限（102ページ）

関連タスク

ローカルUNIXユーザおよびグループに対する制限の管理（102ページ）

URIからのローカルUNIXユーザのロード

Storage Virtual Machine（SVM）にローカルUNIXユーザを1つずつ手動で作成する代わりに、`vserver services name-service unix-user load-from-uri`コマンドを使用して、ローカルUNIXユーザのリストをUniform Resource Identifier（URI）からSVMにロードすることで作業の手間を削減できます。

タスク概要

クラスタ内のローカルUNIXユーザ数に対するデフォルトの上限値は32,768です。クラスタ管理者はこの制限を変更できます。

手順

1. ロードするローカルUNIXユーザのリストが含まれているファイルを作成します。

このファイルには、次に示すUNIXの/etc/passwd形式でユーザ情報が記されている必要があります。
user_name: *password*: *user_ID*: *group_ID*: *full_name*

*password*フィールドの値と、*full_name*フィールドに続くフィールド（*home_directory*および*shell*）の値はコマンドにより破棄されます。

サポートされる最大ファイル サイズは2.5MBです。

クラスタ内のローカルUNIXユーザ数に対するデフォルトの上限値は32,768です。クラスタ管理者はこの制限を変更できます。

2. リストに重複した情報が含まれていないことを確認します。

   リストに重複したエントリが含まれている場合、リストのロードは失敗し、エラー メッセージが表示されます。

3. ファイルをサーバにコピーします。

   サーバには、ストレージ システムからHTTP、HTTPS、FTP、またはFTPS経由で到達できる必要があります。

4. ファイルのURIを確認します。

   このURIは、ファイルの場所をストレージ システムに示すためのアドレスです。

   例

   ```
   ftp://ftp.example.com/passwd
   ```

5. ローカルUNIXユーザのリストが含まれているファイルをURIからSVMにロードします。

   vserver services name-service unix-user load-from-uri -vserver *vserver_name* -uri {ftp|http|ftps|https}://*uri* -overwrite {true|false}

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

   -uri {**ftp**|**http**|**ftps**|**https**}://*uri*には、ファイルのロードに使用するURIを指定します。

   -overwrite {**true**|**false**}で、既存の情報を上書きするかどうかを指定します。デフォルトは**false**です。

例

次のコマンドは、ローカルUNIXユーザのリストをftp://ftp.example.com/passwdというURIからvs1というSVMにロードします。SVM内の既存のユーザは、URIを使用してロードした情報によって上書きされません。

```
node::> vserver services name-service unix-user load-from-uri -
vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

関連コンセプト

ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限（102ページ）

関連タスク

ローカルUNIXユーザおよびグループに対する制限の管理（102ページ）

ローカルUNIXグループの作成

`vserver services name-service unix-group create`コマンドを使用すると、Storage Virtual Machine（SVM）のローカルのUNIXグループを作成できます。ローカルUNIXグループはローカルUNIXユーザとともに使用します。

タスク概要

クラスタ内のローカルUNIXグループおよびグループ メンバーの合計数に対するデフォルトの上限値は32,768です。クラスタ管理者はこの制限を変更できます。

手順

1. ローカルUNIXグループを作成します。

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-vserver` *`vserver_name`*には、SVM名を指定します。

   `-name` *`group_name`*には、グループ名を指定します。グループ名は64文字以内にする必要があります。

   `-id` *`integer`*には、グループIDを指定します。

例

次のコマンドは、vs1という名前のSVM上にengという名前のローカル グループを作成します。グループIDは101です。

```
vs1::> vserver services name-service unix-group create -vserver vs1
-name eng -id 101
```

関連コンセプト

ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限（102ページ）

関連タスク

ローカルUNIXユーザおよびグループに対する制限の管理（102ページ）

関連参照情報

ローカルUNIXグループの管理用コマンド（101ページ）

URIからのローカルUNIXグループのロード

ローカルUNIXグループを1つずつ手動で作成する代わりに、`vserver services name-service unix-group load-from-uri`コマンドを使用して、ローカルUNIXグループのリストをUniform Resource Identifier（URI;ユニバーサル リソース識別子）からStorage Virtual Machine（SVM）にロードすることもできます。

タスク概要

クラスタ内のローカルUNIXグループおよびグループ メンバーの合計数に対するデフォルトの上限値は32,768です。クラスタ管理者はこの制限を変更できます。

手順

1. ロードするローカルUNIXグループのリストが含まれているファイルを作成します。
   このファイルには、次に示すUNIXの`/etc/group`形式でグループ情報が記されている必要があります。
   `group_name``:` *`password`*`:` *`group_ID`*`:` *`comma_separated_list_of_users`*

   *`password`*フィールドの値はコマンドにより破棄されます。

   サポートされる最大ファイル サイズは1MBです。

   グループ ファイルの1行の最大長は、32,768文字です。

2. リストに重複した情報が含まれていないことを確認します。
   重複したエントリがリストに含まれていると、リストのロードに失敗します。すでにSVMに存在するエントリがある場合は、`-overwrite`パラメータを**`true`**に設定してすべての既存エントリを新しいファイルによって上書きするか、新しいファイルに既存のエントリと重複するエントリが一切含まれていないようにする必要があります。

3. ファイルをサーバにコピーします。
   サーバには、ストレージ システムからHTTP、HTTPS、FTP、またはFTPS経由で到達できる必要があります。

4. ファイルのURIを確認します。
   このURIは、ファイルの場所をストレージ システムに示すためのアドレスです。

   例

   `ftp://ftp.example.com/group`

5. ローカルUNIXグループのリストが含まれているファイルをURIからSVMにロードします。

   `vserver services name-service unix-group load-from-uri -vserver` ***`vserver_name`*** **`-uri {ftp|http|ftps|https}://`*`uri`*` -overwrite {true|false}`**

   `-vserver` *`vserver_name`*には、SVM名を指定します。

   `-uri` {**`ftp`**|**`http`**|**`ftps`**|**`https`**}://*`uri`*には、ファイルのロードに使用するURIを指定します。

   `-overwrite` {**`true`**|**`false`**}で、既存の情報を上書きするかどうかを指定します。デフォルトは**`false`**です。このパラメータに**`true`**を指定した場合、Data ONTAPは、指定されたSVMの既存のローカルUNIXグループ データベース全体を、ロードするファイルに含まれているエントリで置き換えます。

例

次のコマンドは、ローカルUNIXグループのリストを`ftp://ftp.example.com/group`というURIを使用してvs1というSVMにロードします。SVM内の既存のグループは、URIを使用してロードした情報によって上書きされません。

```
vs1::> vserver services name-service unix-group load-from-uri -
vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

関連コンセプト

ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限（102ページ）

関連タスク

ローカルUNIXユーザおよびグループに対する制限の管理（102ページ）

ネーム マッピングの使用方法

Data ONTAPでは、ネーム マッピングを使用して、CIFS IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをCIFS IDにマッピングします。この情報は、NFSクライアントからの接続かCIFSクライアントからの接続かに関係なく、ユーザ クレデンシャルを取得して適切なファイル アクセスを提供するために必要になります。

通常、ネーム マッピングは、Data ONTAPがマルチプロトコル対応であり、同じデータへのCIFSクライアントとNFSクライアントのアクセスをサポートすることが理由で必要となります。FlexVolを備えたStorage Virtual Machine（SVM）に格納されているデータでは、UNIXまたはNTFS形式のアクセス権が使用されます。クライアントが許可されるには、クレデンシャルがセキュリティ形式と一致する必要があります。次のシナリオを考えてみましょう。

CIFSクライアントがUNIX形式のアクセス権を使用するデータにアクセスしようとする場合、UNIX形式のアクセス権に対してCIFSクレデンシャルを使用することはできないため、Data ONTAPではクライアントを直接許可できません。クライアント要求を適切に許可するには、Data ONTAPではまず、CIFSクレデンシャルを適切なUNIXクレデンシャルにマッピングし、UNIXクレデンシャルを使用してUNIX形式のアクセス権と比較できるようにする必要があります。

NFSクライアントがNTFS形式のアクセス権を使用するデータにアクセスしようとする場合、NTFS形式のアクセス権に対してUNIXクレデンシャルを使用することはできないため、Data ONTAPではクライアントを直接許可できません。クライアント要求を適切に許可するには、Data ONTAPではまず、UNIXクレデンシャルを適切なNTFSクレデンシャルにマッピングし、NTFSクレデンシャルを使用してNTFS形式のアクセス権と比較できるようにする必要があります。

ネーム マッピングを使用する必要がない例外が2つあります。

- 純粋なUNIX環境を構成しており、ボリュームに対してCIFSアクセスまたはNTFSセキュリティ形式を使用する予定がない場合。
  このシナリオでは、NFSクライアントのUNIXクレデンシャルを使用してUNIX形式のアクセス権と直接比較できるため、ネーム マッピングは必要ありません。
- 代わりにデフォルト ユーザが使用されるように設定している場合。
  このシナリオでは、すべてのクライアント クレデンシャルをそれぞれマッピングするのではなく、すべてのクライアント クレデンシャルが同じデフォルト ユーザにマッピングされるため、ネーム マッピングは必要ありません。

ネーム マッピングはユーザに対してのみ使用でき、グループに対しては使用できません。CIFSユーザをGroup ID（GID;グループID）にマッピングしたり、UNIXユーザをActive Directory（AD）内のグループにマッピングしたりすることはできません。同様に、GIDをAD内のグループまたはユーザにマッピングしたり、ADグループをUNIX UIDまたはGIDにマッピングしたりすることもできません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、SALESという単語が先頭または末尾に付くすべてのADユーザを、特定のUNIXユーザおよびそのユーザのUIDにマッピングできます。そのため、AD内の特定のユーザの名前を変更し、正規表現を使用してグループ アクションを効果的にエミュレートすることができます。このようなマッピングは、逆方向に行うこともできます。

関連コンセプト

ネーム マッピングの仕組み（81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)。デフォルトの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。

関連コンセプト

ネーム マッピングの使用方法(80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。 **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。

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。

あるユーザがルールに一致して別のドメインのユーザ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 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ユーザが、「jones」というUNIXユーザに変換されます。

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る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jOeはjOe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jOe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jOe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jOeはJoe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であるとすると、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"
```

関連参照情報

ネーム マッピングの管理用コマンド（100ページ）

デフォルト 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 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必要がある場合は、デフォルト ユーザを設定しないでください。

タスク概要

CIFS認証で、各Windowsユーザを個別のUNIXユーザにマッピングしないようにする場合は、代わりにデフォルトのUNIXユーザを指定できます。

NFS認証で、各UNIXユーザを個別のWindowsユーザにマッピングしないようにする場合は、代わりにデフォルトのWindowsユーザを指定できます。

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
デフォルトのUNIXユーザを設定する	**vserver cifs options modify -default-unix-user *user_name***
デフォルトのWindowsユーザを設定する	**vserver nfs modify -default-win-user *user_name***

関連コンセプト

ネーム マッピングの使用方法（80ページ）
ネーム マッピングの仕組み（81ページ）

関連タスク

不明なUNIXユーザによるNTFSボリュームまたはqtreeへのNFSアクセスの処理（92ページ）

IPv6経由のNFSのサポート

Data ONTAP 8.2以降では、NFSクライアントからIPv6ネットワーク経由で ストレージ システムの ファイルにアクセスできます。

NFSでのIPv6の有効化

NFSクライアントがIPv6ネットワーク経由でストレージ システム上のデータにアクセスできるようにする場合、Data ONTAPではいくつかの設定変更が必要になります。

手順

1. クラスタでIPv6を有効にします。

   この手順はクラスタ管理者が実行する必要があります。クラスタでのIPv6の有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。

2. IPv6のデータLIFを設定します。

   この手順はクラスタ管理者が実行する必要があります。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。

3. NFSクライアント アクセスに関するNFSエクスポート ポリシーおよびルールを設定します。

   クライアントをIPv6アドレスで照合する場合は、それに応じてエクスポート ルールを設定します。

Windows NFSクライアント向けのアクセスの有効化

Data ONTAPではWindows NFSv3クライアントからのファイル アクセスをサポートしています。NFSv3をサポートするWindowsオペレーティング システムを実行しているクライアントから、クラスタのNFSv3エクスポートのファイルにアクセスできるようになります。この機能を正しく使用するには、Storage Virtual Machine（SVM）を適切に設定し、一定の要件および制限事項に注意する必要があります。

開始する前に

SVMでNFSv3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、Windows NFSv3クライアントサポートが無効になっています。

Windows NFSv3クライアントは、Network Status Monitor（NSM;ネットワーク ステータス モニタ）プロトコルをサポートしていません。そのため、Windows NFSv3クライアント セッションでは、ストレージ フェイルオーバーやボリューム移動処理の途中で中断が生じる場合があります。

手順

1. SVMを変更して、NFSクライアントがエクスポートのリストを確認できるようにします。

   ```
   vserver nfs modify -vserver vserver_name -showmount enabled
   ```

2. Windows NFSv3クライアント サポートを有効にします。

   ```
   vserver nfs modify -vserver vserver_name -v3-ms-dos-client enabled
   ```

3. Windows NFSv3クライアントをサポートしているすべてのSVMで、`-enable-ejukebox`および`-v3-connection-drop`パラメータを無効にします。

   `vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled`

   これで、Windows NFSv3クライアントはストレージ システム上にエクスポートをマウントできるようになります。

4. `-o mtype=hard`オプションを使用して、各Windows NFSv3クライアントでハード マウントが使用されるようにします。

   これは、マウントの信頼性を確保するために必要です。

   例

   `mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\`

関連タスク

NFSクライアントによるSVMのエクスポート表示の有効化（89ページ）

Infinite Volumeへのファイル アクセスの設定に関する情報の参照先

Infinite Volumeに対するNFSファイル アクセスのセットアップ方法の詳細については、『*Clustered Data ONTAP Infinite Volumes Management Guide*』を参照してください。

NFSを使用したファイル アクセスの管理

Storage Virtual Machine（SVM）でNFSを有効にして設定したら、NFSを使用したファイル アクセスを管理するためのタスクを実行できます。

NFSv3の有効化と無効化

NFSv3を有効または無効にするには、-v3オプションを変更します。これにより、NFSv3プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。デフォルトでは、NFSv3が有効です。

手順

1. 次のいずれかを実行します。

目的	入力するコマンド
NFSv3を有効にする	**vserver nfs modify -vserver *vserver_name* -v3 enabled**
NFSv3を無効にする	**vserver nfs modify -vserver *vserver_name* -v3 disabled**

NFSv4.0の有効化と無効化

NFSv4.0を有効または無効にするには、-v4.0オプションを変更します。これにより、NFSv4.0プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。デフォルトではNFSv4.0は無効になっています。

タスク概要

NFSv4.0は、Infinite Volumeを備えたStorage Virtual Machine（SVM）ではサポートされません。

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
NFSv4.0を有効にする	**vserver nfs modify -vserver *vserver_name* -v4.0 enabled**
NFSv4.0を無効にする	**vserver nfs modify -vserver *vserver_name* -v4.0 disabled**

NFSv4.1の有効化と無効化

NFSv4.1を有効または無効にするには、`-v4.1`オプションを変更します。これにより、NFSv4.1プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。デフォルトではNFSv4.1は無効になっています。

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
NFSv4.1を有効にする	**vserver nfs modify -vserver *vserver_name* -v4.1 enabled**
NFSv4.1を無効にする	**vserver nfs modify -vserver *vserver_name* -v4.1 disabled**

pNFSの有効化と無効化

pNFSは、ストレージ デバイスに対する読み取り / 書き込み処理を直接かつ並行して実行することをNFSクライアントに許可し、ボトルネックとなるNFSサーバをバイパスすることで、処理パフォーマンスを向上させます。Parallel NFS（pNFS）を有効または無効にするには、`-v4.1-pnfs`オプションを変更します。デフォルトではpNFSは有効になっています。

開始する前に

pNFSを使用するには、NFSv4.1のサポートが必要です。

pNFSを有効にする場合は、まずNFSリファーラルを無効にする必要があります。両方を同時に有効にすることはできません。

SVMでpNFSとKerberosを併用する場合は、SVM上のすべてのLIFでKerberosを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。

状況	入力するコマンド
pNFSを有効にする	**vserver nfs modify -vserver *vserver_name* -v4.1-pnfs enabled**
pNFSを無効にする	**vserver nfs modify -vserver *vserver_name* -v4.1-pnfs disabled**

関連タスク

NFSv4リファーラルの有効化と無効化（127ページ）
NFSv4.1の有効化と無効化（89ページ）

NFSクライアントによるSVMのエクスポート表示の有効化

NFSクライアントは、`showmount -e`コマンドを使用して、NFSサーバで使用可能なエクスポートのリストを確認できます。これは、ユーザがNFSサーバにマウントするファイル システムを特定するのに役立ちます。デフォルトでは、Data ONTAPは、NFSクライアントによるNFSサーバのエクスポ

ート リストの表示を許可していませんが、それぞれのStorage Virtual Machine（SVM）でこの機能を個別に有効にすることができます。

開始する前に

SVMでNFSv3が有効になっている必要があります。

クライアントは、ポート635経由でSVMにアクセスできる必要があります。

タスク概要

クライアントの出力には、SVMのボリュームおよびqtreeのエクスポートのリストが表示されます。ただし、クライアント アクセス リストは表示されず、すべてにアクセス権があるように表示されます。エクスポートへのクライアント アクセスをチェックするには、代わりに`vserver export-policy check-access`コマンドを使用する必要があります。

Data ONTAPは、エクスポートのリストをキャッシュしています。たとえば、クラスタでのボリュームのアンマウントなどによってエクスポート リストに変更が発生しても、キャッシュが期限切れになるか、管理者が`vserver export-policy cache flush`コマンドを使用してフラッシュするまで、エクスポート パスはキャッシュ内に残ります。

手順

1. SVMを変更して、NFSクライアントがエクスポートのリストを確認できるようにします。

   `vserver nfs modify -vserver` *`vserver_name`* `-showmount enabled`

例

次のコマンドは、vs1というSVMでshowmount機能を有効にします。

```
cluster1::> vserver nfs modify -vserver vs1 -showmount enabled
```

NFSクライアントで次のコマンドを入力すると、IPアドレスが10.63.21.9のNFSサーバ上のエクスポートのリストが表示されます。

```
# showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/ (everyone)
```

関連タスク

エクスポートへのクライアント アクセスのチェック（52ページ）
エクスポート ポリシー キャッシュのフラッシュ（111ページ）

TCPおよびUDP経由のNFSアクセスの制御

TCPおよびUDP経由でのStorage Virtual Machine（SVM）へのNFSアクセスを有効または無効にするには、それぞれ-tcpおよび-udpパラメータを使用します。これにより、環境内のNFSクライアントがTCPまたはUDP経由でデータにアクセスできるかどうかを制御できます。

タスク概要

これらのパラメータはNFSのみに適用されます。補助プロトコルには影響を与えません。たとえば、TCP経由のNFSが無効になっていても、TCP経由でのマウント処理は成功します。TCPまたはUDPトラフィックを完全にブロックするには、エクスポート ポリシー ルールを使用します。

手順

1. 次のいずれかを実行します。

設定するNFSアクセスの状態	入力するコマンド
TCP経由で有効化	**vserver nfs modify -vserver *vserver_name* -tcp enabled**
TCP経由で無効化	**vserver nfs modify -vserver *vserver_name* -tcp disabled**
UDP経由で有効化	**vserver nfs modify -vserver *vserver_name* -udp enabled**
UDP経由で無効化	**vserver nfs modify -vserver *vserver_name* -udp disabled**

関連コンセプト

TCP最大読み取りサイズおよび書き込みサイズの変更によるNFSv3のパフォーマンスの向上（130ページ）

非予約ポートからのNFS要求の制御

-mount-rootonlyオプションを有効にすると、非予約ポートからのNFSマウント要求を拒否することができます。非予約ポートからのすべてのNFS要求を拒否するには、-nfs-rootonlyオプションを有効にします。

タスク概要

デフォルトでは、オプション-mount-rootonlyは**enabled**になっています。

デフォルトでは、オプション-nfs-rootonlyは**disabled**になっています。

これらのオプションは、NULLプロシージャには適用されません。

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
非予約ポートからのNFSマウント要求を許可する	**vserver nfs modify -vserver *vserver_name* -mount-rootonly disabled**

状況	入力するコマンド
非予約ポートからのNFSマウント要求を拒否する	`vserver nfs modify -vserver vserver_name -mount-rootonly enabled`
非予約ポートからのすべてのNFS要求を許可する	`vserver nfs modify -vserver vserver_name -nfs-rootonly disabled`
非予約ポートからのすべてのNFS要求を拒否する	`vserver nfs modify -vserver vserver_name -nfs-rootonly enabled`

不明なUNIXユーザによるNTFSボリュームまたはqtreeへのNFSアクセスの処理

NTFSセキュリティ形式のボリュームまたはqtreeへの接続を試みるUNIXユーザを識別できない場合、Data ONTAPはそのユーザをWindowsユーザに明示的にマッピングできません。Data ONTAPでは、そのようなユーザのアクセスを拒否するように設定してセキュリティを厳しくするか、またはデフォルトのWindowsユーザにマッピングするように設定してすべてのユーザに最小限のアクセスを保証することができます。

開始する前に

このオプションを有効にする場合は、デフォルトのWindowsユーザを設定しておく必要があります。

タスク概要

UNIXユーザがNTFSセキュリティ形式のボリュームまたはqtreeへのアクセスを試みると、Data ONTAPがNTFS権限を正しく評価できるように、そのUNIXユーザはまずWindowsユーザにマッピングされます。設定されているユーザ情報ネーム サービス ソースでそのUNIXユーザの名前を検索できなかった場合、特定のWindowsユーザにそのUNIXユーザを明示的にマッピングすることができません。このような不明なUNIXユーザの処理方法には次の選択肢があります。

- 不明なUNIXユーザのアクセスを拒否する。
  NTFSボリュームまたはqtreeにアクセスしようとするすべてのUNIXユーザについて明示的なマッピングを要求することで、より厳しいセキュリティを適用します。
- 不明なUNIXユーザをデフォルトのWindowsユーザにマッピングする。
  すべてのユーザにデフォルトのWindowsユーザとしてNTFSボリュームまたはqtreeへの最小限のアクセスを許可することで、セキュリティは低下しますが利便性は向上します。

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。

不明なUNIXユーザへのデフォルトのWindowsユーザのマッピング	入力するコマンド
有効にする	`vserver nfs modify -vserver vserver_name -map-unknown-uid-to-default-windows-user enabled`
無効にする	`vserver nfs modify -vserver vserver_name -map-unknown-uid-to-default-windows-user disabled`

3. admin権限レベルに戻ります。

