NASストレージの管理
ONTAP 9

NetApp
December 20, 2024

目次

NASストレージの管理

System Managerを使用したNASプロトコルの管理

System ManagerによるNAS管理の概要

このセクションのトピックでは、ONTAP 9 .7以降のリリースでSystem Managerを使用してNAS環境を構成および管理する方法について説明します。

従来のSystem Manager（ONTAP 9 .7以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- "NFSセツテイノカイヨウ"
- "SMBセツテイノカイヨウ"

System Managerでサポートされるワークフロー

- NASファイルサービスに使用するクラスタの初期設定。
- 変化するストレージニーズに対応する追加のボリュームプロビジョニング。
- 業界標準の認証およびセキュリティ機能の設定とメンテナンス。

System Managerを使用すると、NASサービスをコンポーネント レベルで管理できます。

- プロトコル – NFS、SMB、または両方（NASのマルチプロトコル）
- ネーム サービス – DNS、LDAP、NIS
- ネーム サービス スイッチ
- KerberosとTLSのセキュリティ
- エクスポートと共有
- qtree
- ユーザおよびグループのネーム マッピング

VMwareデータストア用のNFSストレージのプロビジョニング

Virtual Storage Console for VMware vSphere（VSC）を使用してESXiホスト用のONTAPベースのストレージシステムにNFSボリュームをプロビジョニングする前に、System Manager for ONTAP 9 .7以降を使用してNFSを有効にしてください。

System Managerでを作成したら"NFS 対応の Storage VM"、VSCを使用してNFSボリュームをプロビジョニングし、データストアを管理します。

VSC 7.0以降では、VSCがに組み込まれて "ONTAP Tools for VMware vSphere 仮想アプライアンス"おり、VSC、vStorage APIs for Storage Awareness（VASA）Provider、およびStorage Replication Adapter（SRA）for VMware vSphereの機能が含まれています。

で "NetAppのInteroperability Matrix"、現在使用しているONTAPリリースとVSCリリースの互換性を確認して

ください。

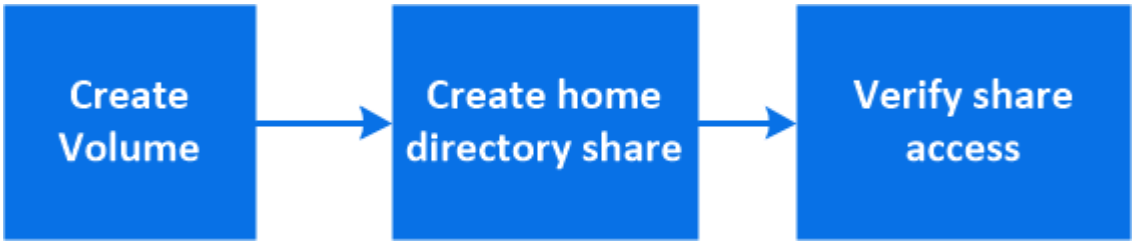
System Manager Classic（ONTAP 9.7以前のリリース）を使用してESXiホストからデータストアへのNFSアクセスを設定するには、を参照してください。 "VSCを使用したESXi向けのNFS設定の概要"

詳細については、およびVSCリリースのドキュメントを参照してください "TR-4597 ：『 VMware vSphere for ONTAP 』"。

ホームディレクトリ用のNASストレージのプロビジョニング

SMBプロトコルを使用して、ホームディレクトリ用のストレージを提供するボリュームを作成します。

この手順では、にホームディレクトリ用の新しいボリュームを作成し"SMB対応の既存のStorage VM"ます。ボリュームの設定時にシステムのデフォルトを受け入れることも、カスタム設定を指定することもできます。



FlexVolボリュームを作成することも、ハイパフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。も参照してください"FlexGroupボリュームを使用した大規模ファイルシステム用のNASストレージのプロビジョニング"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

手順

1. SMBが有効なStorage VMに新しいボリュームを追加します。
   a. [ストレージ]>[ボリューム]を選択し、[追加]*をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      SMBプロトコルが設定されているStorage VMのみが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

      - この時点で * Save * をクリックすると、 System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。
      - さらに * その他のオプション * をクリックしてボリュームの設定をカスタマイズし、許可、サービス品質、データ保護などのサービスを有効にすることができます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。
2. [ワークフローでステップ 2 、ステップ 2] [* ストレージ] > [共有] をクリックし、 [* 追加] をクリックして、 [* ホームディレクトリ *] を選択します。
3. Windowsクライアントで次の手順を実行して、共有にアクセスできることを確認します。
   a. エクスプローラで、次の形式で共有にドライブをマッピングします。
      `\\<SMB_Server_Name>\<Share_Name>`

変数（%w、%d、または%u）を使用して共有名を作成した場合は、解決された名前でアクセスをテストしてください。

b. 新しく作成したドライブで、テストファイルを作成して削除します。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

  - QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
  - 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
  - ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

    このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻り、[step2]ホームディレクトリのプロビジョニングを完了します。

NFSを使用したLinuxサーバ用のNASストレージのプロビジョニング

ONTAP System Manager（9.7以降）でNFSプロトコルを使用して、Linuxサーバ用のストレージを提供するボリュームを作成します。

この手順では、に新しいボリュームを作成し"NFS対応の既存のStorage VM"ます。ボリュームの設定時にシステムのデフォルトを受け入れることも、カスタム設定を指定することもできます。

FlexVolボリュームを作成することも、ハイパフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。も参照してください"FlexGroupボリュームを使用した大規模ファイルシステム用のNASストレージのプロビジョニング"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

ONTAP NFSプロトコルの機能の範囲の詳細については、を参照して"NFSリファレンスの概要"ください。

手順

1. NFS対応Storage VMに新しいボリュームを追加してください。
   a. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      NFSプロトコルが設定されているStorage VMだけが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

      - この時点で * Save * をクリックすると、 System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。

        デフォルトのエクスポートポリシーでは、すべてのユーザにフルアクセスが許可されます。

      - さらに * その他のオプション * をクリックしてボリュームの設定をカスタマイズし、許可、サービス品質、データ保護などのサービスを有効にすることができます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。
2. [step2-complete-prov, Step 2 in the workflow]] Linuxクライアントで、次の手順を実行してアクセスを確認します。
   a. Storage VMのネットワークインターフェイスを使用してボリュームを作成してマウントします。
   b. 新しくマウントしたボリュームで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

   アクセスの検証が完了したら、マウントボリュームに対して必要なUNIXの所有権と権限を設定できます"ボリュームのエクスポートポリシーを使用してクライアントアクセスを制限します"。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

- QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
- 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

  このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻り、[step2-complete-prov]NFSを使用するLinuxサーバのプロビジョニングを完了します。

ONTAPで実行するその他の方法

実行するタスク	参照先
System Managerクラシック（ONTAP 9 .7以前）	"NFSセツテイノカイヨウ"
ONTAPコマンドラインインターフェイス（CLI）	"CLIを使用したNFSの設定 - 概要"

エクスポートポリシーを使用したアクセスの管理

エクスポートポリシーを使用して、LinuxクライアントからNFSサーバへのアクセスを有効にします。

この手順では、のエクスポートポリシーを作成または変更し"NFS対応の既存のStorage VM"ます。

手順

1. System Manager で、 * Storage * > * Volumes * をクリックします。
2. NFS 対応ボリュームをクリックし、 * 詳細 * をクリックします。
3. [* エクスポートポリシーの編集 *] をクリックし、 [* 既存のポリシーの選択 *] または [* 新しいポリシーの追加 *] をクリックします。

SMBを使用した**Windows**サーバ用の**NAS**ストレージのプロビジョニング

ONTAP 9 .7以降で利用可能なSystem Managerを使用して、SMBプロトコルを使用して、Windowsサーバ用のストレージを提供するボリュームを作成します。

この手順では、に新しいボリュームを作成し"SMB対応の既存のStorage VM"、ボリュームのルート（/）ディレクトリの共有を作成します。ボリュームの設定時にシステムのデフォルトを受け入れることも、カスタム設定を指定することもできます。SMBの初期設定後、追加の共有を作成してそのプロパティを変更することもできます。

FlexVolボリュームを作成することも、ハイパフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。も参照してください"FlexGroupボリュームを使用した大規模ファイルシステム用のNASストレージのプロビジョニング"。

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

ONTAP SMBプロトコル機能の範囲の詳細については、を参照して"SMBリファレンスノガイヨウ"ください。

開始する前に

- ONTAP 9.13.1以降では、新しいボリュームに対して容量分析とアクティビティ追跡をデフォルトで有効にすることができます。System Managerでは、クラスタレベルまたはStorage VMレベルでデフォルト設定を管理できます。詳細については、を参照してください "ファイルシステム分析を有効にする"。

手順

1. SMBが有効なStorage VMに新しいボリュームを追加します。
   a. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* 追加] をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      SMBプロトコルが設定されているStorage VMのみが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、*[Storage VM]*フィールドは表示されません。

      - この時点で*[保存]*を選択した場合、System Managerはデフォルトのシステム設定を使用してFlexVolボリュームを作成および追加します。
      - [その他のオプション]*を選択すると、ボリュームの構成をカスタマイズして、許可、サービス品質（QoS）、データ保護などのサービスを有効にすることができます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。
2. [step2-sat-prov-win, Step 2 in the workflow]]共有がアクセス可能であることを確認するためにWindowsクライアントに切り替えます。
   a. エクスプローラで、次の形式で共有にドライブをマッピングします。
      `\\_SMB_Server_Name__Share_Name_`
   b. 新しく作成したドライブで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

アクセスの検証が完了したら、共有ACLを使用してクライアントアクセスを制限し、マッピングしたドライブに必要なセキュリティプロパティを設定できます。詳細については、を参照してください "SMB共有を作成する" 。

共有を追加または変更する

SMBの初期設定後に共有を追加できます。共有は、選択したデフォルト値とプロパティを使用して作成されます。これらは後で変更できます。

共有を設定するときは、次の共有プロパティを設定できます。

- アクセス権限
- 共有プロパティ
  - Hyper-V over SMBおよびSQL Server over SMBデータを含む共有の継続的可用性を有効にする（ONTAP 9 10.1以降）。関連項目：
    - "Hyper-V over SMBノケイソクテキカヨウセイヲヒエタキヨウユウノヨウケン"
    - "SQLServeroverSMBテノケイソクテキカヨウセイヲヒエタキヨウユウ"
  - この共有へのアクセス時にSMB 3.0でデータを暗号化します。

初期設定後に、次のプロパティを変更することもできます。

- シンボリックリンク
  - シンボリックリンクとワイドリンクを有効または無効にする
- 共有プロパティ
  - クライアントにSnapshotコピーディレクトリへのアクセスを許可します。
  - oplockを有効にして、クライアントがファイルをロックし、コンテンツをローカルにキャッシュできるようにします（デフォルト）。
  - ユーザのアクセス権限に基づいて共有リソースを表示するには、Access-Based Enumeration（ABE；アクセスベースの列挙）を有効にします。

手順

SMB 対応ボリュームに新しい共有を追加するには、 [ストレージ] 、 [共有] の順にクリックし、 [追加] をクリックして [共有 **] を選択します。

既存の共有を変更するには、**[ストレージ]>[共有]**をクリックし、をクリックし ⋮ て[*編集]を選択します。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

  - QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
  - 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。

◦ ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻り、[step2-compl-prov-win]SMBを使用したWindowsサーバのプロビジョニングを完了します。

ONTAPで実行するその他の方法

実行するタスク	参照先
System Managerクラシック（ONTAP 9 .7以前）	"SMBセツテイノカイヨウ"
ONTAPコマンドラインインターフェイス	"CLIヲシヨウシタSMBセツテイノカイヨウ"

NFSとSMBの両方を使用したWindowsとLinux用のNASストレージのプロビジョニング

NFSまたはSMBプロトコルを使用して、クライアントにストレージを提供するボリュームを作成します。

この手順では、に新しいボリュームを作成し"既存の Storage VM で NFS プロトコルと SMB プロトコルの両方が有効になっています"ます。

NFSプロトコルは、一般にLinux環境で使用されます。SMBプロトコルは、一般にWindows環境で使用されます。ただし、NFSとSMBはどちらもLinuxとWindowsのどちらでも使用できます。

FlexVolボリュームを作成することも、ハイパフォーマンスが求められる大規模なファイルシステムの場合はFlexGroupボリュームを作成することもできます。を参照して "FlexGroupボリュームを使用した大規模ファイルシステム用のNASストレージのプロビジョニング"

このボリュームの仕様をAnsible Playbookに保存することもできます。詳細については、を参照してください"Ansible Playbookを使用してボリュームやLUNを追加または編集"。

手順

1. NFSとSMBの両方が有効になっているStorage VMに新しいボリュームを追加してください。

   a. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* 追加] をクリックします。

   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      NFSプロトコルとSMBプロトコルの両方が設定されているStorage VMのみが表示されます。NFS プロトコルと SMB プロトコルが設定された Storage VM が 1 つしかない場合、「 * Storage VM * 」フィールドは表示されません。

   c. をクリックし、[NFS経由でエクスポート]*を選択します。

      デフォルトの設定では、すべてのユーザにフルアクセスが許可されます。あとでエクスポートポリシーにルールを追加できます。

   d. [* SMB / CIFS で共有] を選択します。

      共有が作成され、デフォルトのアクセス制御リスト（ ACL ）が「 Everyone 」グループに「 Full Control 」に設定されます。あとでACLに制限を追加できます。

   e. この時点で * Save * をクリックすると、 System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。

   また、許可、QoS、データ保護など、必要な追加サービスを引き続き有効にすることもできます。を参照して[ボリューム構成をカスタマイズする]から、ここに戻って次の手順を実行します。

2. [step2-sed-prov-nfs-smb、ワークフローの手順2] Linuxクライアントで、エクスポートがアクセス可能であることを確認します。

   a. Storage VMのネットワークインターフェイスを使用してボリュームを作成してマウントします。

   b. 新しくマウントしたボリュームで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

3. Windowsクライアントで次の手順を実行して、共有にアクセスできることを確認します。

   a. エクスプローラで、次の形式で共有にドライブをマッピングします。
      `\\_SMB_Server_Name__Share_Name_`

   b. 新しく作成したドライブで、テストファイルを作成してテキストを書き込み、ファイルを削除します。

   アクセスの検証が完了したら"ボリュームのエクスポートポリシーを使用してクライアントアクセスを制限し、共有 ACL を使用してクライアントアクセスを制限します"、エクスポートおよび共有ボリュームに所有権と権限を設定できます。

ボリューム構成をカスタマイズする

システムのデフォルトをそのまま使用する代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

手順

[* その他のオプション *] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

  ONTAP 9 .8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したり、QoSを無効にしたりできます。

  - QoS を無効にするには、「 * Custom * 」、「 * Existing * 」、「 * none * 」の順に選択します。
  - 「 * Custom * 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
  - ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

    このオプションは、リモートキャッシュオプションまたはFlexGroupボリュームオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ * ボリュームデータをクラスタ全体に分散 * を選択）。

  このオプションは、パフォーマンスサービスレベル * で手動配置 * を選択した場合は使用できません。それ以外の場合、追加するボリュームはデフォルトでFlexVol volumeになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirrorを使用したデータ保護（ローカルまたはリモート）を選択し、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻って、[step2-compl-prov-nfs-smb]WindowsサーバおよびLinuxサーバのマルチプロトコルプロビジョニングを完了します。

ONTAPで実行するその他の方法

実行するタスク	参照するコンテンツ
System Managerクラシック（ONTAP 9 .7以前）	"SMB と NFS のマルチプロトコル構成の概要"
ONTAPコマンドラインインターフェイス	• "CLIヲシヨウシタSMBセツテイノカイヨウ" • "CLIを使用したNFSの設定 - 概要" • "セキュリティ形式とその影響とは" • "マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別"

Kerberosによるクライアントアクセスの保護

Kerberosを有効にしてNASクライアントのストレージアクセスを保護します。

この手順では、またはに対して有効になっている既存のStorage VMでKerberosを設定し"NFS""SMB"ます。

作業を開始する前に、ストレージシステムでDNS、NTP、およびを設定しておく必要があり"LDAP"ます。

手順

1. ONTAPコマンドラインで、Storage VMのルートボリュームのUNIX権限を設定します。

   a. Storage VMのルートボリュームに対する関連する権限を表示します。 `volume show -volume root_vol_name-fields user,group,unix-permissions`