```
set -privilege admin
```

関連コンセプト

ネーム マッピングの使用方法（80ページ）
ネーム マッピングの仕組み（81ページ）

関連タスク

デフォルト ユーザの設定（85ページ）

非予約ポートを使用してNFSエクスポートをマウントするクライアントに関する注意事項

非予約ポートを使用してNFSエクスポートをマウントするクライアントをサポートするストレージ システムでは、ユーザがrootでログインする場合でも、`-mount-rootonly`オプションを無効にする必要があります。HummingbirdクライアントやSolaris NFS / IPv6クライアントがこれに該当します。

`-mount-rootonly`オプションを有効にした場合、NFSクライアントで非予約ポート、つまり1,024以上のポートを使用してNFSエクスポートをマウントすることはできません。

ドメインの検証によるネットグループのより厳密なアクセス チェックの実行

Data ONTAPは、ネットグループに対するクライアント アクセスを評価する際に追加の検証をデフォルトで実行します。追加チェックでは、クライアントのドメインがStorage Virtual Machine（SVM）のドメイン設定に一致しているかどうかが確認されます。一致していない場合、Data ONTAPはクライアント アクセスを拒否します。

タスク概要

Data ONTAPがクライアント アクセス用のエクスポート ポリシー ルールを評価し、あるエクスポート ポリシー ルールにネットグループが含まれていた場合、Data ONTAPはクライアントのIPアドレスがそのネットグループに属しているかどうかを確認する必要があります。そのために、Data ONTAPは、DNSを使用してクライアントのIPアドレスをホスト名に変換し、完全修飾ドメイン名（FQDN）を取得します。

ネットグループ ファイルにホストの短縮名のみが記載されていて、そのホストの短縮名が複数のドメインに存在している場合、このチェックがないと、別のドメインのクライアントがアクセス権を取得することが可能になります。

この問題を回避するために、Data ONTAPは、ホストに対してDNSから返されたドメインをSVMに対して設定されているDNSドメイン名のリストと比較し、一致した場合はアクセスが許可されます。一致しなかった場合、アクセスは拒否されます。

この検証はデフォルトで有効になっています。この検証機能は、advanced権限レベルで使用可能な`-netgroup-dns-domain-search`パラメータを変更することで管理できます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

ネットグループのドメイン検証の設定	コマンド
有効にする	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search enabled`
無効にする	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search disabled`

3. 権限レベルをadminに設定します。

   ```
   set -privilege admin
   ```

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。

NFSv3サービスで使用するポートの変更

ストレージ システムのNFSサーバは、マウント デーモンやNetwork Lock Managerのようなサービスを使用して、特定のデフォルト ネットワーク ポートを介してNFSクライアントと通信します。デフォルト ポートは、ほとんどのNFS環境で正しく機能するので変更する必要はありませんが、別のネットワーク ポートをNFSv3環境で使用したい場合は変更できます。

開始する前に

ストレージ システムでNFSポートを変更すると、すべてのNFSクライアントがシステムに再接続する必要があるため、変更に先立ってこの情報をユーザに伝えておく必要があります。

タスク概要

NFSマウント デーモン、Network Lock Manager、Network Status Monitor、およびNFSクォータ デーモンの各サービスで使用されるポートをStorage Virtual Machine（SVM）ごとに設定できます。ポー

ト番号の変更は、データへのアクセスにTCPとUDPのどちらを使用するNFSクライアントにも影響を与えます。

NFSv4およびNFSv4.1のポートは変更できません。

手順

1. 権限レベルをadvancedに設定します。

   set -privilege advanced

2. NFSへのアクセスを無効にします。

   vserver nfs modify -vserver *vserver_name* -access false

3. 特定のNFSサービスのNFSポートを設定します。

   vserver nfs modify -vserver *vserver_name nfs_port_parameter port_number*

NFSポート パラメータ	説明	デフォルト ポート
-mountd-port	NFSマウント デーモン	635
-nlm-port	Network Lock Manager	4045
-nsm-port	Network Status Monitor	4046
-rquotad-port	NFSクォータ デーモン	4049

   デフォルト ポート以外で使用可能なポート番号の範囲は、1,024～65,535です。各NFSサービスで固有のポートを使用する必要があります。

4. NFSへのアクセスを有効にします。

   vserver nfs modify -vserver *vserver_name* -access true

5. network connections listening showコマンドを使用して、ポート番号の変更を確認します。

6. admin権限レベルに戻ります。

   set -privilege admin

例

次のコマンドは、vs1という SVMでNFSマウント デーモンのポートを1113に設定します。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- ------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700         TCP/ctlopcp
vs1              data1:4046                      TCP/sm
vs1              data1:4046                      UDP/sm
vs1              data1:4045                      TCP/nlm-v4
vs1              data1:4045                      UDP/nlm-v4
vs1              data1:1113                      TCP/mount
```

```
vs1              data1:1113                          UDP/mount
....

vs1::*> set -privilege admin
```

NFSサーバの管理用コマンド

Data ONTAPには、NFSサーバ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
NFSサーバを作成する	`vserver nfs create`
NFSサーバを表示する	`vserver nfs show`
NFSサーバを変更する	`vserver nfs modify`
NFSサーバを削除する	`vserver nfs 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。

関連タスク

NFSサーバの作成(33ページ)

ネーム サービスに関する問題のトラブルシューティング

ネーム サービスの問題でクライアントでアクセス エラーが発生した場合は、`vserver services name-service getxxbyyy`コマンド ファミリーを使用して、さまざまなネーム サービス検索を手動で実行したり、検索の詳細や結果を調べたりして、トラブルシューティングに役立てることができます。

タスク概要

- 各コマンドでは、次の情報を指定できます。
  - 検索を実行するノードまたはStorage Virtual Machine(SVM)の名前。
    特定のノードまたはSVMでネーム サービス検索を実行して、想定されるネーム サービス設定問題の検索範囲を絞り込むことができます。
  - 検索に使用されたソースを表示するかどうか。
    正しいソースが使用されたかどうかをチェックできます。
- Data ONTAPは、設定されているネーム サービス スイッチの順序に基づいて検索を実行するためのサービスを選択します。
- これらのコマンドはadvanced権限レベルで使用できます。

手順

1. 次のいずれかを実行します。

取得する情報	使用するコマンド
ホスト名のIPアドレス	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname`（IPv4アドレス専用）
グループのメンバー（グループIDを指定）	`vserver services name-service getxxbyyy getgrbygid`
グループのメンバー（グループ名を指定）	`vserver services name-service getxxbyyy getgrbyname`
ユーザが属しているグループのリスト	`vserver services name-service getxxbyyy getgrlist`
IPアドレスのホスト名	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr`（IPv4アドレス専用）
ユーザ情報（ユーザ名を指定）	`vserver services name-service getxxbyyy getpwbyname` `-use-rbac`パラメータを**true**に設定すると、RBACユーザの名前解決をテストできます。
ユーザ情報（ユーザIDを指定）	`vserver services name-service getxxbyyy getpwbyuid` `-use-rbac`パラメータを**true**に設定すると、RBACユーザの名前解決をテストできます。
クライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrp`
クライアントのネットグループメンバーシップ（ホスト単位のネットグループ検索を使用）	`vserver services name-service getxxbyyy netgrpbyhost`

例

次の例は、ホストacast1.eng.example.comのIPアドレスの取得を試みることでSVM vs1のDNSルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -
vserver vs1 -hostname acast1.eng.example.com -address-family all -
show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

次の例は、UIDが501768のユーザのユーザ情報の取得を試みることでSVM vs1のNIS検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -
vserver vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
```

```
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

次の例は、ldap1というユーザのユーザ情報の取得を試みることでSVM vs1のLDAP検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -
vserver vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

次の例は、クライアントdnshost0がネットグループlnetgroup136のメンバーであるかどうかを調べることでSVM vs1のネットグループ検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver
vs1 -netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

2. 実行したテストの結果を分析し、必要な措置を実施します。

例

状況	チェック対象
ホスト名またはIPアドレスの検索に失敗したか、間違った結果が得られた	DNS設定
検索を実施したソースが正しくない	ネーム サービス スイッチの設定
ユーザまたはグループの検索に失敗したか、間違った結果が得られた	ネーム サービス スイッチの設定 ソース設定（ローカル ファイル、NISドメイン、LDAPクライアント） ネットワーク設定（LIF、ルートなど）

関連タスク

ネーム サービス スイッチ テーブルの設定（62ページ）

関連情報

ネットアップ テクニカル レポート4379:『Name Services Best Practice Guide Clustered Data ONTAP』

ネーム サービス スイッチ エントリの管理用コマンド

ネーム サービス スイッチ エントリは、作成、表示、変更、および削除することができます。

状況	使用するコマンド
ネーム サービス スイッチ エントリを作成する	`vserver services name-service ns-switch create`
ネーム サービス スイッチ エントリを表示する	`vserver services name-service ns-switch show`
ネーム サービス スイッチ エントリを変更する	`vserver services name-service ns-switch modify`
ネーム サービス スイッチ エントリを削除する	`vserver services name-service ns-switch 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。

関連タスク

ネーム サービス スイッチ テーブルの設定（62ページ）

関連情報

ネットアップ テクニカル レポート4379:『Name Services Best Practice Guide Clustered Data ONTAP』

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。

関連タスク

ネーム マッピングの作成（84ページ）

ローカルUNIXユーザの管理用コマンド

Data ONTAPには、ローカルUNIXユーザ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
ローカルUNIXユーザを作成する	`vserver services name-service unix-user create`
URIからローカルUNIXユーザをロードする	`vserver services name-service unix-user load-from-uri`
ローカルUNIXユーザを表示する	`vserver services name-service unix-user show`
ローカルUNIXユーザを変更する	`vserver services name-service unix-user modify`
ローカルUNIXユーザを削除する	`vserver services name-service unix-user 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。

関連タスク

ローカルUNIXユーザの作成(75ページ)

ローカルUNIXグループの管理用コマンド

Data ONTAPには、ローカルUNIXグループ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
ローカルUNIXグループを作成する	`vserver services name-service unix-group create`
ローカルUNIXグループにユーザを追加する	`vserver services name-service unix-group adduser`
URIからローカルUNIXグループをロードする	`vserver services name-service unix-group load-from-uri`
ローカルUNIXグループを表示する	`vserver services name-service unix-group show`
ローカルUNIXグループを変更する	`vserver services name-service unix-group modify`
ローカルUNIXグループからユーザを削除する	`vserver services name-service unix-group deluser`
ローカルUNIXグループを削除する	`vserver services name-service unix-group 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。

関連タスク

ローカルUNIXグループの作成（78ページ）

ローカルUNIXユーザ、グループ、およびグループ メンバーに対する制限

Data ONTAP 8.3以降では、クラスタ内のUNIXユーザおよびグループの最大数に対する制限とそれらの制限を管理するためのコマンドが導入されています。これらの制限は、管理者がクラスタ内にローカルUNIXユーザおよびグループを作りすぎないようにすることでパフォーマンスの問題を回避するのに役立ちます。

ローカルのUNIXユーザ グループとグループ メンバーの合計数には制限があります。さらに、ローカルUNIXユーザ数にも制限があります。これらの制限はクラスタ全体に適用されます。これらの制限はデフォルト値に設定されており、変更可能ですが、あらかじめ割り当てられたハード リミットよりも高い値に設定することはできません。

データベース	デフォルトの制限	ハード リミット
ローカルUNIXユーザ	32,768	65,536
ローカルUNIXグループとグループ メンバー	32,768	65,536

ローカルUNIXユーザおよびグループに対する制限の管理

Data ONTAPには、ローカルUNIXユーザおよびグループに対する制限を管理するための固有のコマンドが用意されています。クラスタ管理者は、これらのコマンドを使用して、ローカルUNIXユーザおよびグループの数が多すぎることに関連すると考えられる、クラスタでのパフォーマンス問題に対応することができます。

タスク概要

これらのコマンドはadvanced権限レベルのクラスタ管理者が使用できます。

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
ローカルUNIXユーザの制限に関する情報を表示する	`vserver services unix-user max-limit show`
ローカルUNIXグループの制限に関する情報を表示する	`vserver services unix-group max-limit show`
ローカルUNIXユーザの制限を変更する	`vserver services unix-user max-limit modify`
ローカルUNIXグループの制限を変更する	`vserver services unix-group max-limit modify`

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。

ローカル ネットグループの管理用コマンド

ローカル ネットグループは、URIからロードしたり、ノード間でのステータスを確認したり、表示または削除したりすることができます。

状況	使用するコマンド
URIからネットグループをロードする	`vserver services name-service netgroup load`
ノード間でのネットグループのステータスを確認する	`vserver services name-service netgroup status` advanced権限レベル以上で使用できます。
ローカル ネットグループを表示する	`vserver services name-service netgroup file show`
ローカル ネットグループを削除する	`vserver services name-service netgroup file 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。

関連タスク

SVMへのネットグループのロード(46ページ)
クライアントIPアドレスがネットグループのメンバーかどうかのチェック(112ページ)
ドメインの検証によるネットグループのより厳密なアクセス チェックの実行(93ページ)

NISドメイン設定の管理用コマンド

Data ONTAPには、NISドメインの設定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
NISドメインの設定を作成する	`vserver services name-service nis-domain create`
NISドメインの設定を表示する	`vserver services name-service nis-domain show`
NISドメインの設定のバインド ステータスを表示する	`vserver services name-service nis-domain show-bound`
NISの統計を表示する	`vserver services name-service nis-domain show-statistics` advanced権限レベル以上で使用できます。
NISの統計をクリアする	`vserver services name-service nis-domain clear-statistics` advanced権限レベル以上で使用できます。
NISドメインの設定を変更する	`vserver services name-service nis-domain modify`
NISドメインの設定を削除する	`vserver services name-service nis-domain 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。

関連タスク

NISドメイン設定の作成（74ページ）

LDAPクライアント設定の管理用コマンド

Data ONTAPには、LDAPクライアント設定を管理するための固有のコマンドが用意されています。

注: SVM管理者は、クラスタ管理者が作成したLDAPクライアント設定を変更したり削除したりできません。

状況	使用するコマンド
LDAPクライアント設定を作成する	`vserver services name-service ldap client create`
LDAPクライアント設定を表示する	`vserver services name-service ldap client show`
LDAPクライアント設定を変更する	`vserver services name-service ldap client modify`
LDAPクライアントのバインド パスワードを変更する	`vserver services name-service ldap client modify-bind-password`
LDAPクライアント設定を削除する	`vserver services name-service ldap client 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。

関連コンセプト

LDAPディレクトリ検索の設定オプション（67ページ）

関連タスク

LDAPクライアント設定の作成（69ページ）

LDAP設定の管理用コマンド

Data ONTAPには、LDAP設定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
LDAP設定を作成する	`vserver services name-service ldap create`
LDAP設定を表示する	`vserver services name-service ldap show`
LDAP設定を変更する	`vserver services name-service ldap modify`
LDAP設定を削除する	`vserver services name-service ldap 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。

関連タスク

SVMでのLDAPの有効化（72ページ）

LDAPクライアント スキーマ テンプレートの管理用コマンド

Data ONTAPには、LDAPクライアント スキーマ テンプレートを管理するための固有のコマンドが用意されています。

注: SVM管理者は、クラスタ管理者が作成したLDAPクライアント スキーマを変更したり削除したりできません。

状況	使用するコマンド
既存のLDAPスキーマ テンプレートをコピーする	`vserver services name-service ldap client schema copy` advanced権限レベル以上で使用できます。
LDAPスキーマ テンプレートを表示する	`vserver services name-service ldap client schema show`
LDAPスキーマ テンプレートを変更する	`vserver services name-service ldap client schema modify` advanced権限レベル以上で使用できます。
LDAPスキーマ テンプレートを削除する	`vserver services name-service ldap client schema delete` advanced権限レベル以上で使用できます。

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

新しいLDAPクライアント スキーマの作成（65ページ）

NFS Kerberosインターフェイス設定の管理用コマンド

Data ONTAPには、NFS Kerberosインターフェイスの設定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
NFS KerberosをLIFで有効にする	`vserver nfs kerberos interface enable`
NFS Kerberosインターフェイスの設定を表示する	`vserver nfs kerberos interface show`
NFS Kerberosインターフェイスの設定を変更する	`vserver nfs kerberos interface modify`
NFS KerberosをLIFで無効にする	`vserver nfs kerberos interface disable`

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

NFS Kerberos設定の作成（59ページ）

NFS Kerberos Realm設定の管理用コマンド

Data ONTAPには、NFS Kerberos Realmの設定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
NFS Kerberos Realmの設定を作成する	`vserver nfs kerberos realm create`
NFS Kerberos Realmの設定を表示する	`vserver nfs kerberos realm show`
NFS Kerberos Realmの設定を変更する	`vserver nfs kerberos realm modify`
NFS Kerberos Realmの設定を削除する	`vserver nfs kerberos realm 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。

関連タスク

NFS Kerberos realm設定の作成（58ページ）

エクスポート ポリシーの管理用コマンド

Data ONTAPには、エクスポート ポリシー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
エクスポート ポリシーに関する情報を表示する	`vserver export-policy show`
エクスポート ポリシーの名前を変更する	`vserver export-policy rename`
エクスポート ポリシーをコピーする	`vserver export-policy copy`
エクスポート ポリシーを削除する	`vserver export-policy 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。

関連タスク

エクスポート ポリシーの作成（42ページ）
エクスポートへのクライアント アクセスのチェック（52ページ）

エクスポート ルールの管理用コマンド

Data ONTAPには、エクスポート ルール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
エクスポート ルールを作成する	`vserver export-policy rule create`
エクスポート ルールに関する情報を表示する	`vserver export-policy rule show`
エクスポート ルールを変更する	`vserver export-policy rule modify`
エクスポート ルールを削除する	`vserver export-policy rule delete`

注: 複数の異なるクライアントに一致する同一のエクスポート ルールを複数設定している場合は、エクスポート ルールの処理時にそれらのルールの内容が同じままになるようにします。

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

エクスポート ポリシーへのルールの追加(43ページ)
エクスポートへのクライアント アクセスのチェック(52ページ)

clustered Data ONTAPでのエクスポートのフェンシングまたはフェンシング解除

Data ONTAP 7-Modeでは、`exportfs -b`コマンドを使用してクライアントをフェンシングまたはフェンシング解除できます。clustered Data ONTAPにはこれに相当するコマンドはありませんが、エクスポート ポリシー ルールを作成することで同じタスクを実行できます。

タスク概要

フェンシングとは、1つ以上のクライアントからあるエクスポートへのアクセス権を読み取り専用に制限することで、読み取り / 書き込みアクセス権があれば削除して、該当クライアントを読み取り専用アクセス リストの最上部に配置します。

フェンシング解除とは、1つ以上のクライアントにあるエクスポートへの保証された読み取り / 書き込みアクセスを許可することで、該当するクライアントを読み取り / 書き込みアクセス リストの最上部に配置します。

手順

1. クライアントのフェンシングまたはフェンシング解除を行うボリュームのエクスポート ポリシーを特定します。

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`*

2. `vserver export-policy rule create` コマンドを使用して、新しいエクスポート ポリシー ルールを作成します。

   クライアントのフェンシングまたはフェンシング解除のどちらを行うかに応じて、適切なパラメータを指定します。

目的	エクスポート ルールで使用するパラメータ
クライアントをフェンシングする	`-rwrule none -rorule any -ruleindex 1`
クライアントのフェンシングを解除する	`-rwrule any -rorule any -ruleindex 1`

   エクスポートのエクスポート ポリシーに新しいルールを追加後、7-Modeの機能と同様にクライアントがフェンシングまたはフェンシング解除されます。

NFSクレデンシャル キャッシュの設定

Data ONTAPは、クレデンシャル キャッシュを使用してNFSエクスポート アクセスのユーザ認証に必要な情報を格納し、アクセスの高速化とパフォーマンスの向上を実現します。情報がクレデンシ

ャル キャッシュに格納される期間を設定して、環境に合わせてクレデンシャル キャッシュをカスタマイズできます。

NFSクレデンシャル キャッシュの仕組み

NFSユーザがストレージ システム上のNFSエクスポートへのアクセスを要求すると、Data ONTAPは、ユーザの認証を行うために外部ネーム サーバまたはローカル ファイルからユーザ クレデンシャルを取得する必要があります。その後、Data ONTAPは、以降の参照用にこれらのクレデンシャルを内部のクレデンシャル キャッシュに格納します。NFSクレデンシャル キャッシュの仕組みを理解しておくと、パフォーマンスおよびアクセスに関する潜在的な問題に対処できます。

クレデンシャル キャッシュがなければ、Data ONTAPはNFSユーザからアクセスが要求されるたびにネーム サービスに問い合わせなければなりません。多数のユーザがアクセスする、負荷の高いストレージ システムでは、これはすぐに深刻なパフォーマンス上の問題につながり、不要な遅延や、場合によってはNFSクライアント アクセスの拒否さえ引き起こす可能性があります。

クレデンシャル キャッシュがあれば、Data ONTAPは取得したユーザ クレデンシャルをあらかじめ決められた期間だけ格納しておき、同じNFSクライアントから再び要求があっても迅速かつ容易にアクセスを提供できます。この方法には次の利点があります。

- 外部ネーム サーバ（NISやLDAPなど）に対する要求の処理を減らすことで、ストレージ システムの負荷が軽減されます。
- 外部ネーム サーバに送信する要求を減らすことで、外部ネーム サーバの負荷が軽減されます。
- ユーザの認証を行う際に外部ソースからクレデンシャルを取得する待ち時間をなくすことで、ユーザ アクセスがスピード アップします。