      Storage VM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
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	755

   a. これらの値が表示されない場合は、コマンドを使用し `volume modify`て更新します。

2. Storage VMのルートボリュームのユーザ権限を設定します。

   a. ローカルUNIXユーザを表示します。 `vserver services name-service unix-user show -vserver vserver_name`

      Storage VMに次の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**
NFS	500	0
root	0	0

+

   ◦ 注： 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。手順 5 を参照してください。

      a. これらの値が表示されない場合は、コマンドを使用し `vserver services name-service unix-user modify`て更新します。

3. Storage VMのルートボリュームのグループ権限を設定します。

   a. ローカルUNIXグループを表示します。 `vserver services name-service unix-group show -vserver vserver_name`

      Storage VMに次の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**
デーモン	1
root	0

a. これらの値が表示されない場合は、コマンドを使用し `vserver services name-service unix-group modify`て更新します。

4. System Managerに切り替えてKerberosを設定
5. System Manager で、 * Storage > Storage VM* をクリックし、 Storage VM を選択します。
6. [* 設定 *] をクリックします。
7. [Kerberos]をクリックします →
8. Kerberos Realm の下の * Add * をクリックし、次のセクションを完了します。
   - Kerberos Realmの追加

     KDCベンダーに応じて設定の詳細を入力します。

   - Realmへのネットワークインターフェイスの追加

     [* 追加] をクリックし、ネットワーク・インターフェイスを選択します。

9. 必要に応じて、Kerberosプリンシパル名からローカルユーザ名へのマッピングを追加します。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. をクリックし、[ネームマッピング]*の下をクリックします →。
   c. [KerberosからUNIX]*で、正規表現を使用してパターンと置換を追加します。

TLSによるセキュアなNFSクライアントアクセスの有効化または無効化

NFSクライアントとONTAPの間でネットワーク経由で送信されるすべてのデータを暗号化するようにNFS over TLSを設定すると、NFS接続のセキュリティを強化できます。これにより、NFS接続のセキュリティが向上します。これは、が有効になっている既存のStorage VMで設定できます"NFS"。

ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

TLSを有効にする

NFSクライアントに対してTLS暗号化を有効にすると、転送中のデータのセキュリティを強化できます。

開始する前に

NFS over TLSについては、を参照し"要件"てください。

1. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
2. [NFS]タイルで、*[NFS over TLS設定]*をクリックします。
3. [NFS over TLS設定]*領域で、TLSを有効にするNFSネットワークインターフェイスを選択します。
4. そのインターフェイスのをクリックし ⋮ ます。
5. [**Enable**] をクリックします。

6. [ネットワークインターフェイスのTLS設定]*ダイアログで、次のいずれかのオプションを選択して、TLSで使用する証明書を含めます。
   - インストール済み証明書：ドロップダウンリストから、以前にインストールした証明書を選択します。
   - 新しい証明書：証明書の共通名を選択します。
   - 外部の**CA**署名証明書：手順に従って、証明書と秘密鍵の内容をボックスに貼り付けます。
7. [保存（ Save ）] をクリックします。

TLSの無効化

転送中データのセキュリティ強化が必要なくなった場合は、NFSクライアントのTLSを無効にできます。

手順

1. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
2. [NFS]タイルで、*[NFS over TLS設定]*をクリックします。
3. [NFS over TLS設定]*領域で、TLSを無効にするNFSネットワークインターフェイスを選択します。
4. そのインターフェイスのをクリックし ⋮ ます。
5. [**Disable**] をクリックします。
6. 表示された確認ダイアログで*[無効化]*を選択します。

ネームサービスを使用したクライアントアクセスの提供

ONTAPによるNASクライアントの認証にLDAPまたはNISを使用したホスト、ユーザ、グループ、またはネットグループ情報の検索を有効にします。

この手順では、またはが有効になっている既存のStorage VMのLDAP設定またはNIS設定を作成または変更し"NFS""SMB"ます。

LDAP設定の場合は、環境で必要なLDAP設定の詳細を確認し、デフォルトのONTAP LDAPスキーマを使用する必要があります。

手順

1. 必要なサービスを設定します。 * Storage > Storage VM* をクリックします。
2. Storage VMを選択し、*[設定]*をクリックし、[LDAP]または[NIS]のをクリックし ⚙ ます。
3. ネームサービススイッチに変更を反映します。[ネームサービススイッチ]の下にあるをクリックします。 ✎

ディレクトリとファイルを管理します。

System Managerのボリューム表示を展開して、ディレクトリとファイルを表示および削除します。

ONTAP 9 .9.1以降では、低レイテンシの非同期ディレクトリ削除機能によってディレクトリが削除されます。

ONTAP 9 .9.1以降でのファイルシステムの表示の詳細については、を参照してください"ファイルシステム分析の概要"。

ステップ

1. Storage > Volumes （ストレージ）を選択します。ボリュームを展開して内容を表示します。

System Managerを使用したホスト固有のユーザとグループの管理

10.1以降では、ホストまたは**ONTAP 9**ホストに固有のユーザとグループを**System Manager**で管理できます。

次の手順を実行できます。

ウィンドウ	UNIX
• Windowsのユーザとグループの表示 • [add-edit-delete-Windows] • [manage-windows-users]	• UNIXユーザおよびグループの表示 • [add-edit-delete-UNIX] • [manage-unix-users]

Windowsのユーザとグループの表示

System Managerでは、Windowsのユーザとグループのリストを表示できます。

手順

1. System Manager で、 * Storage > Storage VM* をクリックします。
2. Storage VM を選択し、 * Settings * タブを選択します。
3. [* Host Users and Groups* （ホストユーザーとグループ * ）] 領域までスクロールします。

   「 * Windows * 」セクションには、選択した Storage VM に関連付けられている各グループのユーザ数の概要が表示されます。

4. Windows *セクションでをクリックします → 。
5. [グループ]*タブをクリックし、グループ名の横にあるをクリックすると、 ⌄ そのグループの詳細が表示されます。
6. グループ内のユーザーを表示するには、グループを選択し、 * ユーザー * タブをクリックします。

Windowsグループの追加、編集、削除

System Managerでは、Windowsグループを追加、編集、または削除して管理できます。

手順

1. System Managerで、Windowsグループのリストを表示します。を参照してください Windowsのユーザとグループの表示。
2. [* グループ *] タブでは、次のタスクを使用してグループを管理できます。

実行する処理	実行する手順

グループを追加します	1. をクリックします。 Add 2. グループ情報を入力します。 3. 権限を指定します。 4. グループメンバーを指定します（ローカルユーザ、ドメインユーザ、またはドメイングループを追加します）。
グループを編集します	1. グループ名の横にあるをクリックし、*[編集]*をクリックします。 2. グループ情報を変更します。
グループを削除します	1. 削除するグループの横にあるチェックボックスをオンにします。 2. をクリックします。 Delete *注：*グループ名の横にあるをクリックし、*削除*をクリックして、1つのグループを削除することもできます。

Windowsユーザの管理

System Managerでは、Windowsユーザの追加、編集、削除、有効化、無効化を行うことができます。Windowsユーザのパスワードを変更することもできます。

手順

1. System Managerで、グループのユーザのリストを表示します。を参照してください Windowsのユーザとグループの表示。
2. **[Users]** タブでは、次のタスクを実行してユーザを管理できます。

実行する処理	実行する手順
ユーザを追加します	1. をクリックします。 Add 2. ユーザ情報を入力します。
ユーザを編集します	1. ユーザ名の横にあるをクリックし、*[編集]*をクリックします。 2. ユーザ情報を変更します。

ユーザを削除します	1. 削除するユーザの横にあるチェックボックスをオンにします。 2. をクリックします。 Delete *注：*ユーザー名の横にあるをクリックし、*削除*をクリックして、1人のユーザーを削除することもできます 。
ユーザパスワードを変更します	1. ユーザ名の横にあるをクリックし 、*[パスワードの変更]*をクリックします。 2. 新しいパスワードを入力し、確認のためにもう一度入力します。
ユーザを有効にします	1. 有効にする無効になっている各ユーザの横にあるチェックボックスをオンにします。 2. をクリックします Enable
ユーザを無効にします	1. 無効にする有効な各ユーザの横にあるチェックボックスをオンにします。 2. をクリックします Disable