Data ONTAPは、ポジティブ クレデンシャルとネガティブ クレデンシャルの両方をクレデンシャル キャッシュに格納します。ポジティブ クレデンシャルは、ユーザが認証されてアクセス権を付与されたことを意味します。ネガティブ クレデンシャルは、ユーザが認証されずにアクセスが拒否されたことを意味します。

デフォルトでは、ポジティブ クレデンシャルは24時間保存されます。つまり、ユーザの最初の認証から24時間は、そのユーザからのすべてのアクセス要求でキャッシュされたクレデンシャルが使用されます。24時間が経過したあとに同じユーザからアクセスが要求されると、処理が最初から繰り返されます。Data ONTAPはキャッシュされたクレデンシャルを破棄し、適切なネーム サービス ソースから再びクレデンシャルを取得します。最初の24時間にネーム サーバ上でクレデンシャルが変更された場合、次の24時間で使用できるよう、更新されたクレデンシャルがキャッシュされます。

デフォルトでは、ネガティブ クレデンシャルは2時間保存されます。つまり、ユーザに対する最初のアクセス拒否から2時間は、そのユーザからのすべてのアクセス要求は拒否されます。2時間が経過したあとに同じユーザからアクセスが要求されると、処理が最初から繰り返されます。Data ONTAPは適切なネーム サービス ソースから再びクレデンシャルを取得します。最初の2時間にネーム サーバ上でクレデンシャルが変更された場合、次の2時間で使用できるよう、更新されたクレデンシャルがキャッシュされます。

NFSクレデンシャル キャッシュのTime-To-Liveを変更する理由

NFSクレデンシャル キャッシュのTime-To-Live（TTL）の変更が問題の解決に役立つ場合があります。どのような状況がこれに該当するのか、またそうした変更がどのような影響を及ぼすのかを理解しておく必要があります。

理由

次の状況では、デフォルトTTLの変更を検討します。

問題	修正アクション
Data ONTAPからの要求の負荷が高いため、環境内のネーム サーバのパフォーマンスが低下している。	キャッシュされているポジティブおよびネガティブ クレデンシャルのTTLを長くして、Data ONTAPからネーム サーバへの要求数を減らします。
ネーム サーバ管理者がこれまで拒否されていたNFSユーザに対してアクセスを許可する変更を行った。	キャッシュされているネガティブ クレデンシャルのTTLを短くして、Data ONTAPが外部ネーム サーバに更新されたクレデンシャルを要求し、NFSユーザがアクセスを取得できるようになるまでの時間を短縮します。
ネーム サーバ管理者がこれまで許可されていたNFSユーザに対してアクセスを拒否する変更を行った。	キャッシュされているポジティブ クレデンシャルのTTLを短くして、Data ONTAPが外部ネーム サーバに更新されたクレデンシャルを要求し、NFSユーザのアクセスが拒否されるようになるまでの時間を短縮します。

影響

ポジティブおよびネガティブ クレデンシャルをキャッシュしておく期間は個別に変更することができます。ただし、変更によるメリットとデメリットの両方を理解する必要があります。

状況または条件	メリット	デメリット
ポジティブ クレデンシャルのキャッシュ時間を長くする	Data ONTAPがクレデンシャルの要求をネーム サーバに送信する頻度が低くなり、ネーム サーバの負荷が軽減されます。	以前はアクセスを許可されていたが許可されなくなったNFSユーザに対し、アクセスを拒否するのにかかる時間が長くなります。
ポジティブ クレデンシャルのキャッシュ時間を短くする	以前はアクセスを許可されていたが許可されなくなったNFSユーザに対し、アクセスを拒否するのにかかる時間が短くなります。	Data ONTAPがクレデンシャルの要求をネーム サーバに送信する頻度が高くなり、ネーム サーバの負荷が増大します。
ネガティブ クレデンシャルのキャッシュ時間を長くする	Data ONTAPがクレデンシャルの要求をネーム サーバに送信する頻度が低くなり、ネーム サーバの負荷が軽減されます。	以前はアクセスを許可されていなかったが許可されるようになったNFSユーザに対し、アクセスを許可するのにかかる時間が長くなります。
ネガティブ クレデンシャルのキャッシュ時間を短くする	以前はアクセスを許可されていなかったが許可されるようになったNFSユーザに対し、アクセスを許可するのにかかる時間が短くなります。	Data ONTAPがクレデンシャルの要求をネーム サーバに送信する頻度が高くなり、ネーム サーバの負荷が増大します。

キャッシュされたNFSユーザ クレデンシャルのTTLの設定

Storage Virtual Machine（SVM）のNFSサーバを変更することで、Data ONTAPがNFSユーザのクレデンシャルを内部キャッシュに格納する期間であるTime-To-Live（TTL）を設定できます。これにより、ネーム サーバの高負荷に関する問題や、NFSユーザ アクセスに影響を及ぼすクレデンシャルの変更に関する問題を軽減できます。

タスク概要

これらのパラメータは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. 次のうち必要な操作を実行します。

TTLを変更するキャッシュ対象	使用するコマンド
ポジティブ クレデンシャル	**vserver nfs modify -vserver *vserver_name* -cached-cred-positive-ttl *time_to_live*** TTLの単位はミリ秒です。デフォルト値は24時間（86,400,000ミリ秒）です。この値の許容範囲は1分（60,000ミリ秒）～7日間（604,800,000ミリ秒）です。
ネガティブ クレデンシャル	**vserver nfs modify -vserver *vserver_name* -cached-cred-negative-ttl *time_to_live*** TTLの単位はミリ秒です。デフォルト値は2時間（7,200,000ミリ秒）です。この値の許容範囲は1分（60,000ミリ秒）～7日間（604,800,000ミリ秒）です。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

エクスポート ポリシー キャッシュの管理

Data ONTAPは、複数のエクスポート ポリシー キャッシュを使用してエクスポート ポリシーに関連する情報を格納し、アクセスを高速化します。問題が発生した場合には、エクスポート ポリシー キャッシュを管理するためのいくつかのタスクを実行することができます。

Data ONTAPでのエクスポート ポリシー キャッシュの使用方法

システム パフォーマンスを向上するために、Data ONTAPはローカル キャッシュを使用してホスト名やネットグループなどの情報を格納します。これにより、外部ソースから情報を取得する場合よりも迅速にエクスポート ポリシー ルールを処理できます。キャッシュとは何か、またキャッシュによって何が行われるのかを理解すると、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に役立ちます。

エクスポート ポリシーを設定し、NFSエクスポートへのクライアント アクセスを制御します。それぞれのエクスポート ポリシーにはルールが含まれ、各ルールにはアクセスを要求しているクライアントを一致させるためのパラメータが含まれています。一部のパラメータは、ドメイン名、ホスト名、ネットグループなどのオブジェクトを解決するためにData ONTAPとDNSサーバやNISサーバのような外部ソースとの通信を必要とします。

外部ソースとのこうした通信には少し時間がかかります。パフォーマンスを向上するために、Data ONTAPは、各ノードで複数のキャッシュに情報をローカルに格納することで、エクスポート ポリシー ルールのオブジェクトの解決にかかる時間を短縮します。

キャッシュ名	格納される情報の種類
Access	対応するエクスポート ポリシーへのクライアントのマッピング
Name	対応するUNIXユーザIDへのUNIXユーザ名のマッピング
ID	対応するUNIXユーザIDおよび拡張されたUNIXグループIDへのUNIXユーザIDのマッピング
Host	対応するIPアドレスへのホスト名のマッピング

キャッシュ名	格納される情報の種類
Netgroup	メンバーの対応するIPアドレスへのネットグループのマッピング
Showmount	SVMネームスペースからエクスポートされたディレクトリのリスト

Data ONTAPによって外部ネーム サーバ上の情報が取得されてローカルに格納されたあとに、外部ネーム サーバ上の情報を変更した場合、キャッシュの情報が古くなる可能性があります。Data ONTAPは一定の間隔でキャッシュを自動的に更新しますが、有効期限や更新間隔、アルゴリズムはキャッシュごとに異なります。

キャッシュの情報が古くなる理由としてもう1つ考えられるのは、Data ONTAPがキャッシュされた情報の更新を試みた際にネーム サーバとの通信でエラーが発生した場合です。この場合、Data ONTAPは、クライアントの中断を避けるために現在ローカル キャッシュに格納されている情報を引き続き使用します。

その結果、成功するはずのクライアント アクセス要求がエラーとなったり、エラーとなるはずのクライアント アクセス要求が成功したりする可能性があります。クライアント アクセスのこのような問題をトラブルシューティングする際には、一部のエクスポート ポリシー キャッシュを表示して手動でフラッシュできます。

エクスポート ポリシー キャッシュのフラッシュ

エクスポート ポリシー キャッシュを手動でフラッシュすると(`vserver export-policy cache flush`)、古くなった可能性のある情報が削除され、Data ONTAPが適切な外部リソースから最新情報を取得します。これは、NFSエクスポートへのクライアント アクセスに関するさまざまな問題の解決に役立ちます。

タスク概要

エクスポート ポリシー キャッシュの情報は、次の理由によって古くなる可能性があります。

- エクスポート ポリシー ルールの変更
- ネーム サーバ内のホスト名レコードの変更
- ネーム サーバ内のネットグループ エントリの変更
- ネットグループの完全なロードを妨げていたネットワーク停止からのリカバリ

手順

1. 次のいずれかを実行します。

フラッシュ対象	入力するコマンド
すべてのエクスポート ポリシー キャッシュ(showmountを除く)	**vserver export-policy cache flush -vserver *vserver_name***
エクスポート ポリシー ルールのアクセス キャッシュ	**vserver export-policy cache flush -vserver *vserver_name* -cache access** オプションの-nodeパラメータを使用すると、アクセス キャッシュをフラッシュするノードを指定できます。
ホスト名キャッシュ	**vserver export-policy cache flush -vserver *vserver_name* -cache host**

フラッシュ対象	入力するコマンド
netgroupキャッシュ	**vserver export-policy cache flush -vserver *vserver_name* -cache netgroup** ネットグループの処理は大量のリソースを消費します。ネットグループ キャッシュのフラッシュは、古いネットグループが原因で発生したクライアント アクセスに関する問題の解決を試みる場合にのみ行ってください。
showmountキャッシュ	**vserver export-policy cache flush -vserver *vserver_name* -cache showmount**

エクスポート ポリシー ネットグループ キューおよびキャッシュの表示

Data ONTAPでは、ネットグループのインポート時および解決時にネットグループ キューを使用し、結果として得られる情報を格納するためにネットグループ キャッシュを使用します。エクスポート ポリシーのネットグループに関する問題のトラブルシューティング時には、`vserver export-policy netgroup queue show`および`vserver export-policy netgroup cache show`コマンドを使用して、ネットグループ キューのステータスやネットグループ キャッシュの内容を表示できます。

手順

1. 次のいずれかを実行します。

エクスポート ポリシー ネットグループに関する表示対象	入力するコマンド
キュー	**vserver export-policy netgroup queue show**
キャッシュ	**vserver export-policy netgroup cache show -vserver *vserver_name***

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。

クライアントIPアドレスがネットグループのメンバーかどうかのチェック

ネットグループに関するNFSクライアント アクセスの問題のトラブルシューティング時には、`vserver export-policy netgroup check-membership`コマンドを使用すると、クライアントIPが特定のネットグループのメンバーであるかどうかを確認できます。

タスク概要

ネットグループ メンバーシップのチェックにより、クライアントがネットグループのメンバーであるかどうかをData ONTAPが認識しているかどうかを確認できます。また、ネットグループ情報の更新中にData ONTAPのネットグループ キャッシュが一時的な状態にあるかどうかもわかります。この情報は、クライアントが予期せずアクセスを許可または拒否された理由を把握するのに役立ちます。

手順

1. クライアントIPアドレスのネットグループ メンバーシップをチェックします。

   vserver export-policy netgroup check-membership -vserver *vserver_name* -netgroup *netgroup_name* -client-ip *client_ip*

   このコマンドは次のいずれかの結果を返します。

   - クライアントはネットグループのメンバーです。
     リバース ルックアップ スキャンまたはホスト単位のネットグループ検索によって確認されました。

- クライアントはネットグループのメンバーです。
  クライアントはData ONTAPのネットグループ キャッシュに見つかりました。
- クライアントはネットグループのメンバーではありません。
- Data ONTAPが現在ネットグループ キャッシュを更新中のため、クライアントのメンバーシップを判断できません。
  更新が完了するまで、メンバーシップを明示的に判断することはできません。`vserver export-policy netgroup queue show`コマンドを使用してネットグループのロードを監視し、ロード完了後に再びチェックを試みてください。

例

次の例は、IPアドレスが172.17.16.72のクライアントがSVM vs1上のネットグループmercuryのメンバーであるかどうかをチェックします。

```
 cluster1::> vserver export-policy netgroup check-membership -
vserver vs1 -netgroup  mercury -client-ip 172.17.16.72
```

関連タスク

ドメインの検証によるネットグループのより厳密なアクセス チェックの実行（93ページ）

関連参照情報

ローカル ネットグループの管理用コマンド（103ページ）

アクセス キャッシュの仕組み

Data ONTAPは、アクセス キャッシュを使用して、ボリュームまたはqtreeへのクライアント アクセス処理に対するエクスポート ポリシー ルールの評価結果を格納します。クライアントからI/O要求が送信されるたびにエクスポート ルールを評価する場合にくらべ、かなり迅速にアクセス キャッシュから情報を取得でき、パフォーマンスが向上します。

NFSクライアントがボリュームまたはqtree上のデータにアクセスするためのI/O要求を送信するたびに、Data ONTAPはそれぞれのI/O要求を評価して、そのI/O要求を許可するか拒否するかを決定する必要があります。この評価には、そのボリュームまたはqtreeに関連付けられているすべてのエクスポート ポリシー ルールのチェックが伴います。ボリュームまたはqtreeへのパスがいくつかのジャンクション ポイントを経由している場合は、パスに沿って複数のエクスポート ポリシーに対してこのチェックを実行しなければならない可能性があります。

この評価は、最初のマウント要求だけでなく、読み取り、書き込み、リスト、コピーなど、NFSクライアントから送信されたすべてのI/O要求について行われます。

Data ONTAPは、該当するエクスポート ポリシー ルールを特定して要求を許可するか拒否するかを決定したあと、その情報を格納するエントリをアクセス キャッシュに作成します。

NFSクライアントがI/O要求を送信すると、Data ONTAPは、そのクライアントのIPアドレス、SVMのID、およびターゲット ボリュームまたはqtreeに関連付けられているエクスポート ポリシーを記録したうえで、まずアクセス キャッシュをチェックして一致するエントリがないか確認します。一致するエントリがアクセス キャッシュ内に存在する場合、格納されている情報を使用してI/O要求を許可または拒否します。一致するエントリが存在しない場合、Data ONTAPは、前述したように、すべての該当するポリシー ルールを評価する通常の処理を実行します。

アクセス キャッシュからの情報の取得は、I/O要求のたびにエクスポート ポリシー ルールの評価を最初から実行する場合よりもずっと高速です。そのため、アクセス キャッシュを使用すると、クライアント アクセス チェックのオーバーヘッドが軽減され、パフォーマンスが大幅に向上します。

アクセス キャッシュ パラメータの仕組み

アクセス キャッシュ内にあるエントリの更新期間を制御するパラメータがいくつかあります。これらのパラメータの仕組みを理解すると、各パラメータを変更して、アクセス キャッシュを調整したり、パフォーマンスと格納情報の最新度のバランスをとることができます。

アクセス キャッシュに格納されるエントリは、ボリュームまたはqtreeへのアクセスを試みるクライアントに適用される1つ以上のエクスポート ルールで構成されます。これらのエントリは、一定期間格納されたあと、更新されます。更新間隔はアクセス キャッシュ パラメータによって決定し、アクセス キャッシュ エントリのタイプによって異なります。

アクセス キャッシュ エントリのタイプ	説明	更新間隔（秒）
ポジティブ エントリ	クライアントのアクセスが拒否されなかったアクセス キャッシュ エントリです。	最小値：300 最大値：86,400 デフォルト：3,600
ネガティブ エントリ	クライアントのアクセスが拒否されたアクセス キャッシュ エントリです。	最小値：60 最大値：86,400 デフォルト：3,600

例

NFSクライアントがクラスタ上のボリュームへのアクセスを試みます。Data ONTAPは、エクスポート ポリシー ルールに照らしてクライアントをチェックし、エクスポート ポリシー ルールの設定に基づいてクライアントにアクセスを許可します。Data ONTAPはこのエクスポート ポリシー ルールをポジティブ エントリとしてアクセス キャッシュに格納します。デフォルトでは、Data ONTAPは、このポジティブ エントリを1時間（3,600秒）アクセス キャッシュ内に保持したあと、このエントリを自動的に更新して情報を最新の状態に保ちます。

不要なエントリでアクセス キャッシュがいっぱいになるのを避けるために、クライアント アクセスの判断に一定期間使用されていない既存のアクセス キャッシュ エントリをクリアする追加のパラメータがあります。この`-harvest-timeout`パラメータには60～2,592,000秒の範囲の値を指定できます。デフォルトは86,400秒です。

アクセス キャッシュのパフォーマンスの最適化

複数のパラメータを設定して、アクセス キャッシュを最適化したり、パフォーマンスとアクセス キャッシュ内に保存された情報の更新間隔とのバランスを取ったりすることができます。

タスク概要

アクセス キャッシュの更新間隔を設定する際には、次の点に注意してください。

- 値を大きくすると、エントリがアクセス キャッシュに保存される期間が長くなります。
  長所としては、Data ONTAPがアクセス キャッシュ エントリの更新で消費するリソースが減少するため、パフォーマンスが向上します。短所は、エクスポート ポリシー ルールが変更されてアクセス キャッシュ エントリが古くなった場合、エントリが更新されるまでの時間が長くなることです。その結果、アクセスできるはずのクライアントが拒否され、拒否されるはずのクライアントがアクセスを許可される可能性があります。
- 値を小さくすると、Data ONTAPがアクセス キャッシュ エントリを更新する頻度が高くなります。
  長所は、エントリが比較的新しいため、クライアントに対するアクセスの許可または拒否が正しく行われる可能性が高くなることです。短所としては、Data ONTAPがアクセス キャッシュ エントリの更新で消費するリソースが増加するため、パフォーマンスが低下します。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

変更の対象	コマンド
ポジティブ エントリの更新間隔	`vserver export-policy access-cache config modify-all-vservers -refresh-period-positive` *`timeout_value`*
ネガティブ エントリの更新間隔	`vserver export-policy access-cache config modify-all-vservers -refresh-period-negative` *`timeout_value`*
古いエントリのタイムアウト時間	`vserver export-policy access-cache config modify-all-vservers -harvest-timeout` *`timeout_value`*