UNIXユーザおよびグループの表示

System Managerでは、UNIXユーザおよびグループのリストを表示できます。

手順

1. System Manager で、 * Storage > Storage VM* をクリックします。
2. Storage VM を選択し、 * Settings * タブを選択します。
3. [* Host Users and Groups* （ホストユーザーとグループ * ）] 領域までスクロールします。

   「 * unix * 」セクションには、選択した Storage VM に関連付けられた各グループのユーザ数の概要が表示されます。

4. [UNIX]セクションでをクリックします 。
5. [* グループ *] タブをクリックすると、そのグループの詳細が表示されます。
6. グループ内のユーザーを表示するには、グループを選択し、 * ユーザー * タブをクリックします。

UNIXグループを追加、編集、または削除する

System Managerでは、UNIXグループを追加、編集、または削除して管理できます。

手順

1. System Managerで、UNIXグループのリストを表示します。を参照してください UNIXユーザおよびグループの表示。

2. [* グループ *] タブでは、次のタスクを使用してグループを管理できます。

実行する処理	実行する手順
グループを追加します	1. をクリックします。 + Add 2. グループ情報を入力します。 3. （任意）関連付けられているユーザを指定します。
グループを編集します	1. グループを選択します。 2. をクリックします。 Edit 3. グループ情報を変更します。 4. （オプション）ユーザを追加または削除します。
グループを削除します	1. 削除するグループを選択します。 2. をクリックします。 Delete

UNIXユーザを管理します。

System Managerでは、Windowsユーザを追加、編集、削除して管理できます。

手順

1. System Managerで、グループのユーザのリストを表示します。を参照してください UNIXユーザおよびグループの表示。
2. [**Users**] タブでは、次のタスクを実行してユーザを管理できます。

実行する処理	実行する手順
ユーザを追加します	1. をクリックします。 + Add 2. ユーザ情報を入力します。
ユーザを編集します	1. 編集するユーザを選択します。 2. をクリックします。 Edit 3. ユーザ情報を変更します。
ユーザを削除します	1. 削除するユーザを選択します。 2. をクリックします。 Delete

NFSアクティブクライアントの監視

ONTAP 9 8以降では、クラスタでNFSのライセンスが有効な場合に、アクティブなNFSクライアント接続がSystem Managerに表示されます。

これにより、どのNFSクライアントがStorage VMにアクティブに接続しているか、どのNFSクライアントがアイドル状態であるか、どのNFSクライアントが切断されているかを簡単に確認できます。

NFS クライアントの各 IP アドレスについて、 * nfs clients * display show に * Time of last access * Network interface IP address * nfs connection version * Storage VM name と表示されます

また、過去 48 時間にアクティブだった NFS クライアントのリストが * Storage > Volumes * の表示にも表示され、 NFS クライアントの数は * Dashboard * 表示にも表示されます。

ステップ

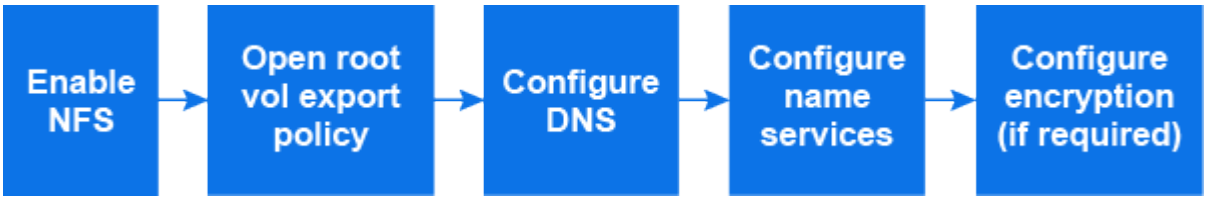
1. NFS クライアントアクティビティを表示します。 [*Hosts] > [NFS Clients] をクリックします。

NASストレージの有効化

NFSを使用した**Linux**サーバ用の**NAS**ストレージの有効化

Storage VMを作成または変更して、Linuxクライアントにデータを提供するためのNFSサーバを有効にします。

次の手順を使用して、NFSプロトコル用に新規または既存のStorage VMを有効にします。



開始する前に

環境で必要なネットワークサービス、認証サービス、またはセキュリティサービスの設定の詳細をメモしておいてください。

手順

1. Storage VMでNFSを有効にします。
   - 新しいStorage VMの場合：**[ストレージ]>[Storage VM]***をクリックし、[追加]をクリックして**Storage VM**名を入力し、[SMB / CIFS、NFS、S3]タブで[NFSの有効化]*を選択します。
     i. デフォルトの言語を確認します。
     ii. ネットワークインターフェイスを追加
     iii. Storage VM管理者アカウント情報の更新（オプション）
   - 既存のStorage VMの場合：**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[NFS]*の下をクリックし ⚙ ます。
2. Storage VMルートボリュームのエクスポートポリシーを開きます。
   a. [ストレージ]>[ボリューム]をクリックし、**Storage VM**のルートボリューム（デフォルトでは**_volume-name__root**）を選択して、[エクスポートポリシー]*に表示されるポリシーをクリックします。
   b. [追加]*をクリックしてルールを追加します。
      - クライアント仕様= `0.0.0.0/0`

- アクセスプロトコル= NFS
- アクセスの詳細 = UNIX読み取り専用

3. ホスト名解決に使用するDNSを設定します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[DNS]*の下をクリックし ます。
4. ネームサービスを必要に応じて設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックし、[LDAP]または[NIS]をクリックします 。
   b. [ネームサービススイッチ]タイル内をクリックし て変更を反映します。
5. 必要に応じて暗号化を設定します。

NFSクライアントの**TLS**の設定

ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

手順

1. 作業を開始する前に、『for NFS over TLS』を参照してください"要件"。
2. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
3. [NFS]タイルで、*[NFS over TLS設定]*をクリックします。
4. [NFS over TLS設定]*領域で、TLSを有効にするNFSネットワークインターフェイスを選択します。
5. そのインターフェイスのをクリックし ます。
6. [**Enable**] をクリックします。
7. [ネットワークインターフェイスのTLS設定]*ダイアログで、次のいずれかのオプションを選択して、TLSで使用する証明書を含めます。
   - インストール済み証明書：ドロップダウンリストから、以前にインストールした証明書を選択します。
   - 新しい証明書：証明書の共通名を選択します。
   - 外部の**CA**署名証明書：手順に従って、証明書と秘密鍵の内容をボックスに貼り付けます。
8. [保存（ Save ）] をクリックします。

Kerberosの設定

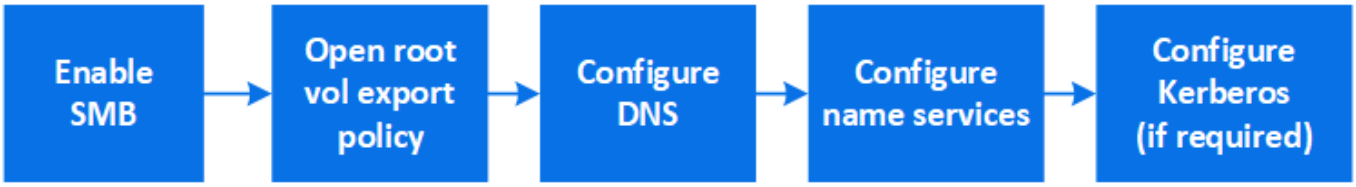
手順

1. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
2. [Kerberos]タイル内をクリックし 、*[追加]*をクリックします。

SMBを使用した**Windows**サーバ用の**NAS**ストレージの有効化

Windowsクライアントにデータを提供するためのSMBサーバを有効にするために、Storage VMを作成または変更します。

この手順では、新規または既存のStorage VMでSMBプロトコルを有効にします。環境で必要なネットワークサービス、認証サービス、またはセキュリティサービスについて、設定の詳細が提供されていることを前提としています。



手順

1. Storage VMでSMBを有効にします。
   a. 新しいStorage VMの場合：* Storage > Storage VM*をクリックし、* Add をクリックして**Storage VM**名を入力し、 SMB / CIFS、NFS、S3 タブで SMB / CIFSの有効化*を選択します。
      - 次の情報を入力します。
        - 管理者の名前とパスワード
        - サーバ名
        - Active Directoryドメイン
      - 組織単位を確定します。
      - DNS値を確定します。
      - デフォルトの言語を確認します。
      - ネットワークインターフェイスを追加
      - Storage VM管理者アカウント情報の更新（オプション）
   b. 既存のStorage VMの場合：**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[SMB]*の下をクリックし ます。
2. Storage VMルートボリュームのエクスポートポリシーを開きます。
   a. [ストレージ]>[ボリューム]をクリックし、**Storage VM**のルートボリューム（デフォルトでは**_volume-name_root_**）を選択し、[エクスポートポリシー]*に表示されるポリシーをクリックします。
   b. [追加]*をクリックしてルールを追加します。
      - クライアント仕様= `0.0.0.0/0`
      - アクセスプロトコル = SMB
      - アクセスの詳細= NTFS読み取り専用
3. ホスト名解決に使用するDNSを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]をクリックし、[DNS]*の下をクリックします 。
   b. DNSサーバに切り替えてSMBサーバをマッピングします。
      - フォワードルックアップ（A -アドレスレコード）とリバースルックアップ（PTR -ポインタレコード）のエントリを作成して、SMBサーバ名をデータネットワークインターフェイスのIPアドレスにマッピングします。
      - NetBIOSエイリアスを使用する場合は、エイリアスの正規名（CNAMEリソースレコード）ルック

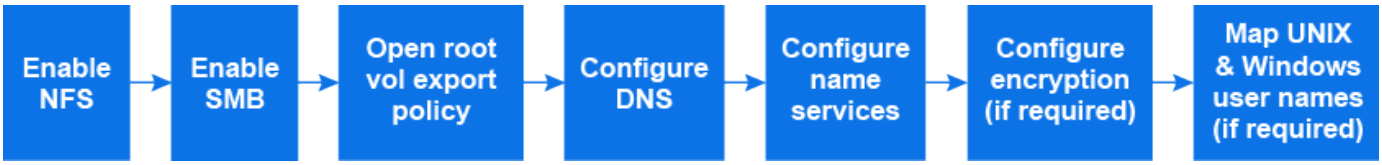
アップエントリを作成して、各エイリアスをSMBサーバのデータネットワークインターフェイスのIPアドレスにマッピングします。

4. ネームサービスを必要に応じて設定
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]をクリックし、[LDAP]または[NIS]*の下をクリックします 。
   b. ネームサービススイッチファイルに変更を反映します。*[ネームサービススイッチ]*の下にあるをクリックします 。
5. 必要に応じてKerberosを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
   b. でをクリックし、[追加]*をクリックし ます。

NFSと**SMB**の両方を使用した**Windows**と**Linux**の**NAS**ストレージの有効化

Storage VMを作成または変更して、NFSサーバとSMBサーバがLinuxクライアントとWindowsクライアントにデータを提供できるようにします。

この手順を使用して、新規または既存のStorage VMがNFSプロトコルとSMBプロトコルの両方を提供できるようにします。



開始する前に

環境で必要なネットワークサービス、認証サービス、またはセキュリティサービスの設定の詳細をメモしておいてください。

手順

1. Storage VMでNFSとSMBを有効にします。
   a. 新しいStorage VMの場合：* Storage > Storage VM*をクリックし、* Add をクリックして**Storage VM**名を入力し、 SMB / CIFS、NFS、S3 タブで SMB / CIFSの有効化*と* NFSの有効化*を選択します。
   b. 次の情報を入力します。
      - 管理者の名前とパスワード
      - サーバ名
      - Active Directoryドメイン
   c. 組織単位を確定します。
   d. DNS値を確定します。
   e. デフォルトの言語を確認します。
   f. ネットワークインターフェイスを追加
   g. Storage VM管理者アカウント情報の更新（オプション）
   h. 既存のStorage VMの場合：* Storage > Storage VM*をクリックし、Storage VMを選択して* Settings *

をクリックします。NFSまたはSMBがまだ有効になっていない場合は、次のサブ手順を実行します。

- [NFS]*の下にあるをクリックします 。
- [SMB]*でをクリックします 。

2. Storage VMルートボリュームのエクスポートポリシーを開きます。
   a. [ストレージ]>[ボリューム]をクリックし、**Storage VM**のルートボリューム（デフォルトでは**_volume-name_root_**）を選択し、[エクスポートポリシー]*に表示されるポリシーをクリックします。
   b. [追加]*をクリックしてルールを追加します。
      - クライアント仕様= `0.0.0.0/0`
      - アクセスプロトコル= NFS
      - アクセスの詳細 = NFS読み取り専用
3. ホスト名解決に使用するDNSを設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]をクリックし、[DNS]*の下をクリックします 。
   b. DNSの設定が完了したら、DNSサーバに切り替えてSMBサーバをマッピングします。
      - フォワードルックアップ（A -アドレスレコード）とリバースルックアップ（PTR -ポインタレコード）のエントリを作成して、SMBサーバ名をデータネットワークインターフェイスのIPアドレスにマッピングします。
      - NetBIOSエイリアスを使用する場合は、エイリアスの正規名（CNAMEリソースレコード）ルックアップエントリを作成して、各エイリアスをSMBサーバのデータネットワークインターフェイスのIPアドレスにマッピングします。
4. ネームサービスを必要に応じて設定します。
   a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックし、[LDAP]または[NIS]をクリックし ます。
   b. ネームサービススイッチファイルに変更を反映します。*[ネームサービススイッチ]*の下にあるをクリックします 。
5. 必要に応じて認証と暗号化を設定します。

NFSクライアントの**TLS**の設定

ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

手順

a. 作業を開始する前に、『for NFS over TLS』を参照してください"要件"。
b. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
c. [NFS]タイルで、*[NFS over TLS設定]*をクリックします。
d. [NFS over TLS設定]*領域で、TLSを有効にするNFSネットワークインターフェイスを選択します。
e. そのインターフェイスのをクリックし ⋮ ます。
f. [**Enable**] をクリックします。
g. [ネットワークインターフェイスのTLS設定]*ダイアログで、次のいずれかのオプションを選択して、TLSで使用する証明書を含めます。
   - インストール済み証明書：ドロップダウンリストから、以前にインストールした証明書を選択します。
   - 新しい証明書：証明書の共通名を選択します。
   - 外部の**CA**署名証明書：手順に従って、証明書と秘密鍵の内容をボックスに貼り付けます。
h. [保存（ Save ）] をクリックします。

Kerberosの設定

手順

a. [ストレージ]>[Storage VM]をクリックし、**Storage VM**を選択して[設定]*をクリックします。
b. [Kerberos]タイル内をクリックし →、*[追加]*をクリックします。

6. 必要に応じてUNIXとWindowsのユーザ名をマッピングします。**[**ネームマッピング**]***でをクリックし、[追加]*をクリックし → ます。

   この処理は、WindowsとUNIXのユーザアカウントが暗黙的にマッピングされない場合にのみ実行します。小文字のWindowsユーザ名がUNIXユーザ名と一致している場合は、この処理を実行します。ユーザ名は、LDAP、NIS、またはローカルユーザを使用してマッピングできます。一致しないユーザセットが2つある場合は、ネームマッピングを設定する必要があります。

CLIを使用したNFSの設定

CLIを使用したNFSの設定 - 概要

ONTAP 9 CLIコマンドを使用して、新規または既存のStorage Virtual Machine（SVM）の新しいボリュームまたはqtreeに格納されているファイルへのNFSクライアントアクセスを設定できます。

次の手順は、ボリュームまたはqtreeへのアクセスを設定する場合に使用します。

- ONTAPで現在サポートされている次のいずれかのバージョンを使用する必要がある：NFSv3、NFSv4、NFSv4.1、NFSv4.2、またはpNFSを含むNFSv4.1。
- System Managerや自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

  System Managerを使用してNASマルチプロトコルアクセスを設定する方法については、を参照してください"NFSとSMBの両方を使用したWindowsとLinux用のNASストレージのプロビジョニング"。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