3. 新しいパラメータ設定を確認します。

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

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。

関連コンセプト

NFSv4ファイル委譲の管理（122ページ）

関連タスク

NFSv4ファイルおよびレコード ロックの設定（125ページ）

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。

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  -
               Delegation Type: write
```

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	**`vserver locks break -vserver`** ***`vserver_name`*** **`-volume`** ***`volume_name`*** **`-path`** ***`path`*** **`-lif`** ***`lif`***
ロックID	**`vserver locks break -lockid`** ***`UUID`***

`-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`

NFSv4.1サーバ実装IDの変更

NFSv4.1プロトコルには、サーバのドメイン、名前、および日付を記録したサーバ実装IDが含まれています。このサーバ実装IDのデフォルト値は変更することができます。デフォルト値を変更することは、たとえば、使用率の統計を収集したり、相互運用性の問題を解決したりする場合に役立つことがあります（詳細については、RFC 5661を参照）。

タスク概要

3つのオプションのデフォルト値は、次のとおりです。

オプション	オプション名	デフォルト値
NFSv4.1実装IDのドメイン	`-v4.1-implementation-domain`	netapp.com
NFSv4.1実装IDの名前	`-v4.1-implementation-name`	クラスタ バージョンの名前
NFSv4.1実装IDの日付	`-v4.1-implementation-date`	クラスタ バージョンの日付

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。

変更するNFSv4.1実装IDのオプション	入力するコマンド
ドメイン	**`vserver nfs modify -v4.1-implementation-domain` *`domain`***
名前	**`vserver nfs modify -v4.1-implementation-name` *`name`***
日付	**`vserver nfs modify -v4.1-implementation-date` *`date`***

3. admin権限レベルに戻ります。

   `set -privilege admin`

NFSv4 ACLの管理

NFSv4 Access Control List（ACL;アクセス制御リスト）を有効化、無効化、設定、変更、および表示できます。

NFSv4 ACLを有効化する利点

NFSv4 ACLを有効化すると多くの利点を得られます。

以下に、その利点を示します。

- ファイルやディレクトリへのユーザ アクセスのより詳細な制御
- NFSセキュリティの向上
- CIFSとの相互運用性の向上
- ユーザあたりの最大NFSグループ数（16）の解除

NFSv4 ACLの仕組み

NFSv4 ACLを使用しているクライアントは、システム上のファイルとディレクトリにACLを設定し、そのACLを表示することができます。ACLが設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、そのACL内のACEのうち、該当する継承フラグが指定されたACLエントリ（ACE）がすべて継承されます。

アクセス チェックでは、CIFSユーザがUNIXユーザにマッピングされ、マッピングされたUNIXユーザとそのユーザのグループ メンバーシップがACLに照らしてチェックされます。

ファイルやディレクトリにACLが設定されている場合、ファイルやディレクトリのアクセスに使用されているプロトコルの種類（NFSv3、NFSv4、またはCIFS）にかかわらず、またシステムでNFSv4が有効でなくなったあとも、そのACLを使用してアクセスが制御されます。

親ディレクトリのNFSv4 ACLのACEに正しい継承フラグが設定されていれば、ファイルやディレクトリは該当するACEを継承します（必要な変更が加えられる可能性があります）。

ACLごとのACEの最大数は、`-v4-acl-max-aces`パラメータで定義するとおり1,024です。このパラメータのデフォルトは400です。`-v4-acl-preserve`パラメータが有効になっており、オブジェクトにUNIXモード ビットとACLの両方が設定されている場合、OWNER、GROUP、およびEVERYONEに適切なアクセス権を付与するには、ACLで3つの必須ACEが必要になります。これらの必須ACEは、ユーザが`chmod`操作を実行してモード ビットを設定するときに、Data ONTAPによって自動的に適用されます。必須ACEが不足しているACLを設定すると、そのACLのACEの数が制限されて不足している必須ACE用にスペースがリザーブされ、モード ビットも設定することにした場合にあとで必須ACEを追加できるようになります。

ファイルやディレクトリがNFSv4要求によって作成される場合、作成されるファイルやディレクトリのACLは、ファイル作成要求にACLが含まれているか、または標準のUNIXファイル アクセス権限のみが含まれているか、および親ディレクトリにACLが設定されているかどうかによって異なります。

- 要求にACLが含まれる場合は、そのACLが使用されます。
- 要求に標準のUNIXファイル アクセス権限のみが含まれ、親ディレクトリにACLがある場合、親ディレクトリのACLのACEに該当する継承フラグが設定されていれば、それらのACEが新しいファイルやディレクトリに継承されます。

  注: 親のACLは、`-v4.0-acl`が**`off`**の場合でも継承されます。

- 要求に標準のUNIXファイル アクセス権限のみが含まれ、親ディレクトリにACLがない場合は、クライアントのファイル モードを使用して標準のUNIXファイル アクセス権限が設定されます。
- 要求に標準UNIXファイル アクセス権限のみが含まれ、親ディレクトリに継承できないACLがある場合は、モード ビットのみを使用して新しいオブジェクトが作成されます。

NFSv4 ACLの変更の有効化と無効化

Data ONTAPがACLが設定されたファイルまたはディレクトリに対してchmodコマンドを受信した場合、デフォルトではACLは保持され、モード ビットの変更を反映して変更されます。代わりにACLを破棄するには、-v4-acl-preserveパラメータを無効にして動作を変更します。

タスク概要

unifiedセキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対するchmod、chgroup、またはchownコマンドを送信した際にNTFSファイル アクセス権を保持するか破棄するかも決定します。

このパラメータのデフォルト設定はenabledです。

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。

状況	入力するコマンド
既存のNFSv4 ACLの保持と変更を有効にする（デフォルト）	`vserver nfs modify -vserver vserver_name -v4-acl-preserve enabled`
保持を無効にして、モード ビットの変更時にNFSv4 ACLを破棄する	`vserver nfs modify -vserver vserver_name -v4-acl-preserve disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

Data ONTAPでのNFSv4 ACLを使用したファイル削除の可否の判別方法

ファイルを削除できるかどうかを判別するために、Data ONTAPは、そのファイルのDELETEビットと、ファイルが含まれるディレクトリのDELETE_CHILDビットの組み合わせを使用します。詳細については、NFS 4.1 RFC 5661を参照してください。

NFSv4 ACLの有効化と無効化

NFSv4 ACLを有効または無効にするには、-v4.0-aclオプションと-v4.1-aclオプションを変更します。これらのオプションはデフォルトで無効になっています。

タスク概要

-v4.0-aclオプションまたは-v4.1-aclオプションは、NFSv4 ACLの設定と表示を制御しますが、アクセス チェックでのNFSv4 ACLの適用は制御しません。

NFSv4.0 ACLは、Infinite Volumeを備えたStorage Virtual Machine（SVM）ではサポートされません。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4.0 ACLを有効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.0-acl enabled**
NFSv4.0 ACLを無効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.0-acl disabled**
NFSv4.1 ACLを有効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.1-acl enabled**
NFSv4.1 ACLを無効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.1-acl disabled**

NFSv4 ACLの最大ACE数の変更

パラメータ`-v4-acl-max-aces`を編集して、各NFSv4 ACLに許可するACEの最大数を変更できます。デフォルトでは、ACLあたりのACEの数は400個に制限されています。この制限値を増やせば、400個以上のACEを含むACLのデータを、Data ONTAPを実行するストレージ システムへ移行することができます。

タスク概要

ただし、この制限値を増やすと、NFSv4 ACLを含むファイルにアクセスするクライアントのパフォーマンスが低下することがあります。

手順

1. 権限レベルをadvancedに設定します。

   set -privilege advanced

2. NFSv4 ACLのACEの最大制限数を変更するには、次のコマンドを入力します。

   vserver nfs modify -v4-acl-max-aces *max_ace_limit*

   *max_ace_limit*値の有効範囲は**192～1024です。**

3. admin権限レベルに戻ります。

   set -privilege admin

NFSv4ファイル委譲の管理

NFSv4ファイル委譲を有効または無効にしたり、NFSv4ファイル委譲統計を取得したりできます。

関連コンセプト

ファイル ロックの管理（115ページ）

NFSv4ファイル委譲の仕組み

Data ONTAPはRFC 3530に従って、読み取りファイル委譲と書き込みファイル委譲をサポートします。

RFC 3530で指定されているとおり、NFSv4クライアントがファイルを開くとき、Data ONTAPはオープン要求や書き込み要求のそれ以降の処理を、開いているクライアントに委譲することができます。ファイル委譲には、次の2つのタイプがあります。

- 読み取り
  読み取りファイル委譲の場合、クライアントは、読み取りのためのファイル オープン要求のうち、他のファイルへの読み取りアクセスを拒否しない要求をローカルで処理できます。バイト単位の読み取りロックもローカルで処理されます。
- 書き込み
  書き込みファイル委譲の場合、クライアントはすべてのオープン要求を処理できます。バイト単位のロック要求はすべてローカルで処理されます。

便宜的ロック（oplock）が有効であるかどうかに関係なく、委譲はすべての形式のqtree内のファイルに対して機能します。

ファイル処理のクライアントへの委譲は、リースが期限切れになったとき、またはストレージ システムが他のクライアントから次の要求を受け取ったときにリコールすることができます。

- ファイルへの書き込み、書き込みのためのファイル オープン、または「読み取り拒否」のためのファイル オープン
- ファイル属性の変更
- ファイルの名前変更
- ファイルの削除

リースが期限切れになると、委譲状態は取り消され、関連するすべての状態は「soft」とマークされます。つまり、以前に委譲状態であったクライアントがリースを更新する前に、ストレージ システムが同じファイルに対して他のクライアントから競合するロック要求を受け取った場合、この競合するロックは認められます。競合するロックがなく、委譲を保持しているクライアントがリース期限を更新した場合、ソフト ロックはハード ロックに変更され、アクセスが競合しても削除されることはありません。ただし、リース期限が更新されても委譲は再び認められません。

サーバがリブートされると、委任状態は失われます。クライアントは、委譲要求プロセスをすべて再実行しなくても、再接続時に委譲状態を再要求することができます。読み取り委譲を保持しているクライアントがリブートされると、すべての委譲状態情報が再接続時にストレージ システムのキャッシュからフラッシュされます。クライアントは委譲要求を発行して新しい委譲を確立する必要があります。

注: NFSv4.0ファイル委譲は、Infinite Volumeを備えたStorage Virtual Machine（SVM）ではサポートされません。

NFSv4読み取りファイル委譲の有効化と無効化

NFSv4読み取りファイル委譲を有効または無効にするには、`-v4.0-read-delegation`オプションまたは`-v4.1-read-delegation`オプションを変更します。読み取りファイル委譲を有効にすると、ファイルのオープンとクローズに伴うメッセージのオーバーヘッドを大幅に軽減できます。

タスク概要

デフォルトでは、読み取りファイル委譲は無効です。

読み取りファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリする必要があることです。

NFSv4.0ファイル委譲は、Infinite Volumeを備えたStorage Virtual Machine（SVM）ではサポートされません。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4読み取りファイル委譲を有効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.0-read-delegation enabled**
NFSv4.1読み取りファイル委譲を有効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.1-read-delegation enabled**
NFSv4読み取りファイル委譲を無効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.0-read-delegation disabled**
NFSv4.1読み取りファイル委譲を無効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.1-read-delegation disabled**

タスクの結果

ファイル委譲オプションへの変更はすぐに反映されます。NFSのリブートやリスタートは必要ありません。

NFSv4書き込みファイル委譲の有効化と無効化

書き込みファイル委譲を有効または無効にするには、`-v4.0-write-delegation`オプションまたは`-v4.1-write-delegation`オプションを変更します。書き込みファイル委譲を有効にすると、ファイルのオープンとクローズだけでなく、ファイルおよびレコードのロックに関連するメッセージのオーバーヘッドを大幅に軽減できます。

タスク概要

デフォルトでは、書き込みファイル委譲は無効です。

書き込みファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリするための追加タスクを実行する必要があることです。

NFSv4.0ファイル委譲は、Infinite Volumeを備えたStorage Virtual Machine（SVM）ではサポートされません。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4書き込みファイル委譲を有効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.0-write-delegation enabled**

状況	操作
NFSv4.1書き込みファイル委譲を有効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.1-write-delegation enabled**
NFSv4書き込みファイル委譲を無効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.0-write-delegation disabled**
NFSv4.1書き込みファイル委譲を無効にする	次のコマンドを入力します。 **vserver nfs modify -vserver *vserver_name* -v4.1-write-delegation disabled**

タスクの結果

ファイル委譲オプションへの変更はすぐに反映されます。NFSのリブートやリスタートは必要ありません。

NFSv4ファイルおよびレコード ロックの設定

NFSv4のファイルおよびレコード ロックを設定するには、ロック リース期間および猶予期間を指定します。

関連コンセプト

ファイル ロックの管理（115ページ）

NFSv4ファイルおよびレコード ロックについて

NFSv4クライアントの場合、Data ONTAPはNFSv4のファイルロック メカニズムをサポートしているため、すべてのファイルのロック状態がリースベース モデルで保持されます。

Data ONTAPは、RFC 3530に従って、「あるNFSクライアントで保持されているすべての状態に対してリース期間を1つ定義します。この定義された期間内にクライアントがリースを更新しない場合は、クライアントのリースに関連付けられたすべての状態がサーバによって解放される可能性があります。」クライアントはファイル読み取りなどの操作を実行して、リースを明示的または暗黙的に更新できます。

Data ONTAPは猶予期間も定義します。猶予期間とは、サーバ リカバリ中にクライアントが自身のロック状態を再要求する、特別な処理期間のことです。

用語	定義（RFC 3530を参照）
リース	Data ONTAPがクライアントを解除不能なロック状態に設定する期間。
猶予期間	サーバ リカバリ中にクライアントが自身のロック状態をData ONTAPに再要求する期間。
ロック	他に特に記載がないかぎり、レコード（バイト範囲）ロックとファイル（共有）ロックの両方を表します。

NFSv4ロック リース期間の指定

NFSv4ロック リース期間（Data ONTAPがクライアントに解除不能なロックを付与する期間）を指定するには、`-v4-lease-seconds`オプションを変更します。リース期間が短いほどサーバのリカバ

リにかかる時間は短くなりますが、多数のクライアントに対処するサーバについてはリース期間を長くすると効果的です。

タスク概要

デフォルトでは、このオプションは**30**に設定されています。このオプションの最小値は**10**です。このオプションの最大値はロック猶予期間の値です。ロック猶予期間は`locking.lease_seconds`オプションで設定できます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds
   number_of_seconds
   ```

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4ロック猶予期間の指定

NFSv4ロック猶予期間（サーバ リカバリ中に、クライアントがロック状態になるようにData ONTAPに再要求する期間）を指定するには、`-v4-grace-seconds`オプションを変更します。

タスク概要

デフォルトでは、このオプションは**45**に設定されています。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds
   number_of_seconds
   ```

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4リファーラルの仕組み

NFSv4リファーラルを有効にすると、Data ONTAPでNFSv4クライアントに対して「SVM内」リファーラルが発行されるようになります。SVM内リファーラルでは、クラスタ ノードがNFSv4要求を受け取ったときに、NFSv4クライアントがStorage Virtual Machine（SVM）の別のLIFを参照します。

NFSv4クライアントは、それ以降、ターゲットLIFでリファーラルを受け取ったパスにアクセスする必要があります。元のクラスタ ノードがこのようなリファーラルを発行するのは、データ ボリュームが存在するクラスタ ノード上のSVMにLIFがあるため、クライアントがデータにより高速にアクセスでき、余分なクラスタ通信が回避されると判断された場合です。

NFSv4リファーラルは、すべてのNFSv4クライアントで一様にサポートできるわけではありません。すべてのクライアントがこの機能をサポートするとは限らない環境では、リファーラルを有効にしないでください。この機能が有効で、この機能をサポートしていないクライアントがサーバからリファーラルを受け取った場合、そのクライアントはボリュームにアクセスできずにエラーとなります。

リファーラルの詳細については、RFC3530を参照してください。

注: リファーラルはInfinite Volumeを備えたSVMではサポートされません。

NFSv4リファーラルの有効化と無効化

FlexVolを備えたStorage Virtual Machine（SVM）でNFSv4リファーラルを有効にするには、`-v4-fsid-change`オプションと、`-v4.0-referrals`オプションまたは`-v4.1-referrals`オプションを有効にします。NFSV4リファーラルを有効にすると、この機能をサポートするNFSv4クライアントのデータへのアクセス スピードを向上できます。

開始する前に

NFSリファーラルを有効にする場合は、まずParallel NFSを無効にする必要があります。両方を同時に有効にすることはできません。

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。

状況	入力するコマンド
NFSv4リファーラルを有効にする	**`vserver nfs modify -vserver *vserver_name* -v4-fsid-change enabled`** **`vserver nfs modify -vserver *vserver_name* -v4.0-referrals enabled`**
NFSv4リファーラルを無効にする	**`vserver nfs modify -vserver *vserver_name* -v4.0-referrals disabled`**
NFSv4.1リファーラルを有効にする	**`vserver nfs modify -vserver *vserver_name* -v4-fsid-change enabled`** **`vserver nfs modify -vserver *vserver_name* -v4.1-referrals enabled`**
NFSv4.1リファーラルを無効にする	**`vserver nfs modify -vserver *vserver_name* -v4.1-referrals disabled`**

3. admin権限レベルに戻ります。

   `set -privilege admin`

関連タスク

pNFSの有効化と無効化（89ページ）

NFS統計の表示

パフォーマンスの監視と問題の診断を行うために、ストレージ システム上のStorage Virtual Machine（SVM）に対するNFS統計を表示できます。

手順

1. `statistics catalog object show`コマンドを使用して、データを表示できるNFSオブジェクトを特定します。

例

statistics catalog object show -object nfs*

`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。

2. `statistics start`コマンドとオプションの`statistics stop`コマンドを使用して、1つ以上のオブジェクトからデータ サンプルを収集します。
3. `statistics show`コマンドを使用してサンプル データを表示します。

例：NFSv3のパフォーマンスの監視

以下に、NFSv3プロトコルのパフォーマンス データを表示する例を示します。

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。

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、正常に行われた読み込み要求および書き込み要求の数と読み込み要求と書き込み要求の総数の比較を示すカウンタを指定することにより、サンプルのデータを表示します。

```
vs1::> statistics show -sample-id nfs_sample -counter read_total|
write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                                 Value
    --------------------------- ---------------------------
    read_success                                            40042
    read_total                                              40042
    write_success                                         1492052
    write_total                                           1492052
```

VMware vStorage over NFSのサポート

Data ONTAPは、NFS環境で特定のVMware vStorage API for Array Integration（VAAI）機能をサポートしています。

サポートされる機能

次の機能がサポートされます。

- コピー オフロード
  ESXiホストで、仮想マシンや仮想マシン ディスク（VMDK）のコピーを、ホストを介さずにソースとデスティネーションのデータ ストア間で直接行うことができます。これにより、ESXiホストのCPUサイクルやネットワーク帯域幅を節約できます。ソース ボリュームがスパース ボリュームの場合、コピー オフロードでスペース効率が保持されます。
- スペース リザベーション
  スペースをリザーブしてVMDKファイル用のストレージ スペースを確保します。

制限事項

NFSでVMware vStorageを使用する際には、次の制限事項があります。

- vStorageは、Infinite Volumeを備えたStorage Virtual Machine（SVM）ではサポートされません。
- 次の場合にコピー オフロード処理が失敗することがあります。
  - ソースまたはデスティネーションのボリュームでwaflironを実行しているとき（ボリュームが一時的にオフラインになるため）。
  - ソース ボリュームまたはデスティネーション ボリュームを移動しているとき。
  - ソースまたはデスティネーションのLIFを移動しているとき。
  - テイクオーバーまたはギブバック処理を実行しているとき。
- 次のシナリオでは、ファイル ハンドル形式の違いによってサーバ側のコピーが失敗する可能性があります。
  qtreeのエクスポートを現在または以前に行ったSVMから、これまで一度もqtreeをエクスポートしたことがないSVMへデータのコピーを試みた場合。この問題を回避するには、コピー先SVMで少なくとも1つのqtreeをエクスポートします。

関連情報

ネットアップの技術情報アーティクル3011208：「What VAAI configurations are supported on Data ONTAP storage controllers?」

VMware vStorage over NFSの有効化と無効化

FlexVolを備えたStorage Virtual Machine（SVM）でVMware vStorage over NFSのサポートを有効または無効にするには、`vserver nfs modify`コマンドを使用します。

タスク概要

デフォルトでは、VMware vStorage over NFSのサポートは無効になっています。

手順

1. 次のコマンドを入力して、SVMにおける現在のvStorageのサポート ステータスを表示します。

   `vserver nfs show -vserver vserver_name -instance`

2. 次のいずれかを実行します。

状況	入力するコマンド
VMware vStorageのサポートを有効にする	**`vserver nfs modify -vserver vserver_name -vstorage enabled`**
VMware vStorageのサポートを無効にする	**`vserver nfs modify -vserver vserver_name -vstorage disabled`**

終了後の操作

この機能を使用する前に、VMware VAAIのNFSプラグインをインストールする必要があります。詳細については、『*Installing the NetApp NFS Plug-in for VMware VAAI*』を参照してください。

関連情報

ネットアップのマニュアル：NetApp NFS Plug-in for VMware VAAI

rquotaのサポートの有効化と無効化

Data ONTAPでは、remote quota protocol バージョン1（rquota v1）をサポートしています。rquotaプロトコルを使用すると、NFSクライアントは、リモート マシンからユーザとグループのクォータ情報を取得できます。FlexVolを備えたStorage Virtual Machine（SVM）でrquotaを有効にするには、`vserver nfs modify`コマンドを使用します。

タスク概要

デフォルトでは、rquota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
SVMでrquotaのサポートを有効にする	**vserver nfs modify -vserver *vserver_name* -rquota enable**
SVMでrquotaのサポートを無効にする	**vserver nfs modify -vserver *vserver_name* -rquota disable**

クォータの詳細については、『*clustered Data ONTAP 論理ストレージ管理ガイド*』を参照してください。

TCP最大読み取りサイズおよび書き込みサイズの変更によるNFSv3のパフォーマンスの向上

高遅延のネットワーク経由でストレージ システムに接続するNFSv3クライアントのパフォーマンスを向上させるには、TCPの読み取りと書き込みのサイズを変更します。

クライアントがワイド エリア ネットワーク（WAN）または10ミリ秒を超える遅延速度のメトロ エリア ネットワーク（MAN）などの高遅延ネットワークを介してストレージ システムにアクセスする場合、TCPの読み取り / 書き込みの最大サイズを変更することで、ネットワーク接続のパフォーマンスが向上する場合があります。ローカル エリア ネットワーク（LAN）などの低遅延ネットワークでストレージ システムにアクセスするクライアントは、これらのパラメータを変更してもパフォーマンスの向上はあまり期待できません。スループットの向上が遅延の影響を上回ることがない場合は、これらのパラメータを使用しないでください。

ストレージ環境がこれらのパラメータの変更の恩恵を受けるかどうかを判断するには、まずパフォーマンスの低いNFSクライアントで総合的なパフォーマンス評価を行ってください。パフォーマンスの低さが、クライアント上の過剰なラウンド トリップによる遅延とデータ量の少ない要求によるものかどうかを確認します。このような条件の場合、クライアントとサーバは、接続を介して送信されるデータ量の少ない要求と応答を待機することにそのデューティ サイクルの大部分を費やすので、利用可能な帯域幅を完全に使用することができません。

NFSv3の要求サイズを大きくすることにより、クライアントとサーバは、利用可能な帯域幅をより効果的に使用でき、単位時間当たりの転送データ量が多くなるため、結果として、接続の全体的な効率が向上します。

ストレージ システムとクライアントの間で設定が異なる場合があることに留意してください。最大1MBの読み取りサイズをサポートするようにストレージ システムを構成しても、クライアントが64KBしかサポートしない場合、マウントの読み込みサイズは64KB以下に制限されます。

これらのパラメータを変更する前に注意しなければならないのは、変更した結果、データ量の多い応答を構築して送信するのに時間がかかり、ストレージ システムでのメモリ消費が増えるというこ

とです。ストレージ システムへの高遅延接続が多くなるほど、メモリ消費量は多くなります。メモリ容量が高いストレージ システムでは、パラメータの変更による影響はほとんどありません。メモリ容量の低いストレージ システムでは、パフォーマンスが著しく低下する可能性があります。

これらのパラメータをうまく調整できるかどうかは、クラスタの複数のノードからデータを取得できるかどうかによります。クラスタ ネットワーク固有の遅延によって、応答の全体的な遅延を増加させる可能性があります。これらのパラメータを使用するときに、遅延が全体的に増大しがちです。したがって、遅延の影響を受けやすいワークロードは悪影響をもたらす可能性があります。

NFSv3 TCP最大読み取りサイズおよび書き込みサイズの変更

`-v3-tcp-max-read-size`および`-v3-tcp-max-write-size`オプションを変更して、NFSv3 TCPの読み取りと書き込みの最大サイズを指定できます。これらのオプションを変更すると、ストレージ環境によっては、TCP上のNFSv3のパフォーマンスが向上することがあります。

開始する前に

クラスタ内のすべてのノードでData ONTAP 8.1以降が実行されている必要があります。

タスク概要

これらのオプションは、Storage Virtual Machine（SVM）ごとに個別に変更できます。

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。

状況	入力するコマンド
NFSv3 TCPの最大読み取りサイズの変更	**`vserver nfs modify -vserver *vserver_name* -v3-tcp-max-read-size *integer_max_read_size***`
NFSv3 TCPの最大書き込みサイズの変更	**`vserver nfs modify -vserver *vserver_name* -v3-tcp-max-write-size *integer_max_write_size***`

オプション	範囲	デフォルト値
`-v3-tcp-max-read-size`	8,192～1,048,576バイト	65,536バイト
`-v3-tcp-max-write-size`	8,192～65,536バイト	65,536バイト

注: 入力する読み取りまたは書き込みの最大サイズは、4KB（4,096バイト）の倍数値でなければなりません。リクエストが要件を満たしていない場合は、パフォーマンスが低下します。

3. admin権限レベルに戻ります。

   `set -privilege admin`

4. 変更内容を確認するには、`vserver nfs show`コマンドを使用します。

5. 静的マウントを使用しているクライアントがある場合、変更したパラメータのサイズを有効にするには、いったんアンマウントしてから再度マウントします。

例

次のコマンドでは、vs1というSVMのNFSv3 TCP の最大読み取りサイズを1,048,576バイトに設定しています。