  コマンド構文の詳細については、CLIヘルプおよびONTAPのマニュアルページを参照してください。

- 新しいボリュームはUNIXファイル権限を使用して保護されます。
- SVM管理者Privilegesではなく、クラスタ管理者Privilegesが必要です。

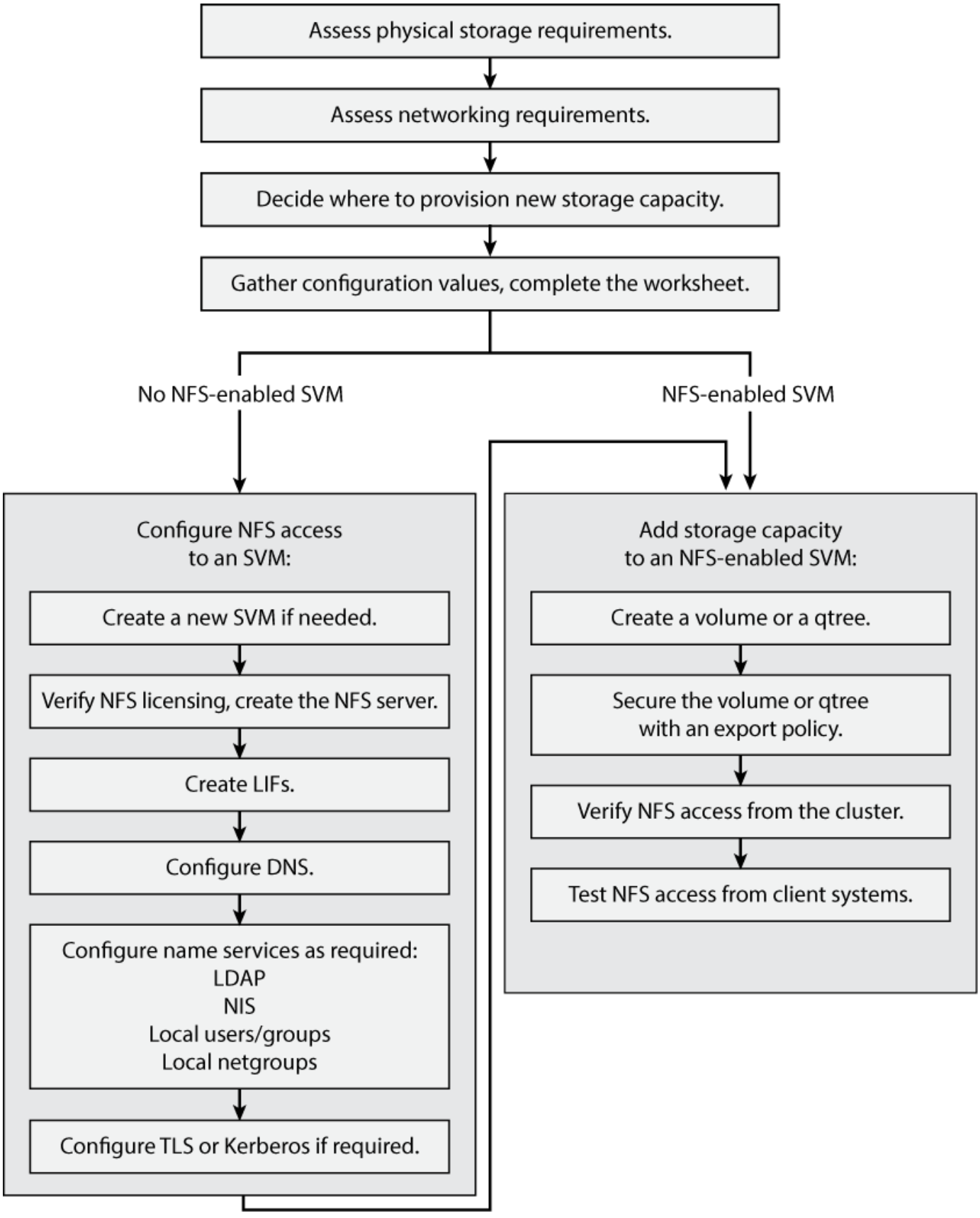
ONTAP NFSプロトコルの機能の範囲の詳細については、を参照して"NFSリファレンスの概要"ください。

ONTAPで実行するその他の方法

実行するタスク	参照先
再設計されたSystem Manager（ONTAP 9 .7以降で使用可能）	"NFSを使用したLinuxサーバ用のNASストレージのプロビジョニング"
System Manager Classic（ONTAP 9 .7以前で使用可能）	"NFSセツテイノカイヨウ"

NFSの設定ワークフロー

NFSを設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存のSVMへのNFSアクセスを設定するか、すでにNFSアクセスの設定が完了している既存のSVMにボリュームまたはqtreeを追加するかによってワークフローが異なります。


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

準備

物理ストレージ要件の評価

クライアント用のNFSストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリューム用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。

   ```
   storage aggregate show
   ```

   十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 十分なスペースを備えたアグリゲートがない場合は、コマンドを使用して既存のアグリゲートにディスクを追加する `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成し `storage aggregate create`ます。

ネットワーク要件の評価

クライアントにNFSストレージを提供する前に、ネットワークが正しく設定されてNFSのプロビジョニング要件を満たしていることを確認する必要があります。

必要なもの

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）

- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）
- 外部ファイアウォール

手順

1. 使用可能な物理ポートと仮想ポートを表示します。

   ```
   network port show
   ```

   - 可能な場合は、データネットワークの速度が最も速いポートを使用してください。
   - 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。

2. サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットが存在し、十分な数のアドレスが使用可能であることを確認してください： +

   ```
   network subnet show
   ```

   サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。

3. 使用可能なIPspaceを表示します。

   ```
   network ipspace show
   ```

   デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

4. IPv6アドレスを使用する場合は、IPv6がクラスタで有効になっていることを確認します。

   ```
   network options ipv6 show
   ```

   必要に応じて、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

新しい**NFS**ストレージ容量のプロビジョニング先の検討

新しいNFSボリュームまたはqtreeを作成する前に、そのボリュームを新規、既存のどちらのSVMに配置するかを決め、配置先のSVMでどのような設定が必要になるかを確認しておく必要があります。それによって以降のワークフローが決まります。

選択肢

- 新しいSVM、またはNFSが有効になっているが設定はまだ完了していない既存のSVMにボリュームまたはqtreeをプロビジョニングする場合は、「SVMへのNFSアクセスの設定」と「NFS対応SVMへのNFSストレージの追加」の両方の手順を実行します。

  SVMへのNFSアクセスの設定

  NFS対応SVMへのNFSストレージの追加

  次のいずれかに該当する場合は、新しいSVMを作成します。

- クラスタでNFSを初めて有効にする場合。
- クラスタ内の既存のSVMでNFSサポートを有効にするのが望ましくない場合。
- クラスタ内に NFS 対応の SVM が 1 つ以上あり、分離されたネームスペースに別の NFS サーバが必要な場合（マルチテナンシーシナリオ）。NFSが有効になっているものの設定されていない既存のSVMでストレージをプロビジョニングする場合にも、このオプションを選択する必要があります。これが当てはまるのは、SANアクセス用のSVMを作成している場合や、SVM作成時にどのプロトコルも有効になっていなかった場合です。

SVMでNFSを有効にしたあとに、ボリュームまたはqtreeのプロビジョニングに進みます。

- NFSアクセスの設定が完了している既存のSVMでボリュームまたはqtreeをプロビジョニングする場合は、「NFS対応SVMへのストレージ容量の追加」の手順を完了します。

  NFS対応SVMへのストレージ容量の追加

NFS設定情報を収集するためのワークシート

NFS設定ワークシートを使用すると、クライアントのNFSアクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所に関する決定に応じて、ワークシートのいずれかまたは両方のセクションを完了する必要があります。

SVMへのNFSアクセスを設定する場合は、両方のセクションを完了する必要があります。

- SVMへのNFSアクセスの設定
- NFS対応SVMへのストレージ容量の追加

NFS対応SVMにストレージ容量を追加する場合は、次の操作のみを完了する必要があります。

- NFS対応SVMへのストレージ容量の追加

SVMへの**NFS**アクセスの設定

- SVM を作成するためのパラメータ *

新しいSVMを作成する場合は、コマンドで次の値を指定します `vserver create`。

フィールド	説明	あなたの価値
`-vserver`	新しいSVMの名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意のSVM名を適用する別の命名規則に従います。	

`-aggregate`	新しいNFSストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-rootvolume`	SVMルート ボリュームの一意の名前を指定します。	
`-rootvolume-security-style`	SVMのUNIXセキュリティ形式を使用します。	`unix`
`-language`	このワークフローではデフォルトの言語設定を使用します。	`C.UTF-8`
`ipspace`	IPspace は、 Storage Virtual Machine （ SVM ）が属する個別の IP アドレススペースです。	

* NFS サーバ作成用のパラメータ *

新しいNFSサーバを作成し、サポートされているNFSバージョンを指定する場合は、コマンドで次の値を指定し `vserver nfs create`ます。

NFSv4以降を有効にする場合は、セキュリティを強化するためにLDAPを使用する必要があります。

フィールド	説明	あなたの価値
`-v3 -v4.0`、、、 `-v4.1 -v4.1 -pnfs`	必要に応じてNFSバージョンを有効にします。 が有効になっている場合は、ONTAP 9 .8以降でもv4.2がサポートされ `v4.1`ます。	
`-v4-id-domain`	IDマッピングドメイン名。	
`-v4-numeric-ids`	所有者IDの数値のサポート（有効または無効）。	

* NFS接続のTLS暗号化を有効にするパラメータ*

コマンドでは、次の値を指定します `vserver nfs tls interface enable`。

ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

フィールド	説明	あなたの価値
`-vserver`	論理インターフェイスが存在するSVM。	
`-lif`	NFS over TLSを使用して転送中の暗号化を有効にする論理インターフェイスの名前。	
`-certificate-name`	Storage VMに設定されているX.509証明書の名前。	

- LIF 作成用のパラメータ *

LIFを作成する場合は、コマンドで次の値を指定します `network interface create`。

Kerberosを使用する場合は、複数のLIFでKerberosを有効にする必要があります。

フィールド	説明	あなたの価値
`-lif`	新しいLIFの名前を指定します。	
`-role`	このワークフローではデータLIFのロールを使用します。	`data`
`-data-protocol`	このワークフローではNFSプロトコルのみを使用します。	`nfs`
`-home-node`	LIFに対してコマンドを実行したときにLIFが戻るノード `network interface revert`。	
`-home-port`	LIFに対してコマンドを実行したときにLIFが戻るポートまたはインターフェイスグループ `network interface revert`。	
`-address`	新しいLIFによるデータアクセスに使用する、クラスタ上のIPv4アドレスまたはIPv6アドレスを指定します。	

`-netmask`	LIFのネットワークマスクとゲートウェイ。	
`-subnet`	IPアドレスのプール。および `-netmask`の代わりに使用して `-address`、アドレスとネットマスクを自動的に割り当てます。	
`-firewall-policy`	このワークフローではデフォルトのデータファイアウォールポリシーを使用します。	`data`

- DNS ホスト名解決のパラメータ *

DNSを設定する場合は、コマンドで次の値を指定します `vserver services name-service dns create`。

フィールド	説明	あなたの価値
`-domains`	最大5つのDNSドメイン名。	
`-name-servers`	DNSネームサーバごとに最大3つのIPアドレス。	

ネームサービス情報

- ローカルユーザー作成用のパラメータ *

コマンドを使用してローカルユーザを作成する場合は、次の値を指定し `vserver services name-service unix-user create`ます。Uniform Resource Identifier（URI）からUNIXユーザを含むファイルをロードしてローカルユーザを設定する場合は、これらの値を手動で指定する必要はありません。

	ユーザ名 (`-user`)	ユーザID (`-id`)	グループID (`-primary-gid`)	フルネーム (`-full-name`)
例	johnm	123	100	John Miller
1				
2				
3				
…				
n				

- ローカルグループを作成するためのパラメータ *

コマンドを使用してローカルグループを作成する場合は、次の値を指定し `vserver services name-service unix-group create`ます。UNIXグループを含むファイルをURIからロードしてローカルグループを設定する場合は、これらの値を手動で指定する必要はありません。

	グループ名(-name)	グループID(-id)
例	エンジニアリング	100
1		
2		
3		
…		
n		

- NISのパラメータ*

コマンドでは、次の値を指定します `vserver services name-service nis-domain create`。

ONTAP 9 .2以降では、 `-nis-servers`フィールドがフィールドに置き換わります `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

フィールド	説明	あなたの価値
`-domain`	SVMが名前検索に使用するNISドメインを指定します。	
`-active`	アクティブなNISドメインサーバを指定します。	`true`または `false`
`-servers`	ONTAP 9.0 、 9.1 ： NIS ドメイン設定で使用される NIS サーバの 1 つ以上の IP アドレスを指定します。	
`-nis-servers`	ONTAP 9.2 ：ドメイン設定で使用される NIS サーバの IP アドレスおよびホスト名をカンマで区切って指定します。	

- LDAPのパラメータ*

コマンドでは、次の値を指定します `vserver services name-service ldap client create`。

また、自己署名ルートCA証明書ファイルも必要 `.pem`です。

ONTAP 9 .2以降では、 `-ldap-servers`フィールドがフィールドに置き換わります `-servers`。この新しいフィールドには、LDAPサーバのホスト名またはIPアドレスを指定できます。

フィールド	説明	あなたの価値
`-vserver`	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`	新しいLDAPクライアント設定に割り当てる名前。	
`-servers`	ONTAP 9.0 、 9.1 ： 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。	
`-ldap-servers`	ONTAP 9.2 ： LDAP サーバの IP アドレスおよびホスト名をカンマで区切って指定します。	
`-query-timeout`	このワークフローのデフォルトの秒数を使用し`3`ます。	`3`
`-min-bind-level`	最小バインド認証レベルを指定します。デフォルトはです `anonymous`。署名と封印が設定されている場合はに設定する必要があります `sasl`。	
`-preferred-ad-servers`	1つ以上の優先Active Directoryサーバ（カンマで区切ったIPアドレス）	
`-ad-domain`	Active Directoryドメイン。	
`-schema`	使用するスキーマテンプレート。デフォルトまたはカスタムのスキーマを使用できます。	
`-port`	このワークフローにはデフォルトのLDAPサーバポートを使用し`389`ます。	`389`

フィールド	説明	あなたの価値
`-bind-dn`	バインドユーザの識別名。	
`-base-dn`	ベース識別名。デフォルトは（root）です `""`。	
`-base-scope`	このワークフローのデフォルトのベース検索範囲を使用します `subnet`。	`subnet`
`-session-security`	LDAPの署名または署名と封印を有効にします。デフォルトはです `none`。	
`-use-start-tls`	LDAP over TLSを有効にします。デフォルトはです `false`。	

- Kerberos 認証のパラメータ *

コマンドでは、次の値を指定します `vserver nfs kerberos realm create`。一部の値は、Microsoft Active DirectoryをKey Distribution Center（KDC；キー配布センター）サーバとして使用するか、MITまたはその他のUNIX KDCサーバとして使用するかによって異なります。

フィールド	説明	あなたの価値
`-vserver`	KDCと通信するSVMを指定します。	
`-realm`	Kerberos Realmを指定します。	
`-clock-skew`	クライアントとサーバ間で許容されるクロックスキュー。	
`-kdc-ip`	KDCのIPアドレス。	
`-kdc-port`	KDCポート番号。	
`-adserver-name`	Microsoft KDC のみ： AD サーバ名を指定します。	
`-adserver-ip`	Microsoft KDC のみ： AD サーバの IP アドレスを指定します。	
`-adminserver-ip`	UNIX KDC のみ：管理サーバの IP アドレスを指定します。	

-adminserver-port	UNIX KDC のみ：管理サーバのポート番号を指定します。	
-passwordserver-ip	UNIX KDC のみ：パスワードサーバの IP アドレスを指定します。	
-passwordserver-port	UNIX KDC のみ：パスワードサーバのポートを指定します。	
-kdc-vendor	KDCベンダー。	{Microsoft
Other}	-comment	必要なコメントを指定します。

コマンドでは、次の値を指定します vserver nfs kerberos interface enable。

フィールド	説明	あなたの価値
-vserver	Kerberos設定を作成するSVMの名前を指定します。	
-lif	Kerberosを有効にするデータLIFを指定します。Kerberosは複数のLIFで有効にすることができます。	
-spn	サービスプリンシパル名（SPN）	
-permitted-enc-types	Kerberos over NFSで許可される暗号化タイプ。クライアントの機能に応じて推奨されます。 aes-256	
-admin-username	KDCからSPNシークレットキーを直接取得するためのKDC管理者のクレデンシャル。パスワードは必須です	
-keytab-uri	KDC管理者のクレデンシャルがない場合は、SPNキーが含まれているKDCのkeytabファイル。	
-ou	Microsoft KDCのRealmを使用してKerberosを有効にした場合にMicrosoft Active Directoryサーバアカウントが作成される組織単位（OU）。	