```
vs1::> vserver nfs modify -vserver vs1 -v3-tcp-max-read-size 1048576
```

NFSユーザに許可するグループID数の設定

Data ONTAPは、Kerberos（RPCSEC_GSS）認証を使用してNFSユーザ クレデンシャルを処理する場合、デフォルトで最大32個のグループIDをサポートしています。AUTH_SYS認証を使用する場合のグループIDのデフォルトの最大数は、RFC 5331で定義されている16個です。デフォルト数を超えるグループに属しているユーザがいる場合は、この最大数を1,024まで増やすことができます。

タスク概要

ユーザのクレデンシャルにデフォルト数を超えるグループIDが含まれている場合、超過分のグループIDは切り捨てられます。そのため、ユーザがストレージ システムのファイルへのアクセスを試みるとエラーが発生する可能性があります。グループの最大数は、SVMごとに、環境内の最大グループ数と同じ値に設定する必要があります。

次の表に、グループIDの最大数を決定する`vserver nfs modify`コマンドの2つのパラメータと、3つの設定例を示します。

パラメータ	設定	グループIDの最大数
`-extended-groups-limit` `-auth-sys-extended-groups`	**`32`** **`disabled`** これらはデフォルトの設定です。	RPCSEC_GSS：32 AUTH_SYS：16
`-extended-groups-limit` `-auth-sys-extended-groups`	**`256`** **`disabled`**	RPCSEC_GSS：256 AUTH_SYS：16
`-extended-groups-limit` `-auth-sys-extended-groups`	**`512`** **`enabled`**	RPCSEC_GSS：512 AUTH_SYS：512

注: 古いNFSクライアントの一部は、AUTH_SYSの拡張グループに対応していない可能性があります。

手順

1. 権限レベルをadvancedに設定します。

   `set -privilege advanced`

2. 次のうち必要な操作を実行します。

最大グループ数の設定対象	入力するコマンド
RPCSEC_GSSのみ（AUTH_SYSはデフォルト値16のまま）	**`vserver nfs modify -vserver *vserver_name* -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`**
RPCSEC_GSSとAUTH_SYSの両方	**`vserver nfs modify -vserver *vserver_name* -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`**

3. `-extended-groups-limit`の値を確認し、AUTH_SYSが拡張グループを使用していることを確認します。

vserver nfs show -vserver *vserver_name* -fields auth-sys-extended-groups,extended-groups-limit

4. admin権限レベルに戻ります。

   set -privilege admin

例

次の例は、AUTH_SYS認証の拡張グループを有効にし、AUTH_SYS認証とRPCSEC_GSS認証の両方で拡張グループの最大数を512に設定します。これらの変更は、SVM vs1にアクセスするクライアントに対してのみ行われます。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups
enabled -extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

NTFSセキュリティ形式のデータへのrootユーザ アクセスの制御

NTFSセキュリティ形式のデータへのNFSクライアント アクセスを許可したり、NTFSクライアントによるNFSセキュリティ形式データへのアクセスを許可したりするようにData ONTAPを設定することができます。NFSデータ ストアでNTFSセキュリティ形式を使用する際には、rootユーザによるアクセスの処理方法を決定し、それに応じてStorage Virtual Machine（SVM）を設定する必要があります。

タスク概要

rootユーザがNTFSセキュリティ形式のデータにアクセスする際には、次の2つのオプションがあります。

- その他すべてのNFSユーザと同様にrootユーザをWindowsユーザにマッピングし、NTFS ACLに従ってアクセスを管理する。
- NTFS ACLを無視してフル アクセスをrootに対して提供する。

手順

1. 権限レベルをadvancedに設定します。

   set -privilege advanced

2. 次のうち必要な操作を実行します。

rootユーザへの対処方法.	入力するコマンド
Windowsユーザへのマッピング	**vserver nfs modify -vserver *vserver_name* -ignore-nt-acl-for-root disabled**

rootユーザへの対処方法.	入力するコマンド
NT ACLチェックのバイパス	`vserver nfs modify -vserver vserver_name -ignore-nt-acl-for-root enabled`

このパラメータはデフォルトで無効になっています。

このパラメータが有効になっていてもrootユーザに対するネーム マッピングが存在しない場合、Data ONTAPはデフォルトのSMB管理者のクレデンシャルを監査に使用します。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

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。

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が確認されます。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（135ページ）

サポートされる監査イベント ログの形式（139ページ）
監査できるSMBイベント（140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（150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（145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（164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に依存します。

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に依存します。
  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（146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（150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（136ページ）

関連タスク

監査イベント ログの手動ローテーション（160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 ポリシーのステージング 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と、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（EVT / 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

イベントID（EVT / EVTX）	イベント	説明	カテゴリ
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
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。 **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

イベントID（EVT / EVTX）	イベント	説明	カテゴリ
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">00000000000401;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（153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（かっこ内）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

```
                                 Junction                       Junction
Vserver   Volume       Language Active    Junction Path     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.text

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">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">(data1);/dir1/file1.txt:stream1</
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">00000000000401;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と、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（156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
SVM名 監査設定を作成するSVMの名前。SVMはすでに存在している必要があります。	`-vserver` *vserver_name*	○	○	
ログ デスティネーション パス 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。 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。 パスが有効でない場合、監査設定コマンドは失敗します。 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。	`-destination` *text*	○	○	

情報の種類	オプション	必須	含める	値
監査するイベントのカテゴリ 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。 • ファイル アクセス イベント（SMBとNFSv4の両方） • 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 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ドメイン以降で使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。 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。 **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。 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。	`-events {`**`file-ops`**`|`**`cifs-logon-logoff`**`|`**`cap-staging`**`}`	×		
ログ ファイルの出力形式 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。	`-format {`**`xml`**`|`**`evtx`**`}`	×		

情報の種類	オプション	必須	含める	値
ログ ファイルのローテーションの制限 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。 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` *integer*	×		

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
ログ ファイルの最大サイズ 監査ログ ファイルの最大サイズを指定します。	`-rotate-size` {*integer*[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
ログ ローテーション スケジュール:月 監査ログのローテーションを実行する月を指定します。 指定できる値は、**January**～**December**と、**all**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。	`-rotate-schedule-month` *chron_month*	×		
ログ ローテーション スケジュール:曜日 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。 指定できる値は、**January**～**December**と、**all**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。	`-rotate-schedule-dayofweek` *chron_dayofweek*	×		
ログ ローテーション スケジュール:日 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。 指定できる値は、**1**～**31**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。	`-rotate-schedule-day` *chron_dayofmonth*	×		
ログ ローテーション スケジュール:時間 監査ログのローテーションを実行する時間を決めます。 指定できる値の範囲は、**0**(午前零時)～**23**(午後11時)です。**all**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。	`-rotate-schedule-hour` *chron_hour*	×		
ログ ローテーション スケジュール:分 監査ログのローテーションを実行する分を決めます。 指定できる値の範囲は、**0**～**59**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。	`-rotate-schedule-minute` *chron_minute*	○(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(152ページ)
監査の要件と考慮事項(138ページ)
サポートされる監査イベント ログの形式(139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（150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（150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（152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（152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（146ページ）
Data ONTAP CLIを使用したNTFS監査ポリシーの設定方法（156ページ）
監査設定の管理（160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（153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（156ページ）
SVMでの監査の有効化と無効化（161ページ）
監査設定の削除（163ページ）
監査イベント ログの手動ローテーション（160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	コマンド
ログ サイズ	**vserver audit create -vserver *vserver_name* -destination *path* -events [{file-ops|cifs-logon-logoff|cap-staging}] [-format {xml|evtx}] [-rotate-limit *integer*] [-rotate-size {*integer*[KB|MB|GB|TB|PB]}]**
スケジュール	**vserver audit create -vserver *vserver_name* -destination *path* -events [{file-ops|cifs-logon-logoff|cap-staging}] [-format {xml|evtx}] [-rotate-limit *integer*] [-rotate-schedule-month *chron_month*] [-rotate-schedule-dayofweek *chron_dayofweek*] [-rotate-schedule-day *chron_dayofmonth*] [-rotate-schedule-hour *chron_hour*] -rotate-schedule-minute *chron_minute*** **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（136ページ）
監査できるSMBイベント（140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（157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	a. **[追加]**をクリックします。 b. **[選択するオブジェクト名を入力してください]**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。 c. **[OK]**をクリックします。
ユーザまたはグループから監査を削除する	a. **[選択するオブジェクト名を入力してください]**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。 b. **[削除]**をクリックします。 c. **[OK]**をクリックします。 d. 残りの手順は不要です。
ユーザまたはグループの監査を変更する	a. **[選択するオブジェクト名を入力してください]**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。 b. **[編集]**をクリックします。 c. **[OK]**をクリックします。

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（140ページ）

関連タスク

CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示（158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（157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

監査できるSMBイベント（140ページ）

関連タスク

CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示（158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

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。

関連コンセプト

NFSv4 ACLの管理（119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（145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

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（152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 Acces 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	**vserver security file-directory show -vserver *vserver_name* -path *path***
詳細情報を展開	**vserver security file-directory show -vserver *vserver_name* -path *path* -expand-mask true**

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-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|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-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|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（164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（139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（150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	**vserver audit enable -vserver *vserver_name***
無効	**vserver audit disable -vserver *vserver_name***

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（163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（150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	*vserver audit modify*と-destinationパラメータ
監査するイベントのカテゴリの変更	*vserver audit modify*と-eventsパラメータ **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	*vserver audit modify*と-format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	*vserver audit modify*と -rotate-sizeパラメータ
時間間隔に基づいた自動保存の有効化	*vserver audit modify*と-rotate-schedule-month、-rotate-schedule-dayofweek、-rotate-schedule-day、-rotate-schedule-hour、および-rotate-schedule-minuteパラメータ
保存されるログ ファイルの最大数の指定	*vserver audit modify*と -rotate-limit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 disable -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（161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（161ページ）
監査設定の削除（163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（138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。

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て、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。

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（167ページ）
FPolicyと外部FPolicyサーバとの連携（168ページ）
SVMネームスペースにおけるFPolicyサービスの仕組み（171ページ）
FPolicyの設定タイプ（171ページ）
FPolicyの設定手順とは（176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（168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（168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 ブロッキング
- 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（169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て、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（189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。

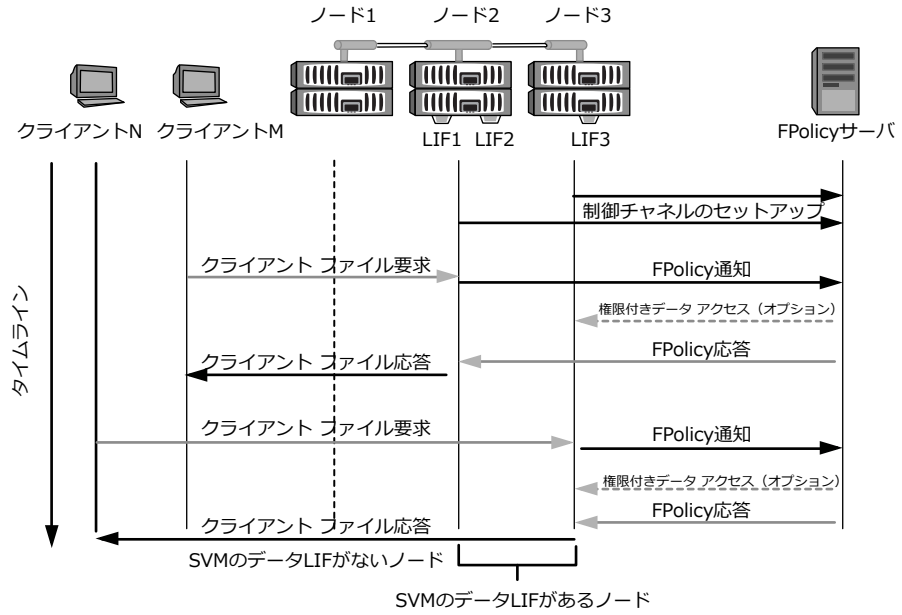
Storage Virtual Machine（SVM）に属しているすべてのノードは、TCP/IPを使用して外部FPolicyサーバへの接続を開始します。FPolicyサーバへの接続のセットアップには、ノードのデータLIFを使

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 ジャンクションがファイル アクセスに与える影響（11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（15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（189ページ）
FPolicyの設定の作成（197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キングを行います。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 ブロッキングを使用すると、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 ブロッキングでもサポートされます。
- ネイティブ ファイル ブロッキングと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 ブロッキ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 ブロッキング機能では、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 ブロッキングは、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 ブロッキング、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、滅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。

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

FPolicyポリシーの設定の計画（189ページ）
FPolicyの設定の作成（197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（177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（168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（168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（169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（177ページ）

関連タスク

FPolicyポリシーの有効化と無効化（203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ると、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もありません。

関連コンセプト

FPolicy構成の計画（177ページ）
FPolicyの設定の作成（197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（176ページ）
FPolicyの設定の作成（197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
SVM この外部エンジンに関連付けるSVMの名前を指定します。 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。	`-vserver` *vserver_name*
エンジンの名前 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。 **注:** 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。 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。 • **a～z** • **A～Z** • **0～9** • 「_」、「-」、および「.」	`-engine-name` *engine_name*
プライマリFPolicyサーバ 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。 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。 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。	`-primary-servers` *IP_address*,...
ポート番号 FPolicyサービスのポート番号を指定します。	`-port` *integer*
セカンダリFPolicyサーバ 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。 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。	`-secondary-servers` *IP_address*,...

情報の種類	オプション
外部エンジンのタイプ 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。 **synchronous**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。 **asynchronous**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。	`-extern-engine-type` *`external_engine_type`* このパラメータには、次のいずれかの値を指定できます。 • **`synchronous`** • **`asynchronous`**
FPolicyサーバとの通信のためのSSLオプション 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。 • **`no-auth`**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。 • **`server-auth`**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。 • **`mutual-auth`**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。 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。	`-ssl-option` {**`no-auth`**|**`server-auth`**|**`mutual-auth`**}
証明書のFQDNまたはカスタム共通名 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。 **`mutual-auth`**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。	`-certificate-common-name` *`text`*
証明書のシリアル番号 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。 **`mutual-auth`**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。	`-certificate-serial` *`text`*
認証局 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。 **`mutual-auth`**を`-ssl-option`パラメータに指定した場合は、`-certifcate-ca`パラメータの値も指定する必要があります。	`-certifcate-ca` *`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
タイムアウトによる要求のキャンセル 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。 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。 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]
タイムアウトによる要求の破棄 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。 指定できる値の範囲は、**0**～**200**です。	`-reqs-abort-timeout` *integer*[h|m|s]
ステータス要求の送信間隔 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。 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]
FPolicyサーバの未処理要求の最大数 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。 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*
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。 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。 指定できる値の範囲は、**1**～**100**です。デフォルトは**60s**です。	`-server-progress-timeout` *integer*[h|m|s]

情報の種類	オプション
FPolicyサーバへのキープアライブ メッセージの送信間隔 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。 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。 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。	`-keep-alive-interval-`*`integer`*[h|m|s]
再接続の最大試行回数 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。 指定できる値の範囲は、**0**～**20**です。デフォルトは**5**回です。	`-max-connection-retries` *`integer`*
受信バッファ サイズ 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。 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。 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。	`-recv-buffer-size` *`integer`*
送信バッファ サイズ 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。 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。 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。	`-send-buffer-size` *`integer`*
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 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。 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。 デフォルト値は10秒に設定されています。	`-session-timeout` [*`integer`*h] [*`integer`*m] [*`integer`*s]

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。

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 デスティネ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ることで作成できます。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。

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	×		
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	×		

情報の種類	必須	含める	値
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
SVM このFPolicyイベントに関連付けるSVMの名前を指定します。 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。	`-vserver` *vserver_name*
イベント名 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。 この名前に指定できる文字数は最大256文字です。 **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。 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。 • **a～z** • **A～Z** • **0～9** • 「_」、「-」、および「.」	`-event-name` *event_name*
プロトコル 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。 • **cifs** • **nfsv3** • **nfsv4** **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。	`-protocol` *protocol*

情報の種類	オプション
ファイル処理 FPolicyイベントのファイル処理のリストを指定します。 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。 • **`close`**：ファイル クローズ処理 • **`create`**：ファイル作成処理 • **`create-dir`**：ディレクトリ作成処理 • **`delete`**：ファイル削除処理 • **`delete_dir`**：ディレクトリ削除処理 • **`getattr`**：属性取得処理 • **`link`**：リンク処理 • **`lookup`**：検索処理 • **`open`**：ファイル オープン処理 • **`read`**：ファイル読み取り処理 • **`write`**：ファイル書き込み処理 • **`rename`**：ファイル名変更処理 • **`rename_dir`**：ディレクトリ名変更処理 • **`setattr`**：属性設定処理 • **`symlink`**：シンボリック リンク処理 **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。	`-file-operations` *`file_operations`*,...

情報の種類	オプション
フィルタ 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。 • **`monitor-ads`**：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。 • **`close-with-modification`**：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。 • **`close-without-modification`**：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。 • **`first-read`**：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。 • **`first-write`**：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。 • **`offline-bit`**：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。 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。 • **`open-with-delete-intent`**：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。 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。 • **`open-with-write-intent`**：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。 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。 • **`write-with-size-change`**：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。 **注:** `-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。	`-filters` *`filter`*, ...
ボリューム処理が必要かどうか 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。	`-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	○	○	
イベント名	○	○	
プロトコル	×		
ファイル処理	×		
フィルタ	×		
ボリューム処理が必要かどうか	×		

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
SVM名 FPolicyスコープを作成するSVMの名前を指定します。	`-vserver` *`vserver_name`*	○	なし
ポリシー名 FPolicyポリシーの名前を指定します。 この名前に指定できる文字数は最大256文字です。 **注:** 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。 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。 • **a～z** • **A～Z** • **0～9** • 「_」、「-」、および「.」	`-policy-name` *`policy_name`*	○	なし
イベント名 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。 • 1つのポリシーに複数のイベントを関連付けることができます。 • イベントはプロトコルに固有です。 • 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。 • 既存のイベントを指定する必要があります。	`-events` *`event_name`*, ...	○	なし

情報の種類	オプション	必須	デフォルト値
外部エンジン名 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。 • 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。 • 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。 • 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、**native**を指定します。 • 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。	`-engine` *`engine_name`*	○（ポリシーで内部のData ONTAP標準エンジンを使用しない場合）	**native**
スクリーニングを必須にするかどうか 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。 • 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。 • **true**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。 • **false**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。	`-is-mandatory` {**true**|**false**}	×	**true**

情報の種類	オプション	必須	デフォルト値
権限付きアクセスを許可するかどうか 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。 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。 権限付きデータ アクセスの場合は、クラスタで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。 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。	`-allow-privileged-access` {**yes**|**no**}	×（パススルー リードが有効になっていない場合）	**no**
権限があるユーザの名前 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。 • このパラメータの値は、「domain\user name」の形式で指定します。 • `-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。	`-privileged-user-name` *user_name*	×（権限付きアクセスが有効になっていない場合）	なし

情報の種類	オプション	必須	デフォルト値
パススルー リードを許可する 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。 • 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。 • 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 リード専用に開か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。 • 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。	`-is-passthrough-read-enabled {true|false}`	×	**false**

関連コンセプト

FPolicyによるポリシーの処理方法（169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（174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ので、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。

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	○	
ポリシー名	○	
イベント名	○	
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、「?」 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
SVM FPolicyスコープを作成するSVMの名前を指定します。 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。	`-vserver` *`vserver_name`*
ポリシー名 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` *`policy_name`*
共有を含める 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` *`share_name`*, ...
共有を除外する 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` *`share_name`*, ...

情報の種類	オプション
ボリュームを含める 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` *volume_name*, ...
ボリュームを除外する 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` *volume_name*, ...
エクスポート ポリシーを含める 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` *export_policy_name*, ...
エクスポート ポリシーを除外する 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` *export_policy_name*, ...
ファイル拡張子を含める 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` *file_extensions*, ...
ファイル拡張子を除外する 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` *file_extensions*, ...
ディレクトリのファイル拡張子の監視を有効にする 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。 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**|}

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	×		

情報の種類	必須	含める	値
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（198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（199ページ）
   FPolicyポリシーの設定を作成する手順の一環して、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（199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（201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（201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（176ページ）
FPolicy構成の計画（177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（174ページ）
FPolicyの設定に関する情報の表示（203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
   ```

   ```
                               Primary        Secondary          External
   Vserver           Engine    Servers        Servers       Port Engine Type
   ---------------   --------- -------------- ----------- ------ -----------
   vs1.example.com   engine1   10.1.1.2,      -             6789 synchronous
                               10.1.1.3
   ```

   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`

```
                  Event               File                      Is Volume
Vserver           Name      Protocols Operations    Filters     Operation
---------------   --------- --------- ------------- --------- ------------
vs1.example.com   event1    cifs      open, close,  -         false
                                      read, write
```

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 *domainuser_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     Events    Engine    Is Mandatory  Privileged
                 Name                                         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り（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り（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。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
   ```

   ```
                                    Sequence
   Vserver          Policy Name        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（197ページ）
FPolicyサーバの接続の管理（206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	`vserver fpolicy policy external-engine modify`
イベント	`vserver fpolicy policy event modify`
スコープ	`vserver fpolicy policy scope modify`
ポリシー	`vserver fpolicy policy modify`

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（204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

1. 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	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
FPolicyポリシーを無効にする	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

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（204ページ）
有効なFPolicyポリシーに関する情報の表示（205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（197ページ）
FPolicyの設定の変更（202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と、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
ポリシー	vserver fpolicy policy 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。

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	**vserver fpolicy show**
指定したステータスのポリシー	**vserver fpolicy show -status {on|off}**
指定したSVMのポリシー	**vserver fpolicy show -vserver *vserver_name***
指定したポリシー名のポリシー	**vserver fpolicy show -policy-name *policy_name***
指定した外部エンジンを使用するポリシー	**vserver fpolicy show -engine *engine_name***

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
                                          Sequence
Vserver             Policy Name             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、使用するように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	`vserver fpolicy show-enabled`
指定したSVMのポリシー	`vserver fpolicy show-enabled -vserver` ***`vserver_name`***
指定したポリシー名のポリシー	`vserver fpolicy show-enabled -policy-name` ***`policy_name`***
指定したシーケンス番号のポリシー	`vserver fpolicy show-enabled -priority` ***`integer`***

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（166ページ）
同期通知および非同期通知とは（166ページ）
FPolicyと外部FPolicyサーバとの連携（168ページ）
ノードと外部FPolicyサーバの間の通信プロセス（169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	**vserver fpolicy show-engine -server *IP_address***
指定したSVMのもの	**vserver fpolicy show-engine -vserver *vserver_name***
指定したポリシーに関連付けられているもの	**vserver fpolicy show-engine -policy-name *policy_name***
指定したサーバ ステータスのもの	**vserver fpolicy show-engine -server-status *status*** 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。 • **connected** • **disconnected** • **connecting** • **disconnecting**
指定したタイプのもの	**vserver fpolicy show-engine -server-type *type*** 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。 • **primary** • **secondary**
指定の理由によって切断されたもの	**vserver fpolicy show-engine -disconnect-reason *text*** 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。 • **Disconnect command received from CLI.** • **Error encountered while parsing notification response from FPolicy server.** • **FPolicy Handshake failed.** • **SSL handshake failed.** • **TCP Connection to FPolicy server failed.** • **The screen response message received from the FPolicy server is not valid.**

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                                          Server-       Server-
Vserver         Policy    Node         Server    status        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
```

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

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。

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	**vserver fpolicy show-passthrough-read-connection**
指定したSVMのFPolicyパススルー リード接続ステータス	**vserver fpolicy show-passthrough-read-connection -vserver *vserver_name***
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	**vserver fpolicy show-passthrough-read-connection -policy-name *policy_name***
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	**vserver fpolicy show-passthrough-read-connection -policy-name *policy_name* -instance**

表示する接続ステータス情報	入力するコマンド
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	**vserver fpolicy show-passthrough-read-connection -policy-name *policy_name* -server-status *status*** 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。 • **connected** • **disconnected**

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
                                              FPolicy           Server
Vserver          Policy Name   Node          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
```

用語集

このマニュアルに記載されている、ファイル アクセスやプロトコル管理の概念を理解するため、特定の用語の使用方法を理解する必要があります。

A

ACE

Access Control Entry（アクセス制御エントリ）の略。

ACL

Access Control List（アクセス制御リスト）の略。

AD

Active Directoryの略。

adapter（アダプタ）

拡張スロットに差し込むSCSIカード、ネットワーク カード、ホットスワップ アダプタ、シリアル アダプタ、またはVGAアダプタ。*拡張カード*と呼ぶこともあります。

address resolution（アドレス解決）

LANまたはWANの宛先に対応するアドレスを判定する手順。

管理SVM

以前の名称はVserverです。clustered Data ONTAPで、他のSVMが所有するオブジェクトも含め、クラスタ内のすべてのオブジェクトへの全般的な管理アクセス権を持つが、クライアントまたはホストへのデータ アクセスは提供しないStorage Virtual Machine（SVM）。

administrator（管理者）

Data ONTAPシステムシステムの管理に必要な権限を持つアカウント。

agent（エージェント）

ステータスおよび診断情報を収集し、ネットワーク管理ステーションに転送するプロセス。*SNMPエージェント*など。

aggregate（アグリゲート）

アグリゲートに関連付けられているボリュームにストレージを提供する、物理ストレージ リソース（ディスクまたはアレイLUN）をグループ化したもの。アグリゲートは、関連付けられているすべてのボリュームにRAID構成を制御する機能を提供します。

API

*「Application Program Interface（API;アプリケーション プログラム インターフェイス）」*を参照してください。

appliance（アプライアンス）

単一の明確に定義された機能を実行し、導入および運用が容易な装置。

Application Program Interface（API;アプリケーション プログラム インターフェイス）

アプリケーション プログラムが、オペレーティング システムまたはその他のシステム、制御プログラム、通信プロトコルとの通信に使用する言語およびメッセージ形式。

ASCII

American Standard Code for Information Interchange（情報交換用米国標準コード）の略。

ATM

Asynchronous Transfer Mode（非同期転送モード）の略。セルスイッチング機能と多重化機能を組み合わせることで、信頼性の高い効率的なネットワーク サービスを提供する

ネットワーク技術。ATMは、ワークステーションやルータなどのデバイスとネットワークとの間のインターフェイスを提供します。

authentication（認証）

セキュリティで保護されたシステムまたはネットワークにログインするユーザのIDを検証するプロセス。

authorization（許可）

システム リソースの使用を許可されたユーザ、プログラム、プロセス、またはほかのシステムに制限すること。アクセス制御などによって、要求元にサービスの受け取りや処理の実行を許可するかどうかを判断するプロセス。

AutoSupport

ストレージ システムに潜在的な問題がある場合に、お客様のサイトからテクニカル サポートまたはその他の指定した宛先にEメール メッセージを送信するストレージ システム デーモン。

B

big-endian（ビッグエンディアン）

最上位バイトから処理される、ストレージおよび伝送用のバイナリ データ形式。

bind（バインド）

あるプロトコルまたはアプリケーションと別のプロトコルまたはアプリケーション間のソフトウェア接続を確立するプロセス。内部経路を作成します。

C

cache（キャッシュ）

（動詞）素早くアクセスできるようにデータを一時的に格納すること。（名詞）一時的にデータが格納される場所。ディスク キャッシュ、メモリ キャッシュ、Webキャッシュなどの種類があります。

CIFS

*「Common Internet File System（CIFS）」*を参照してください。

CIFS share（CIFS共有）

- Data ONTAPにおいて、ネットワーク ユーザが使用できるように設定されたディレクトリまたはディレクトリ構造。CIFSクライアントのドライブ レターにマッピングできます。単に*共有*と呼ぶこともあります。
- OnCommand Insight（旧SANscreenスイート）において、NASデバイスから公開されるサービス。CIFSプロトコルでファイルベースのストレージを提供します。CIFSは主にMicrosoft Windowsクライアントを対象としていますが、その他のさまざまなオペレーティング システムもCIFS共有にアクセスできます。

CLI

command-line interface（コマンドライン インターフェイス）の略。ストレージ システム プロンプトは、コマンドライン インターフェイスの一例です。

client（クライアント）

クライアント / サーバ アーキテクチャのワークステーションまたはPC。サービスを要求し、別のコンピュータ システムまたはプロセスの応答を受け入れるコンピュータ システムまたはプロセスです。

cluster（クラスタ）

- clustered Data ONTAP 8.xでは、ネームスペースを共有し、1つまたは複数の仮想サーバとして管理できる接続されたノード（ストレージ システム）のグループを指します。これにより、パフォーマンス、信頼性、拡張性が向上します。

- Data ONTAP 7.1リリース ファミリーおよび以前のリリースでは、2つのシステム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設定されたストレージ システム（別名*ノード*）のペアのことです。
- Data ONTAP 7.3および7.2リリース ファミリーでは、*アクティブ / アクティブ構成*といいます。
- ストレージ アレイ ベンダーによっては、ホスト アダプタとポートが存在するハードウェア コンポーネントを*クラスタ*と呼んでいます。同様のコンポーネントを*コントローラ*と呼ぶストレージ アレイ ベンダーもあります。

cluster monitor（クラスタ モニタ）

クラスタ内のノードの関係を管理するソフトウェア。

cluster SVM（クラスタSVM）

データSVMの旧称。「data SVM（データSVM）」を参照してください。

Common Internet File System（CIFS）

Microsoftのファイル共有ネットワーク プロトコル。Server Message Block（SMB;サーバ メッセージ ブロック）から発展したものです。

community（コミュニティ）

SNMPエージェントおよび1つ以上のSNMPマネージャ間の論理的な関係。コミュニティは名前によって識別され、コミュニティの全メンバーは、同じアクセス権を持ちます。

console（コンソール）

ストレージ システムの監視と制御に使用される物理端末または仮想端末。

Copy-On-Write（COW）

過度のディスク スペースを消費せずにSnapshotコピーを作成する手法。

D

Data ONTAP

ネットアップのオペレーティング システム ソフトウェア製品。特許取得済みのファイルシステム テクノロジとネットワーク データ アクセス専用のマイクロカーネル設計を組み合わせることによってファイルサービスを最適化します。

data SVM（データSVM）

以前の名称はデータVserverです。clustered Data ONTAPでは、クラスタからデータ アクセスを提供するStorage Virtual Machine（SVM）を指します。クラスタのハードウェアとストレージ リソースは、クラスタ内のデータSVMによって動的に共有されます。

degraded mode（デグレード モード）

RAIDグループで1本のディスクに障害が発生した場合、またはNVRAMカードのバッテリ残量が少ない場合に使用される、ストレージ システムの動作モード。

disk ID number（ディスクID番号）

ストレージ システムが、起動時にディスクを確認する際に各ディスクに割り当てる番号。

disk shelf（ディスク シェルフ）

ディスク ドライブを搭載し、ストレージ システムに接続されるシェルフ。

DNS

*「Domain Name System（DNS;ドメイン ネーム システム）」*を参照してください。

Domain Name System（DNS;ドメイン ネーム システム）

IPネットワーク上のコンピュータを見つけるためのインターネット サービス。

E

Ethernet adapter（イーサネット アダプタ）

イーサネット インターフェイス カード。

expansion card（拡張カード）

ストレージ システムの拡張スロットに挿入するSCSIカード、NVRAMカード、ネットワーク カード、ホットスワップ カード、またはコンソール カード。*アダプタ*と呼ぶこともあります。

expansion slot（拡張スロット）

拡張カードを挿入するストレージ システム ボード上のスロット。

export（エクスポート）

NFSクライアントがストレージ システムのどの領域を使用できるようにするかを定義するための、NFSのメカニズム。

F

failover（フェイルオーバー）

ネットワーク コンポーネントに物理的な障害が発生した場合に、サービスが中断しないようにデータを代替パスにただちに再ルーティングするプロセス。クラスタリング、およびストレージへのマルチパスに適用されます。クラスタリングの場合、Exchangeサービスなどのサービスがスタンバイ サーバに移動します。ストレージへの複数パスの場合、パスに障害が発生すると、ストレージへの別の物理接続にデータが再ルーティングされます。

file lock（ファイル ロック）

クライアントによって開かれているときのファイルの暗黙的状態。オープン モードに応じて、ファイルをロックして他のすべてのアクセスを防止するか、特定のタイプの共有アクセスを許可することができます。

file server（ファイルサーバ）

複数のユーザにファイル処理とストレージ機能を提供するコンピュータ。

FlexVol

clustered Data ONTAPの論理エンティティで、「FlexVolを備えたSVM」と呼ばれるStorage Virtual Machine（SVM、旧Vserver）に格納される。FlexVolは通常、ユーザ データを保持しますが、ノードまたはSVMのルート ボリュームおよびメタデータ コンテナとしても機能します。FlexVolは、ストレージを単一のアグリゲートから取得します。

FQDN

*「Fully Qualified Domain Name（FQDN;完全修飾ドメイン名）」*を参照してください。

FSID

file system ID（ファイルシステムID）の略。

FTP

File Transfer Protocol（ファイル転送プロトコル）の略。

Fully Qualified Domain Name（FQDN;完全修飾ドメイン名）

インターネット上の特定のコンピュータの完全名。コンピュータのホスト名とそのドメイン名で構成されています。

G

GID

*「Group ID（GID;グループID）」*を参照してください。

Group ID（GID;グループID）

UNIXシステムがグループの識別に使用する番号。

GUI

graphical user interface（グラフィカル ユーザ インターフェイス）の略。

GUID

globally unique identifier（グローバルー意識別子）の略。

H

heartbeat（ハートビート）

アクティブ / アクティブ構成において、一方のストレージ システムから他方のストレージ システムに対して繰り返し送信される信号。ストレージ システムが動作中であることを示します。ハートビート情報はディスク上にも格納されます。

hot spare disk（ホット スペア ディスク）

障害の発生したディスクの代わりに使用できる、ストレージ システムに搭載されているディスク。ディスク障害が発生するまでは、ホット スペア ディスクはRAIDディスク アレイには含まれません。

hot swap（ホット スワップ）

ストレージ システムの実行中にディスクの追加、取り外し、交換を行うプロセス。

hot swap adapter（ホット スワップ アダプタ）

ファイルシステム アクティビティへの影響を最小限に抑えて、ハード ディスクを追加または取り外しできるようにする拡張カード。

HTTP

HyperText Transfer Protocolの略。

I

I/O

入出力。

Infinite Volume

clustered Data ONTAPの論理エンティティで、「Infinite Volumeを備えたSVM」と呼ばれるStorage Virtual Machine（SVM、旧Vserver）に格納される。Infinite Volumeは、ストレージを複数のアグリゲートから取得します。

inode

ストレージ システム上およびUNIXファイルシステム内のファイルに関する情報を含むデータ構造。

interrupt switch（割り込みスイッチ）

一部のストレージ システムの前面パネルに装備されているスイッチ。デバッグに使用します。

K

KDC

Kerberos Key Distribution Center（Kerberosキー配布センター）の略。

L

LAN

local area network（ローカル エリア ネットワーク）の略。

LAN Emulation（LANE;LANエミュレーション）

ATMを基幹ネットワークトポロジとして使用してエミュレートLANを作成するアーキテクチャ、プロトコル、およびサービス。LANEを使用すると、ATMに接続されたエンド システムが、他のLANベースのシステムと通信できます。

LDAP

Lightweight Directory Access Protocolの略。

Lightweight Directory Access Protocol（LDAP）

ディレクトリ サービスにアクセスするためのクライアント / サーバ プロトコル。

local storage system（ローカル ストレージ システム）

ユーザがログインしているストレージ システム。

M

magic directory（マジック ディレクトリ）

名前によってアクセスできるが、ディレクトリの一覧には表示されないディレクトリ。マウント ポイントまたは共有のルートにあるものを除き、.snapshotディレクトリはマジック ディレクトリです。

mail host（メール ホスト）

特定のストレージ システム イベントが発生した場合に、自動的にEメールをテクニカル サポートに送信するクライアント ホスト。

Maintenance mode（保守モード）

システム ブート ディスクからストレージ システムをブートするときに利用できるオプション モードの1つ。保守モードでは、ハードウェアと設定のトラブルシューティング用の特別なコマンドを使用できます。

MIB

Management Information Base（管理情報データベース）の略。SNMPエージェントがネットワーク管理ステーションに送信する情報が記載されたASCIIファイル。

MIME

Multipurpose Internet Mail Extensionsの略。インターネット メッセージ本体のフォーマットを指定および記述するためのメカニズムを定義する仕様。MIMEコンテンツタイプ ヘッダーを含むHTTPレスポンスを受信した場合、HTTPクライアントは受信したデータに適したアプリケーションを起動できます。

N

name server（ネーム サーバ）

ディレクトリ サービスを提供するネットワーク サーバ。

namespace（ネームスペース）

Network-Attached Storage（NAS;ネットワーク接続型ストレージ）環境において、ファイルとファイルへのパス名の集合。

NAS

network-attached storage（ネットワーク接続型ストレージ）の略。

NDMP

Network Data Management Protocol（ネットワークデータ管理プロトコル）の略。ストレージ システムがバックアップ アプリケーションと通信できるようにし、複数のテープ バックアップ デバイスの自動制御機能を提供するプロトコル。

network adapter（ネットワーク アダプタ）

イーサネット、FDDI、またはATMカード。

network management station（ネットワーク管理ステーション）

*「NMS」*を参照してください。

NFS

Network File System（ネットワーク ファイルシステム）の略。

NMS

Network Management Station（ネットワーク管理ステーション）の略。サードパーティのネットワーク管理アプリケーション（SNMPマネージャ）を使用してストレージ システムに関するステータスおよび診断情報を処理するネットワーク上のホスト。

NTFS

New Technology File Systemの略。

NTP

Network Time Protocol（ネットワーク タイム プロトコル）の略。

null user（nullユーザ）

アプリケーションがリモート データにアクセスするために使用するWindows NTマシン アカウント。

NVRAM cache（NVRAMキャッシュ）

ストレージ システム上の不揮発性ランダム アクセス メモリ。受信する書き込みデータおよびNFS要求のロギングに使用されます。NVRAMキャッシュはシステム パフォーマンスを向上させ、ストレージ システムの障害または電源障害が発生した場合のデータ損失を防ぎます。

NVRAM card（NVRAMカード）

ストレージ システムのNVRAMキャッシュを搭載するアダプタ カード。

NVRAM mirror（VRAMミラー）

アクティブ / アクティブ構成において、ストレージ システムのNVRAM（不揮発性RAM）の内容が同期的に更新されたコピー。パートナー ストレージ システムによって維持されます。

P

panic（パニック）

Data ONTAPを実行しているシステムの動作停止を引き起こしている重大なエラー状況。Windowsシステム環境のソフトウェア クラッシュに似ています。

parity disk（パリティ ディスク）

RAID 4ディスクドライブ アレイのパリティ情報が格納されているディスク。RAID-DP保護機能を持つRAIDグループでは、2本のパリティ ディスクにパリティ情報およびダブル パリティ情報が格納されます。障害が発生したディスク ブロック内またはディスク上のデータの再構築に使用されます。

PCI

Peripheral Component Interconnectの略。より新しいストレージ システム モデルで使用されているバス アーキテクチャ。

POST

Power-on self-tests（電源投入時自己診断テスト）の略。電源投入時にストレージ システムによって実行されるテスト。

PVC

Permanent Virtual Circuit（相手固定接続）の略。ATMの接続モードの1つ。通常は手動セットアップによって事前に定義された静的ルートを持つリンク。

Q

qtree

仮想サブ ボリュームとして動作するボリュームのルートにある特別なサブディレクトリ。特殊な属性を備えています。

R

RAID

Redundant Array of Independent Disksの略。ストレージ アレイ内の全ディスクの内容に基づいてパリティ情報を算定することにより、ディスク障害から保護する手法。ストレージ システムでは、RAID4（すべてのパリティ情報を単一ディスクに格納）またはRAID-DP（すべてのパリティ情報を2本のディスクに格納）を使用します。

RAID disk scrubbing（RAIDディスク スクラビング）

システムがRAIDグループ内の各ディスクを読み取り、データを別のディスク領域に再書き込みすることでメディア エラーを修正しようとするプロセス。

S

SCSI adapter（SCSIアダプタ）

SCSIディスク ドライブおよびテープ ドライブをサポートする拡張カード。

SCSI address（SCSIアドレス）

ディスクのSCSIアダプタ番号およびSCSI IDから構成される、ディスクの完全なアドレス。たとえば9a.1などです。

SCSI ID

SCSIチェーン上のディスクドライブの番号（0～6）。

serial adapter（シリアル アダプタ）

一部のストレージ システム モデルにおいて、端末をコンソールとして接続するための拡張カード。

serial console（シリアル コンソール）

ストレージ システムのシリアル ポートに接続されるASCII端末またはANSI端末。ストレージ システムの動作を監視および管理するために使用されます。

share（共有）

ネットワーク ユーザが使用できるように設定され、CIFSクライアントのドライブ レターにマッピング可能なディレクトリまたはディレクトリ構造。*CIFS共有*と呼ばれることもあります。

SID

Windowsオペレーティング システムによって使用されるセキュリティ識別子。

Snapshot copy（Snapshotコピー）

ファイルシステム全体のオンラインの読み取り専用コピー。これによって、ファイルの内容を複製しないで、ユーザのミスによる削除や変更からファイルを保護できます。ユーザがファイルをリストアしたり、使用中のストレージ システムをテープにバックアップしたりできるようになります。

SNMP

Simple Network Management Protocol（簡易ネットワーク管理プロトコル）の略。

storage system（ストレージ システム）

ネイティブ ディスク シェルフ、ストレージ アレイ、またはその両方とデータを送受信する、Data ONTAPを実行しているハードウェア デバイス。ストレージ システムには、コントローラ コンポーネントと内部または外部のディスク ストレージ サブシステム コンポーネントが含まれます。ストレージ システム は、*ファイラー*、*アプライアンス*、*ストレージ アプライアンス*、Vシリーズ システムData ONTAPシステム、または*システム*と呼ばれることもあります。

Storage Virtual Machine（SVM）

clustered Data ONTAP 8.2.1より前の名称は*Vserver*。CLI画面およびvserverコマンド構文では引き続き「Vserver」を使用。一意のネットワーク アドレスでネットワーク アクセスを提供し、個別のネームスペースからデータを提供することができる仮想マシン。クラスタの残りのエンティティとは別に管理可能です。SVMには*管理*、*データ*、および*ノード*の3つの種類があります。特に明示する必要がないかぎり、「SVM」は通常データSVMを指します。

SVC

Switched Virtual Circuit（相手選択接続）の略。シグナリングによって確立される接続で、ユーザはコールの開始時にエンドポイントを定義します。

system board（システム ボード）

ストレージ システムのCPU、拡張バス スロット、およびシステム メモリを搭載したプリント回路基板。

T

takeover（テイクオーバー）

HAペアの一方のノードでシステム障害が発生してリブートできなくなった場合、パートナー ノードが、障害が発生したノードの機能を引き継ぎ、データを提供するプロセス。

TCP

Transmission Control Protocolの略。

TCP / IP

Transmission Control Protocol / Internet Protocolの略。

trap（トラップ）

ストレージ システムでイベントが発生したことを示すために、SNMPエージェントからSNMPマネージャにリクエストなしで送信される非同期メッセージ。

tree quota（ツリー クォータ）

quota qtreeコマンドによって作成されるディレクトリのディスク使用量を制限する、ディスク クォータの一種。指定されたユーザIDまたはグループIDのファイルによってディスク使用量を制限するユーザ クォータおよびグループ クォータとは異なります。

U

UDP

User Datagram Protocolの略。

UID

ユーザ識別番号の略。

Unicode

16ビットの文字セット標準。非営利協会であるUnicode Inc.によって制定および運営されています。

URI

universal resource identifierの略。

URL

uniform resource locatorの略。

UUID

Universal Unique Identifierの略。

V

VCI

Virtual Channel Identifier（仮想チャネル識別子）の略。ATMセル ヘッダーの16ビット フィールドによって定義される一意の数値タグ。セルが伝送される仮想チャネルを識別します。

VGA adapter（VGAアダプタ）

VGA端末をコンソールとして接続するための拡張カード。

VPI

Virtual Path Identifier（仮想パス識別子）の略。ATMセル ヘッダーの8ビット フィールドで、セルをルーティングする仮想パスを示します。

Vserver

clustered Data ONTAP 8.2.1以降の名称は「Storage Virtual Machine（SVM）」。一意のネットワーク アドレスでネットワーク アクセスを提供し、個別のネームスペースからデータ

を提供することができる仮想マシン。クラスタの残りのエンティティとは別に管理可能です。Vserverには *管理*、*ノード*、および *クラスタ*（「クラスタVserver」はData ONTAP 8.2以降では「データVserver」と呼ばれます）の3つの種類があります。特に明示する必要がないかぎり、「Vserver」は通常クラスタ / データVserverを指します。

W

WAFL

Write Anywhere File Layoutの略。書き込みパフォーマンスを最適化するように設計された、ストレージ システム用のファイルシステム。

WAN

wide area network（ワイド エリア ネットワーク）の略。

WINS

Windows Internet Name Serviceの略。

著作権に関する情報

商標に関する情報

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*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

記号

RPCSEC_GSS
Kerberosのサポート *53*
UTF-16
追加文字, Data ONTAPでのファイル名の処理方法 *25*

数字

8.3形式のファイル名
作成 *25*

A

ACE
NFSv4 ACLでの最大数 *122*
ACL
NFSv4, 管理の概要 *119*
NFSv4, 仕組み *120*
NFSv4, 有効化する利点 *120*
NFSv4でのACLの最大数 *122*
NFSv4の変更の有効化と無効化 *121*
NFSv4の有効化と無効化 *121*
AES
NFS Kerberosの設定 *56*
API
サポートされているVMware vStorage, NFS *128*

C

CA証明書
自己署名ルートのインストール, SVM上 *65*
CIFS
Data ONTAPによるNFSクライアントからのファイルアクセスの許可方法 *27*
ファイルの命名規則 *24*
CIFSサーバ
SSL/TLS経由のLDAPの有効化 *65*

D

Data ONTAP
監査プロセスの仕組み *136*
Data ONTAP CLI
NTFS監査ポリシーの設定方法 *156*
DES
NFS Kerberosの設定 *56*

E

EVTX
サポートされる監査イベント ログのファイル形式 *139*
ファイル形式, 監査イベント ログの表示 *139*

F

FlexVol
エクスポート ポリシーの関連付け *49*
セキュリティ形式の設定 *23*
FlexVolを備えたSVM
デフォルトのエクスポート ポリシー *34*
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 *173*
パススルー リードによるHSMのユーザビリティ向上方法 *172*
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 *175*
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 *187*
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 *188*
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 *188*
作成 *199*
設定の計画 *184*
設定用に収集する情報 *189*
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 *182*
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 *182*
SSL認証された接続の設定に関する追加情報 *181*
作成 *198*
設定の計画 *177*
設定用に収集する情報 *183*
FPolicy外部通信
ノードのフェイルオーバー時の実行方法 *170*
FPolicy構成
構成計画の概要 *177*
作成 *197*
情報の表示 *203*
情報を表示するコマンド *204*
情報を表示する際のshowコマンドの仕組み *204*
セットアップ手順 *176*
変更用コマンド *202*
要件、考慮事項、およびベストプラクティスに関する情報 *174*
FPolicyサーバ
FPolicy設定を作成するときに使用する外部の *172*
FPolicyと外部FPolicyサーバとの連携 *168*
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 *209*
外部からの切断 *207*
外部への接続 *206*
外部への接続に関する情報の表示 *207*
機能 *166*
ノードへの通信プロセス *169*
FPolicyサービス
SVMネームスペースにおける仕組み *171*

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 *193*
作成 *201*
収集する設定情報 *196*
設定の計画 *194*
FPolicy接続
外部FPolicyサーバへの接続時の管理責任 *168*
外部サーバ接続に関する情報の表示 *207*
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方法 *168*
権限付きデータ アクセス チャネルの使用方法 *168*
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 *169*
制御チャネルの使用方法 *168*
データLIFの移行とフェイルオーバーの処理方法 *170*
同期アプリケーションおよび非同期アプリケーション *167*
同期通知と非同期通知, 定義 *166*
ノードと外部FPolicyサーバの間の通信プロセス *169*
FPolicy通信
同期通知と非同期通知, 定義 *166*
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 *172*
定義 *171*
ネイティブFPolicyの設定を作成する場合 *172*
FPolicyのセットアップ
推奨事項 *175*
要件 *174*
FPolicyの通知
同期と非同期, 定義 *166*
FPolicyのベストプラクティス
セットアップ *175*
FPolicyフレームワーク
監視できるプロトコル *166*
機能 *166*
クラスタ コンポーネントの役割 *167*
定義 *166*
FPolicyポリシー
FPolicyによる複数の処理方法 *169*
作成 *199*
収集する設定情報 *194*
ステータスに関する情報の表示 *204*
設定の計画 *189*
標準のエンジンを使用する場合のFPolicyスコープの要件 *193*
有効化 *201*
有効化と無効化 *203*
有効な対象に関する情報の表示 *205*

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 *172*

I

Infinite Volume
NFSサポートに関する情報の参照先 *29*
NFSファイル アクセスのセットアップに関する情報の参照先 *87*
セキュリティ スタイルに関する情報の参照先 *22*
IPv6
NFSでの有効化 *86*
NFSのサポート *86*

K

Kerberos
Data ONTAPでのサポート *53*
NFS, インターフェイス設定の管理用 *105*
SVMのNFS設定の作成 *59*
NFSでのKerberos使用によるセキュリティ強化の概要 *53*
NFSでの使用に関する設定要件 *53*
NFSの暗号化タイプの設定 *56*
Realm設定の管理用コマンド *106*
Realm設定の作成 *58*

L

LDAP
新しいクライアント スキーマの作成 *65*
管理用コマンド *104*
クライアント スキーマ テンプレートの管理用コマンド *105*
クライアント設定の管理用コマンド *104*
クライアント設定の作成 *69*
使用するSVMの設定 *73*
ディレクトリ検索の設定オプション *67*
ネーム サービスとしての使用方法の概要 *63*
ネストされたグループ メンバーシップを使用するためのRFC2307bisサポートの有効化 *66*
ネットグループ検索パフォーマンスの向上 *70*
SVMでの有効化 *72*
LIF
FPolicyによるデータの移行とフェイルオーバーの処理方法 *170*
データ, FPolicyの実装での役割 *167*
ファイルアクセス管理の設定要件 *11*

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 *182*

N

NAS
一般的なネームスペース アーキテクチャ *12*
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 *16*
ジャンクション ポイントを指定したボリュームの作成 *15*

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 *17*
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 *18*
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 *15*
NFS
Data ONTAPによるクライアント認証の処理 *26*
Data ONTAPによる読み取り専用ビットの処理方法 *116*
Infinite Volumeサポート, 情報の参照先 *29*
Infinite Volumeのファイル アクセスのセットアップ, 情報の参照先 *87*
IPv6の有効化 *86*
Kerberos暗号化タイプの設定 *56*
Kerberosインターフェイス設定の管理用コマンド *105*
Kerberosでの使用に関する設定要件 *53*
Kerberosのサポート *53*
NFSv4 ACLを有効化する利点 *120*
NFSクレデンシャル キャッシュのTime-To-Liveを変更する理由 *108*
NTFSセキュリティ形式のデータにアクセスするプロセス *30*
Parallelのサポート *29*
TCPおよびUDP経由でのアクセスの制御 *91*
UNIXセキュリティ形式のデータへアクセスするプロセス *30*
v3の有効化と無効化 *88*
v4 ACLの管理の概要 *119*
v4 ACLの仕組み *120*
v4 ACLの有効化と無効化 *121*
v4, Data ONTAPサポートの制限 *28*
v4, ファイル委譲の管理 *122*
v4, ファイル委譲の仕組み *123*
v4, ファイル削除の判別 *121*
v4, ロック猶予期間の指定 *126*
v4, ロック リース期間の指定 *125*
v4.1のサポート *29*
v4.1の有効化と無効化 *89*
v4書き込みファイル委譲の有効化と無効化 *124*
v4のサポート *28*
v4の有効化と無効化 *88*
v4のユーザIDドメインの指定 *57*
v4ファイルおよびレコード ロックの説明 *125*
v4読み取りファイル委譲の有効化と無効化 *123*
Windowsクライアントのサポート *86*
監査設定 *156*
監査できるイベント *145*
キャッシュされたユーザ クレデンシャルのTime-To-Liveの設定 *109*
クライアント, Data ONTAPによるCIFSファイル アクセスの許可方法 *27*
クライアントによるエクスポートのリスト表示の有効化 *89*
サポート, IPv6経由 *86*
サポートされるバージョンとクライアント *27*
統計の表示 *127*
非予約ポートからの要求の制御 *91*
非予約ポートを使用するエクスポートのマウント *93*
ファイル アクセスの管理 *88*
ファイル アクセスのセットアップ *32*
ファイルの命名規則 *24*
不明なUNIXユーザによるNTFSボリュームまたはqtreeへのNFSアクセスの処理 *92*
プロトコル間のファイル ロックの説明 *115*
SVMのプロトコルの変更 *32*
ユーザの許可されるグループID数の設定 *132*
NFSv3
TCPでのパフォーマンスの向上 *130*
TCPの読み取り / 書き込みの最大サイズの変更 *131*
サービス ポートの変更 *95*
NFSv4
ACL, 変更の有効化と無効化 *121*
リファーラルの仕組み *126*
リファーラルの有効化と無効化 *127*
NFSエクスポート
ボリューム ジャンクションの使用方法 *12*
NFSクレデンシャル キャッシュ
仕組み *108*
設定の概要 *107*
NFSサーバ
管理 *97*
作成 *33*
NISドメイン
管理用コマンド *103*
設定の作成 *74*
No space left on deviceエラー:
トラブルシューティング方法 *165*
NTFS
Data ONTAP CLIを使用した監査ポリシーの設定方法 *156*
rootユーザ アクセスの制御 *133*
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 *144*
NTFSボリュームまたはqtree
不明なUNIXユーザによるアクセスの処理 *92*

P

Parallel NFS
有効化と無効化 *89*
pNFS
サポート *29*
有効化と無効化 *89*

Q

qtree
エクスポート *50*
エクスポート ポリシーがクライアント アクセスを制御する仕組み *34*
エクスポート ポリシーの削除 *51*
エクスポート ポリシーの割り当て *50*
セキュリティ形式の設定 *23*
ファイル処理のIDの検証 *51*

R

Realm設定
NFS Kerberosの管理用コマンド *106*
NFS Kerberosの作成 *58*

RFC2307bisのサポート
ネストされたグループ メンバーシップを使用するためのLDAPの有効化 *66*
rootユーザ
NTFSセキュリティ形式のデータへのアクセスの制御 *133*
rquota
有効化と無効化 *130*

S

showmount -eコマンド
NFSクライアントによるエクスポート リストの表示の有効化 *89*
showコマンド
FPolicyの設定を表示する際の仕組み *204*
SMB
Data ONTAPによる読み取り専用ビットの処理方法 *116*
監査できるイベント *140*
プロトコル間のファイル ロックの説明 *115*
SVMのプロトコルの変更 *32*
SMB共有
ボリューム ジャンクションの使用方法 *12*
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 *182*
SSL/TLS経由のLDAP
CIFSサーバでの有効化 *65*
Data ONTAPでのLDAP通信の保護方法の概要 *63*
SVMでの自己署名ルートCA証明書のインストール *65*
通信を保護するための設定および使用方法の概要 *63*
SSL証明書
FPolicy外部エンジン接続の設定に関する追加情報 *181*
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 *182*
SVM
FPolicyによるポリシーの処理方法 *169*
FPolicyの実装での役割 *167*
FPolicyポリシーの作成 *199*
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 *182*
LDAPの有効化 *72*
NASファイル アクセス イベントの監査の概要 *135*
NFS Kerberos設定の作成 *59*
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 *65*
監査を有効にしている場合のリバートのプロセス *164*
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 *164*
監査設定の削除 *163*
監査設定を変更するコマンド *163*
監査の有効化 *152*
監査の有効化と無効化 *161*
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 *165*
デフォルトのエクスポート ポリシー *34*
ネームスペースにおけるFPolicyサービスの仕組み *171*
ネットグループをロード *46*
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 *150*
ファイルとディレクトリの監査設定の作成 *150*
ファイルを監視および管理するためのFPolicyの使用 *166*
プロトコルの変更 *32*
ルート ボリュームでのセキュリティ形式の設定 *23*

T

TCP
NFSv3の読み取り / 書き込みの最大サイズの変更 *131*
NFSv3の読み取りおよび書き込みの最大サイズの変更 *130*
NFSアクセスの制御 *91*
Time-To-Live
NFSクレデンシャル キャッシュを変更する理由 *108*
キャッシュされたNFSユーザ クレデンシャルの設定 *109*
Twitter
マニュアルの変更に関する自動通知の受信方法 *223*

U

UDP
NFSアクセスの制御 *91*
UNIX
URIを使用したローカル グループのロード *78*
URIを使用したローカル ユーザのロード *76*
ローカル ユーザとローカル グループの設定 *75*
ローカルUNIXユーザおよびグループに対する制限の管理 *102*
ローカル グループの管理用コマンド *101*
ローカル グループの作成 *78*
ローカル グループへのユーザの追加 *76*
ローカル ユーザ、グループ、およびグループ メンバーに対する制限 *102*
ローカル ユーザの管理用コマンド *101*
ローカル ユーザの作成 *75*
UNIXアクセス権
Data ONTAPによる維持方法 *21*
Windowsの[セキュリティ]タブを使用した管理方法 *22*
UNIXユーザ
不明な場合のNTFSボリュームまたはqtreeへのアクセスの処理 *92*
URI
SVMへのネットグループのロード *46*
ローカルUNIXグループのロード *78*
ローカルUNIXユーザのロード *76*

V

VMware
NFSでサポートされているvStorage API *128*

vStorage over NFSの有効化と無効化 *129*
vStorage
NFSでサポートされているAPI *128*
over NFSの有効化と無効化 *129*

W

Windows
NFSクライアント, サポート *86*
Windowsの[セキュリティ]タブ
UNIXアクセス権の管理方法 *22*

X

XML
サポートされる監査イベント ログのファイル形式 *139*
ファイル形式, 監査イベント ログの表示 *139*

あ

アーキテクチャ
一般的なNASネームスペース *12*
アクセス
NTFSボリュームまたはqtreeに対する不明なUNIXユーザの処理 *92*
セキュリティ タイプによるクライアントのレベルの決定方法 *38*
アクセス キャッシュ
説明 *113*
タイムアウト値の仕組み *114*
パフォーマンスの最適化 *114*
アクセス制御リスト
次を参照 : ACL
アクセス要求
匿名へのマッピング *36*
アクセス レベル
セキュリティ タイプによるクライアントの決定方法 *38*
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 *138*
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 *175*
暗号化タイプ
NFS Kerberosの設定 *56*
アンマウント
NASネームスペースのボリューム *17*

い

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 *188*
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 *188*
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 *187*
FPolicyに関する情報を表示するコマンド *204*
FPolicyの作成 *199*
FPolicyの設定用に収集する情報 *189*
FPolicyのための設定の計画 *184*
FPolicyの変更用コマンド *202*
SMB, 監査できる *140*
ファイルおよびディレクトリの監査設定の作成 *150*
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 *140*
イベント ログ
監査でサポートされるファイル形式 *139*
監査の手動ローテーション *160*
監査の表示 *139*
イベント ログの形式
EVTXファイル形式のサポート *139*
XMLファイル形式のサポート *139*
インストール
SVM上の自己署名ルートCA証明書 *65*

え

エクスポート
NFSクライアントによるリストの表示の有効化 *89*
qtree *50*
クライアント アクセスのチェック *52*
クライアントのフェンシング *107*
クライアントのフェンシング解除 *107*
エクスポート ポリシー
Data ONTAPによるキャッシュの使用方法 *110*
FlexVolとの関連付け *49*
qtreeからの削除 *51*
qtreeへのクライアント アクセスを制御する仕組み *34*
qtreeへの割り当て *50*
管理 *106*
キャッシュのフラッシュ *111*
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 *52*
作成 *42*
制限とネストされたジャンクション *52*
デフォルト, SVM *34*
ボリュームへのクライアント アクセスを制御する仕組み *34*
ルールのインデックス番号の設定 *48*
ルールの追加 *43*
エクスポート ポリシー キャッシュ
管理の概要 *110*
エクスポート ポリシー ルール
結果を格納するアクセス キャッシュの仕組み *113*
エクスポート ルール
管理用コマンド *106*
機能 *35*
スーパーユーザ アクセスの設定方法 *40*
匿名アクセスの設定方法 *40*
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 *165*
エラー メッセージ
No space left on device *165*

お

大文字と小文字の区別
ファイル名 *24*
オプション
LDAPディレクトリ検索の設定 *67*
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 *173*

か

解除
ロック *118*
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 *63*
外部FPolicyサーバ
FPolicy設定を作成するときに使用する *172*
FPolicyと外部FPolicyサーバとの連携 *168*
接続 *206*
接続に関する情報の表示 *207*
切断 *207*
設定タイプの定義 *171*
次も参照 : 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 *204*
FPolicyの作成 *198*
FPolicyの設定用に収集する情報 *183*
FPolicyのための設定の計画 *177*
FPolicyの変更用コマンド *202*
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 *170*
書き込みファイル委譲
NFSv4の有効化と無効化 *124*
確認
ネットグループのクライアント メンバーシップ *112*
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 *158*
Data ONTAPのプロセスの仕組み *136*
NFSイベントの一覧 *145*
NFSとSMBのファイルおよびフォルダ アクセスの概要 *135*
NFS用の設定 *156*
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 *144*
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 *138*
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 *140*
イベント ログの統合 *136*
イベント ログのローテーション *136*
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 *164*
監査イベント ログの手動変換 *160*
監査イベント ログの表示 *139*
監査が有効なSVMがある場合のリバートのプロセス *164*
監査対象オブジェクトへの完全パスの決定 *142*
監査できるSMBイベント *140*
サポートされる監査イベント ログの形式 *139*
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 *143*
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 *135*
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 *165*
設定に関する情報の表示 *162*
設定に関する要件と考慮事項 *138*
設定の確認 *152*
設定の計画 *146*
設定の削除 *163*
設定を変更するコマンド *163*
ノードが利用できない場合のイベント ログの統合 *136*
ファイルおよびディレクトリ イベントの設定の作成 *150*
ファイルとディレクトリの作成, 設定 *150*
部分的なイベント ログの統合 *136*
SVMでの有効化 *152*
SVMでの有効化と無効化 *161*
有効化または無効化するときの処理 *136*
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 *138*
有効になっていることの確認 *162*
リバート前に監査が有効なSVMで実行する必要がある操作 *164*
リバート前に実行する必要がある操作 *164*
監査イベント ログ
手動ローテーション *160*
監査が有効なSVM
リバート前に実行する必要がある操作 *164*
監査の保証
Data ONTAPによる保証方法 *136*
監査ポリシー
Data ONTAP CLIを使用したNTFSに関する情報の表示 *158*
NTFS, Data ONTAP CLIを使用した設定方法 *156*
Windowsの[セキュリティ]タブを使用した設定 *153*
Windowsの[セキュリティ]タブを使用した表示 *157*
ファイルおよびフォルダの設定の概要 *152*
管理
LDAPクライアント スキーマ テンプレート, コマンド *105*
LDAPクライアント設定, コマンド *104*
LDAPの設定, コマンド *104*
NFS Kerberos Realm設定, コマンド *106*
NFSサーバ *97*
エクスポート ポリシー *106*
エクスポート ルール, コマンド *106*
ネーム サービス スイッチ エントリ *100*
ネーム マッピング, コマンド *100*
ローカルUNIXグループ, コマンド *101*
ローカルUNIXユーザ, コマンド *101*
ローカルUNIXユーザおよびグループの制限 *102*

き

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 *63*
キャッシュ
Data ONTAPでのエクスポート ポリシーの使用方法 *110*
NFSクレデンシャルのTime-To-Liveを変更する理由 *108*
NFSクレデンシャルの設定の概要 *107*
NFSユーザ クレデンシャルのTime-To-Liveの設定 *109*
エクスポート ポリシー ネットグループの表示 *112*
エクスポート ポリシーのフラッシュ *111*
キャッシュ, NFSクレデンシャル
仕組み *108*
キャッシュ, アクセス
説明 *113*
タイムアウト値の仕組み *114*
パフォーマンスの最適化 *114*
キュー
エクスポート ポリシー ネットグループの表示 *112*

く

クエリ設定オプション
LDAPディレクトリ検索 *67*
クライアント
ファイル処理のqtree IDの検証 *51*
クライアント アクセス
セキュリティ タイプによるレベルの決定方法 *38*
ドメインの検証によるネットグループのより厳密なチェックの実行 *93*
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 *165*
クライアント スキーマ
新しいLDAPの作成 *65*
クライアント スキーマ テンプレート
LDAPの管理用コマンド *105*
クライアント設定
LDAPの作成 *69*
クライアント認証
ONTAPによる処理 *26*
クラスタ
FPolicyの実装での役割 *167*
グループ
UNIX, ローカルの作成 *78*
ローカル, UNIX, 設定 *75*
ローカルUNIX, 制限 *102*
ローカルUNIX, 制限の管理 *102*
ローカルUNIXの管理用コマンド *101*
ローカルUNIXのロード, URL *78*
ローカルUNIXへのユーザの追加 *76*
グループID
NFSユーザの許可される数の設定 *132*
グループ情報
LDAPディレクトリ検索の設定オプション *67*
グループ メンバーシップ
ネストされた状態で使用するためのLDAPのRFC2307bisサポートの有効化 *66*
クレデンシャル キャッシュ
NFSの設定の概要 *107*
クレデンシャル キャッシュ, NFS
仕組み *108*

け

計画
FPolicyイベントの設定 *184*
FPolicy外部エンジンの設定 *177*
FPolicy構成の概要 *177*
FPolicyスコープの設定 *194*
FPolicyポリシーの設定 *189*
監査設定 *146*
権限
Data ONTAPによるUNIXの維持方法 *21*
UNIX, Windowsの[セキュリティ]タブを使用した管理方法 *22*
セキュリティ形式によるファイル権限に対する影響 *19*
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 *169*
検索
LDAPディレクトリの設定オプション *67*
検証
監査設定 *152*, *162*
ネットグループのステータス, コマンド *103*
ネットグループの定義の状態 *47*

こ

交換
ネーム マッピング, コマンド *100*
構成
Kerberos Realmの管理用コマンド *106*
LDAPクライアントの作成 *69*
NFS Kerberos Realmの作成 *58*
NISドメインの作成 *74*
監査の計画 *146*
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 *182*
構成オプション
LDAPディレクトリ検索 *67*
構成タイプ
FPolicy, 定義 *171*
考慮事項
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 *138*
監査設定 *138*
コピー
LDAPクライアント スキーマ テンプレート, コマンド *105*
エクスポート ポリシー *106*
コマンド
LDAPクライアント スキーマ テンプレートの管理 *105*
SVMの監査の変更 *163*
ネーム マッピングの管理用 *100*
ローカルUNIXユーザの管理用 *101*
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 *223*

さ

サーバ
CIFSでのSSL/TLS経由のLDAPの有効化 *65*
NFSの作成 *33*
サーバ実装ID
変更 *119*
サービス
Data ONTAPでの名前の使用方法 *26*
削除
LDAPクライアント スキーマ テンプレート, コマンド *105*
LDAPクライアント設定, コマンド *104*
LDAPの設定, コマンド *104*
NFS Kerberos Realm設定, コマンド *106*
NFSサーバ *97*
NISドメイン設定, コマンド *103*
qtreeのエクスポート ポリシー *51*
エクスポート ポリシー *106*
エクスポート ルール, コマンド *106*
監査設定 *163*
ネーム サービス スイッチ エントリ *100*
ネーム マッピング, コマンド *100*
ネットグループ, コマンド *103*
ローカルUNIXグループ, コマンド *101*
ローカルUNIXグループのユーザ, コマンド *101*
ローカルUNIXユーザ, コマンド *101*
作成
FPolicyイベント *199*
FPolicy外部エンジン *198*
FPolicy構成 *197*
FPolicyスコープ *201*
FPolicyポリシー *199*
LDAPクライアント設定 *69*
LDAPクライアント設定, コマンド *104*
LDAPの設定, コマンド *104*
NFS Kerberos Realm設定 *58*
NFS Kerberos Realm設定, コマンド *106*
NFSサーバ *33*
NISドメイン設定 *74*
NISドメイン設定, コマンド *103*
新しいLDAPクライアント スキーマ *65*
エクスポート ポリシー *42*
エクスポート ルール, コマンド *106*
ネーム サービス スイッチ エントリ *100*
ネームマッピング *84*
ファイルおよびディレクトリ イベントの監査設定 *150*
ファイルとディレクトリの監査設定 *150*
ファイル名 *25*
ローカルUNIXグループ *78*
ローカルUNIXグループ, コマンド *101*
ローカルUNIXユーザ *75*
ローカルUNIXユーザ, コマンド *101*
サポートされるプロトコル *10*
サロゲート ペア
Data ONTAPでのUTF-16を含むファイル名の処理方法 *25*

し

自己署名ルートCA証明書
SVMでのインストール *65*
ジャンクション
使用に関するルール *12*
定義 *11*, *12*
ボリューム, SMBおよびNFSネームスペースでの使用方法 *12*
ジャンクション ポイント
指定されていないボリュームの作成 *16*
指定したボリュームの作成 *15*
ボリューム, ネームスペースを作成するための使用方法 *11*
ボリュームに関する情報の表示 *18*
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 *140*
手動ローテーション
監査イベント ログ *160*
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 *223*
証明書
自己署名ルートのインストール, SVM上 *65*
処理
Data ONTAPの監査の仕組み *136*
シンボリック リンク
監査する際の考慮事項 *143*
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 *81*
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 *81*

す

推奨事項
FPolicyのセットアップ *175*
スーパーユーザ アクセス
エクスポート ルールによる設定方法 *40*
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 *169*
スキーマ
新しいLDAPクライアントの作成 *65*
スキーマ テンプレート
LDAPクライアントの管理用コマンド *105*
スコープ
FPolicyに関する情報を表示するコマンド *204*
FPolicyの作成 *201*
FPolicyのための設定の計画 *194*
FPolicyの変更用コマンド *202*
FPolicy用に収集する設定情報 *196*
ステージング ファイル
監査向けの定義 *135*
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 *165*
ステージング ボリューム
監査向けの定義 *135*
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 *138*
スペースに関する問題のトラブルシューティング方法 *165*
ストレージレベルのアクセス保護

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 *158*
ファイルおよびフォルダへのアクセスの保護方法 *94*
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 *165*

せ

制御チャネル
FPolicyでの使用方法 *168*
制限
NFSv4 ACLでのACEの *122*
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 *182*
NFSv4のData ONTAPサポート *28*
認証ベース *10*
ファイルベース *11*
セキュアなLDAP通信
CIFSサーバでのSSL/TLS経由のLDAPの有効化 *65*
セキュリティ
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 *94*
セキュリティ形式
FlexVolでの設定 *23*
qtreeでの設定 *23*
SVMルート ボリュームでの設定 *23*
継承の仕組み *21*
設定のタイミングと場所 *20*
選択方法 *21*
データ アクセスに対する影響の概要 *19*
ファイル権限に対する影響 *19*
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 *182*
セキュリティ タイプ
クライアント アクセス レベルの決定方法 *38*
リストにないものを使用するクライアントの処理方法 *36*
[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 *22*
接続
FPolicy外部エンジンのSSL認証を使用する際の追加情報 *181*
外部FPolicyサーバ *206*
接続クレデンシャル
FPolicy, 権限付きデータ アクセス チャネルでの使用方法 *168*
切断
外部FPolicyサーバから *207*
設定
FlexVolでのセキュリティ形式 *23*
FPolicy *197*
LDAPを使用するためのSVM *73*
NFSの監査 *156*
NFSユーザに対して許可されるグループID数 *132*
qtreeでのセキュリティ形式 *23*
SVMルート ボリュームでのセキュリティ形式 *23*
Windowsの[セキュリティ]タブを使用した監査ポリシー *153*
デフォルト ユーザ *85*
ネーム サービス スイッチ テーブル *62*
ファイルおよびディレクトリ イベントの監査 *150*
ローカルUNIXユーザおよびグループ *75*
設定要件
LIFファイル アクセス管理 *11*

そ

操作
ファイルのqtree IDの検証 *51*
挿入
ネーム マッピング, コマンド *100*
ソフト マウント
使用 *25*

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 *144*
タイムアウト値
アクセス キャッシュでの仕組み *114*
タイムアウト パラメータ
アクセス キャッシュのパフォーマンスの最適化 *114*

つ

追加
エクスポート ポリシーのルール *43*
ローカルUNIXグループへユーザを *76*
追加文字
Data ONTAPでのUTF-16を含むファイル名の処理方法 *25*

て

提案
マニュアルに関するフィードバックの送信方法 *223*
定義
FPolicy *166*
ネットグループの状態の確認 *47*
ディザスタ リカバリ
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 *182*
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 *182*
ディレクトリ イベント
監査設定の作成 *150*
ディレクトリ検索
LDAPの設定オプション *67*
データLIF
FPolicy通信での制御チャネルの使用方法 *168*
FPolicyによる移行とフェイルオーバーの処理方法 *170*
FPolicyの実装での役割 *167*
データ アクセス
セキュリティ形式による影響の概要 *19*

データ アクセス チャネル
FPolicyでの権限付きの使用方法 *168*
権限付きでのFPolicy接続クレデンシャルの使用方法 *168*
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 *144*
デフォルト ユーザ
設定 *85*
テンプレート
LDAPスキーマの管理用コマンド *105*

と

同期
FPolicyアプリケーション *167*
FPolicy通知, 定義 *166*
通信, 権限付きデータ アクセス チャネルの使用方法 *168*
統計
NFSの表示 *127*
統合タスク
監査向けの定義 *135*
匿名
クライアントのマッピング *36*
匿名アクセス
エクスポート ルールによる設定方法 *40*
ドメイン
NISの管理用コマンド *103*
検証によるネットグループのより厳密なアクセス チェックの実行 *93*
ドメイン設定
NISの作成 *74*
トラブルシューティング
エクスポートへのクライアント アクセス *52*
監査イベント ログ ボリュームのスペースに関する問題 *164*
ステージング ボリュームのスペースに関する問題 *165*
ネーム サービスに関する問題 *97*

な

名前
ファイルに使用できる文字 *24*
名前の変更
エクスポート ポリシー *106*

に

認証
Data ONTAPでのユーザのネーム サービスの使用方法 *26*
Data ONTAPによるNFSクライアントの処理 *26*
Kerberosによるセキュリティ, サポート *53*
SSLによるFPolicy外部エンジン接続を使用する際の追加情報 *181*
認証ベース
制限事項 *10*

ね

ネイティブFPolicyサーバ
設定タイプの定義 *171*
ネイティブFPolicyの設定
どのような場合に作成するか *172*
ネーム サービス
Data ONTAPでの使用方法 *26*, *60*
LDAPの使用方法の概要 *63*
LDAPを使用するためのSVMの設定 *73*
設定の概要 *60*
問題のトラブルシューティング *97*
ネーム サービス スイッチ
Data ONTAPでの使用方法 *60*
ネーム サービス スイッチ エントリ
管理用コマンド *100*
削除 *100*
作成 *100*
表示 *100*
変更 *100*
ネーム サービス スイッチ テーブル
設定 *62*
ネームスペース
SVMにおけるFPolicyサービスの仕組み *171*
NASアクセスでのボリューム ジャンクションの使用方法 *12*
NASでのデータ ボリュームの作成と管理の概要 *15*
NAS内のボリュームのマウントまたはアンマウント *17*
NASの一般的なアーキテクチャ *12*
定義 *11*
ネームマッピング
LDAPを使用するためのSVMの設定 *73*
UNIXユーザからWindowsユーザへのマルチドメイン検索 *81*
管理用コマンド *100*
作成 *84*
ネーム マッピング
仕組み *81*
使用方法 *80*
変換ルール *83*
ネストされたグループ メンバーシップ
使用するためのLDAPのRFC2307bisサポートの有効化 *66*
ネットグループ
URIからのロード, コマンド *103*
URIを使用したSVMへのロード *46*
エクスポート ポリシー キャッシュの表示 *112*
エクスポート ポリシー キューの表示 *112*
管理用コマンド *103*
クライアント メンバーシップの確認 *112*
削除, コマンド *103*
定義の状態の確認 *47*
ドメインの検証による厳密なクライアント アクセス チェックの実行 *93*
ノード間でのステータスの確認, コマンド *103*
表示, コマンド *103*
ネットグループ検索
パフォーマンスの向上 *70*
ネットグループ情報
LDAPディレクトリ検索の設定オプション *67*

の

ノード
FPolicy対応の通信プロセス *169*
フェイルオーバー時のFPolicyによる外部通信の実行方法 *170*

は

ハード マウント
使用 *25*
ハード リンク
監査する際の考慮事項 *143*
パス
監査対象オブジェクトでの決定 *142*
パススルー リード
FPolicy, HSMのユーザビリティ向上方法 *172*
FPolicy, アップグレードおよびリバートに関する考慮事項 *175*
FPolicy, 有効になっている場合の読み取り要求の処理方法 *173*
FPolicyの接続のステータスに関する情報の表示 *209*
FPolicyポリシーの作成 *199*
パフォーマンス
NFSv3 TCPでの向上 *130*
アクセス キャッシュの最適化 *114*
パラメータ, タイムアウト
アクセス キャッシュのパフォーマンスの最適化 *114*

ひ

ビット
Data ONTAPによる読み取り専用の処理方法 *116*
非同期
FPolicyアプリケーション *167*
FPolicy通知, 定義 *166*
表示
Data ONTAP CLIを使用したFlexVolのNTFS監査情報 *158*
FPolicy設定に関する情報 *203*
FPolicyの設定, showコマンドの仕組み *204*
FPolicyの設定情報, コマンド *204*
FPolicyパススルー リード接続のステータスに関する情報 *209*
FPolicyポリシーのステータスに関する情報 *204*
LDAPクライアント スキーマ テンプレート, コマンド *105*
LDAPクライアント設定, コマンド *104*
LDAPの設定, コマンド *104*
NFS Kerberos Realm設定, コマンド *106*
NFS Kerberosインターフェイス設定 *105*
NFSサーバ *97*
NFS統計 *127*
NISドメイン設定, コマンド *103*
NISドメイン設定のバインド ステータス, コマンド *103*
Windowsの[セキュリティ]タブを使用した監査ポリシーの情報 *157*
エクスポート ポリシー *106*
エクスポート ルール, コマンド *106*
外部FPolicyサーバへの接続に関する情報 *207*
監査イベント ログ *139*
監査設定に関する情報 *162*
ネーム サービス スイッチ エントリ *100*
ネーム マッピング, コマンド *100*
ネットグループ, コマンド *103*
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 *18*
有効なFPolicyポリシーに関する情報 *205*
ローカルUNIXグループ, コマンド *101*
ローカルUNIXユーザ コマンド *101*
ロックに関する情報 *116*
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 *193*

ふ

ファイル
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 *165*
ファイル アクセス
Data ONTAPによる制御方法 *10*
Infinite Volume, NFSのセットアップに関する情報の参照先 *87*
NFS, 管理 *88*
NFS用のセットアップ *32*
管理のためのLIF設定要件 *11*
ファイル アクセス イベント
監視するためのFPolicyの使用 *166*
ファイル委譲
NFSv4, 管理 *122*
NFSv4書き込みの有効化と無効化 *124*
NFSv4での仕組み *123*
NFSv4読み取りの有効化と無効化 *123*
ファイル イベント
監査設定の作成 *150*
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 *135*
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 *140*
ファイルおよびレコード ロック
NFSv4, 説明 *125*
ファイル監査ポリシー
設定の概要 *152*
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 *139*
ファイル権限
セキュリティ形式による影響 *19*
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 *188*
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 *188*
qtree IDの検証 *51*
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 *187*
ファイルとディレクトリの監査
SVMでの設定の作成 *150*
ファイルベース
制限事項 *11*
ファイル名
NFSとCIFSでの命名規則 *24*

大文字と小文字の区別 *24*
作成 *25*
使用できる文字 *24*
ファイル ロック
解除 *118*
管理の概要 *115*
情報の表示 *116*
プロトコル間, 説明 *115*
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 *223*
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 *188*
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 *188*
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 *187*
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 *170*
フェンシング
クライアントをエクスポートから *107*
フェンシング解除
クライアントをエクスポートから *107*
フォルダ監査ポリシー
設定の概要 *152*
フラッシュ
エクスポート ポリシー キャッシュ *111*
プロトコル
FPolicyで監視可能 *166*
サポート対象 *10*
ファイルのロック, 説明 *115*
SVMの変更 *32*

へ

ベストプラクティス
FPolicyのセットアップ *175*
変換タスク
監査向けの定義 *135*
変更
FPolicyの設定用コマンド *202*
LDAPクライアント スキーマ テンプレート, コマンド *105*
LDAPクライアント設定, コマンド *104*
LDAPの設定, コマンド *104*
NFS Kerberos Realm設定, コマンド *106*
NFS Kerberosインターフェイス設定 *105*
NFSv3 TCPの読み取り / 書き込みの最大サイズ *131*
NFSv3サービス ポート *95*
NFSv4 ACL, 機能の有効化と無効化 *121*
NFSサーバ *97*
NISドメイン設定, コマンド *103*
エクスポート ルール, コマンド *106*
エクスポート ルールのインデックス番号 *48*
監査設定, コマンド *163*
サーバ実装ID *119*
ネーム サービス スイッチ エントリ *100*
ネーム マッピング パターン, コマンド *100*
SVMのプロトコル *32*
ローカルUNIXグループ, コマンド *101*
ローカルUNIXユーザ, コマンド *101*

ほ

ポート
NFSv3サービスでの変更 *95*
非予約からのNFSマウント要求の制御 *91*
ポリシー
Data ONTAPによるエクスポートでのキャッシュの使用方法 *110*
FPolicy, 収集する設定情報 *194*
FPolicyに関する情報を表示するコマンド *204*
FPolicyによる複数のFPolicyの処理方法 *169*
FPolicyのための設定の計画 *189*
FPolicyの変更用コマンド *202*
FPolicyの有効化 *201*
FPolicyの有効化と無効化 *203*
FPolicyポリシーのステータスに関する情報の表示 *204*
エクスポートのキャッシュのフラッシュ *111*
エクスポートの削除, qtreeから *51*
エクスポートの作成 *42*
エクスポートのルールの追加 *43*
エクスポート ポリシーの割り当て, qtree *50*
ファイルおよびフォルダ監査設定の概要 *152*
有効なFPolicyに関する情報の表示 *205*
ポリシー ルール, エクスポート
結果を格納するアクセス キャッシュの仕組み *113*
ボリューム
FlexVolでのセキュリティ形式の設定 *23*
FlexVolへのエクスポート ポリシーの関連付け *49*
NASネームスペースでの作成と管理の概要 *15*
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 *17*
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 *158*
エクスポート ポリシーがクライアント アクセスを制御する仕組み *34*
ジャンクション ポイントを指定した作成 *15*
ジャンクション ポイントを指定しない作成 *16*
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 *11*
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 *138*
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 *165*
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 *94*
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 *18*
ボリューム ジャンクション
SMBおよびNFSネームスペースでの使用方法 *12*
使用に関するルール *12*
定義 *12*

ま

マウント
NASネームスペースのボリューム *17*
ハードの使用 *25*
非予約ポートを使用するNFSエクスポート *93*
マウント要求
NFSの制御, 非予約ポートから *91*

マニュアル
フィードバックの送信方法 223
変更に関する自動通知の受信方法 223

む

無効化
FPolicyポリシー 203
LIFでのNFS Kerberos 105
NFSv3 88
NFSv4 88
NFSv4.1 89
NFSv4リファーラル 127
Parallel NFS 89
pNFS 89
rquotaのサポート 130
vStorage over NFS 129
SVMでの監査 161

め

メンバーシップ
ネストされたグループを使用するためのLDAPのRFC2307bisサポートの有効化 66

ゆ

有効化
CIFSサーバでのSSL/TLS経由のLDAP 65
FPolicyポリシー 201, 203
SVMでのLDAP 72
LIFでのNFS Kerberos 105
NFSv3 88
NFSv4 88
NFSv4.1 89
NFSv4リファーラル 127
NFSでのIPv6 86
Parallel NFS 89
pNFS 89
rquotaのサポート 130
vStorage over NFS 129
SVMでの監査 152
SVMでの監査 161
ユーザ
UNIX, URIを使用したロード 76
UNIX, ローカルの作成 75
ローカル, UNIX, 設定 75
ローカルUNIX, 制限 102
ローカルUNIX, 制限の管理 102
ローカルUNIXグループへの追加 76
ローカルUNIXの管理用コマンド 101
ユーザIDドメイン
NFSv4の指定 57
ユーザ情報
LDAPディレクトリ検索の設定オプション 67
ユーザ認証
Data ONTAPでのネーム サービスの使用方法 26
ユーザ名
マッピングの仕組み 81
ユーザ名マッピング
マルチドメイン検索で使用される信頼できる優先ドメイン 81
優先度
FPolicyによるFPolicyポリシーの処理方法 169

よ

要件
FPolicyのセットアップ 174
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 193
NFSでKerberosを使用するための設定 53
監査設定 138
用語
SSL/TLS経由のLDAP 63
用語集
用語の定義 211
読み取り専用ビット
Data ONTAPによる処理方法 116
読み取りファイル委譲
NFSv4の有効化と無効化 123

り

リバート
FPolicyパススルー リード機能に関する考慮事項 175
監査を有効にしたSVMがある場合のプロセス 164
リファーラル
NFSv4での仕組み 126
NFSv4の有効化と無効化 127

る

ルートCA証明書
SVMでのインストール 65
ルート ボリューム
SVMでのセキュリティ形式の設定 23
ルール, エクスポート ポリシー
結果を格納するアクセス キャッシュの仕組み 113

ろ

ローカルUNIXグループ
管理用コマンド 101
作成 78
制限 102
制限の管理 102
ローカルUNIXユーザ
管理用コマンド 101
作成 75
制限 102
制限の管理 102
ローテーション
監査イベント ログ, 手動 160
ロード
URIからのネットグループ, コマンド 103
URIを使用したローカルUNIXグループのロード 78
URIを使用したローカルUNIXユーザのロード 76
ログ
監査ログの手動ローテーション 160

ログオンおよびログオフ イベント
SMB, 監査できる *140*
ロック
解除 *118*
情報の表示 *116*
ロック猶予期間
NFSv4, 指定 *126*
ロック リース期間
NFSv4の指定 *125*

わ

ワークシート
FPolicyイベントの設定に必要な情報の記録 *189*
FPolicy外部エンジンの設定に必要な情報の記録 *183*
FPolicyスコープの設定に必要な情報の記録 *196*
FPolicyポリシーの設定に必要な情報の記録 *194*
割り当て
qtreeへのエクスポート ポリシー *50*