- エクスポートポリシーおよびルールを作成するためのパラメータ *

コマンドでは、次の値を指定します `vserver export-policy create`。

フィールド	説明	あなたの価値
`-vserver`	新しいボリュームをホストするSVMの名前を指定します。	
`-policyname`	新しいエクスポートポリシーの名前を指定します。	

コマンドでは、ルールごとに次の値を指定し `vserver export-policy rule create`ます。

フィールド	説明	あなたの価値
`-clientmatch`	クライアント一致を指定します。	
`-ruleindex`	ルールリスト内でのエクスポートルールの位置。	
`-protocol`	このワークフローではNFSを使用します。	`nfs`
`-rorule`	読み取り専用アクセスの認証方式を指定します。	
`-rwrule`	読み取り / 書き込みアクセスの認証方式を指定します。	
`-superuser`	スーパーユーザ アクセスの認証方式を指定します。	
`-anon`	匿名ユーザをマッピングするユーザIDを指定します。	

エクスポート ポリシーごとにルールを1つ以上作成する必要があります。

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
例	0.0.0.0/0、@rootaccess_netgroup	任意	krb5	sys	65534
1					

2					
3					
…					
n					

* ボリュームを作成するためのパラメータ *

qtreeではなくボリュームを作成する場合は、コマンドで次の値を指定します `volume create`。

フィールド	説明	あなたの価値
`-vserver`	新しいボリュームをホストする新規または既存のSVMの名前を指定します。	
`-volume`	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
`-aggregate`	新しいNFSボリュームに対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-size`	新しいボリュームのサイズとして任意の整数を指定します。	
`-user`	ボリュームのルートの所有者に設定するユーザの名前またはIDを指定します。	
`-group`	ボリュームのルートの所有者に設定するグループの名前またはIDを指定します。	
`--security-style`	このワークフローにはUNIXセキュリティ形式を使用します。	`unix`
`-junction-path`	新しいボリュームのマウント先とする、ルート（/）の下の場所を指定します。	

`-export-policy`	既存のエクスポート ポリシーを使用する場合は、ボリュームの作成時に名前を入力できます。	

- qtree を作成するためのパラメータ *

ボリュームではなくqtreeを作成する場合は、コマンドで次の値を指定します `volume qtree create`。

フィールド	説明	あなたの価値
`-vserver`	qtreeを含むボリュームが配置されているSVMの名前。	
`-volume`	新しいqtreeを格納するボリュームの名前。	
`-qtree`	新しいqtreeには、64文字以下の一意のわかりやすい名前を指定します。	
`-qtree-path`	ボリュームとqtreeを別 々 の引数として指定する代わりに、qtreeパスをの形式で `/vol/*volume_name/qtree_name*\>` 指定できます。	
`-unix-permissions`	オプション： qtree の UNIX 権限を指定します。	
`-export-policy`	既存のエクスポートポリシーを使用する場合は、qtreeの作成時に名前を入力できます。	

関連情報

- "ONTAPコマンド リファレンス"

SVMへのNFSアクセスの設定

SVMの作成

クラスタ内にNFSクライアントにデータ アクセスを提供するSVMが1つもない場合は、作成する必要があります。

開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

手順

1. SVMを作成します。

   ```
   vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
   ipspace_name
   ```

   - オプションにはUNIX設定を使用し `-rootvolume-security-style`ます。
   - デフォルトのC.UTF-8オプションを使用し `-language`ます。
   - この `ipspace`設定はオプションです。

2. 新しく作成したSVMの設定とステータスを確認します。

   ```
   vserver show -vserver vserver_name
   ```

   `Allowed Protocols`フィールドには
   nfsを指定する必要があります。このリストは後で編集できます。

   `Vserver Operational State`フィールドには状態が表示されている必要があり
   `running`ます。状態が表示された場合は
   `initializing`、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

例

次のコマンドは、データアクセス用のSVMをIPspace ipspaceAに作成します。

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて状態になっていることを示しています running。ルートボリュームには、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あるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP 9 .13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

SVMで**NFS**プロトコルが有効になっていることの確認

SVMでNFSを設定して使用する前に、このプロトコルが有効になっていることを確認する必要があります。

タスクの内容

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、セットアップ時にプロトコルを有効にしなかった場合でも、コマンドを使用してあとから有効にすることができます `vserver add-protocols`。

作成したプロトコルは、 LIF から追加または削除することはできません。

コマンドを使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols`。

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確認します。

   ```
   vserver show -vserver vserver_name -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 `vserver show-protocols`。

2. 必要に応じて、プロトコルを有効または無効にします。

   - NFSプロトコルを有効にするには+
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - プロトコルを無効にするには：+
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`

3. 有効 / 無効な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 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   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を追加することで、NFS経由のアクセスを許可し `nfs`ます。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

SVMルートボリュームのエクスポートポリシーを開く

SVM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には、すべてのクライアントにNFS経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVMとそのボリュームに対するNFSクライアントのアクセスがすべて拒否されます。

タスクの内容

新しいSVMが作成されると、デフォルトのエクスポートポリシー（default）がSVMのルートボリュームに対し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。

デフォルトのエクスポートポリシーですべてのNFSクライアントにアクセスが許可されていることを確認してから、個 々 のボリュームまたはqtreeにカスタムのエクスポートポリシーを作成して個 々 のボリュームへの

アクセスを制限する必要があります。

手順

1. 既存のSVMを使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。

   ```
   vserver export-policy rule show
   ```

   次のようなコマンド出力が表示されます。

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol:  nfs
   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: 65534
                       Superuser Security Types: any
                   Honor SetUID Bits in SETATTR: true
                      Allow Creation of Devices: true
   ```

   オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVM ルートボリュームのエクスポートルールを作成します。

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Kerberosで保護されたボリュームのみをSVMに格納する場合は、ルートボリュームのエクスポートルールオプション、 `-rwrule`、、を `-superuser`または `krb5i`に `krb5`設定できます `-rorule`。例：

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. コマンドを使用してルールの作成を確認します `vserver export-policy rule show`。

結果

これで、SVMで作成されたすべてのボリュームまたはqtreeに、すべてのNFSクライアントからアクセスできるようになります。

NFSサーバを作成する

クラスタでNFSのライセンスが有効であることを確認したら、コマンドを使用してSVM

にNFSサーバを作成し、サポートするNFSのバージョンを指定できます `vserver nfs create`。

タスクの内容

SVM は、 NFS の 1 つ以上のバージョンをサポートするように設定できます。NFSv4以降をサポートしている場合：

- NFSv4ユーザIDマッピングのドメイン名は、NFSv4サーバとターゲットクライアントで同じである必要があります。

  NFSv4サーバとクライアントで同じ名前を使用しているかぎり、LDAPまたはNISドメイン名と同じにする必要はありません。

- ターゲットクライアントがNFSv4数値ID設定をサポートしている必要があります。
- セキュリティ上の理由から、NFSv4環境でのネームサービスにはLDAPを使用する必要があります。

開始する前に

SVM を、 NFS プロトコルを許可するように設定しておく必要があります。

手順

1. クラスタ上でNFSのライセンスが有効であることを確認します。

   ```
   system license show -package nfs
   ```

   サポートされていない場合は、営業担当者にお問い合わせください。

2. NFSサーバを作成します。

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   NFSバージョンは任意に組み合わせて有効にすることができます。pNFSをサポートする場合は、オプションと `-v4.1-pnfs`オプションの両方を有効にする必要があります `-v4.1`。

   v4以降を有効にする場合は、次のオプションが正しく設定されていることも確認してください。

   - `-v4-id-domain`

     （オプション）このパラメータは、NFSv4プロトコルで定義されているユーザ名およびグループ名のドメイン部分を指定します。デフォルトでは、NISドメインが設定されている場合はONTAPが使用し、設定されていない場合はDNSドメインが使用されます。ターゲットクライアントで使用されるドメイン名と一致する値を指定する必要があります。

   - `-v4-numeric-ids`

     （オプション）このパラメータは、NFSv4の所有者属性で数値IDのサポートを有効にするかどうかを指定します。デフォルト設定はenabledですが、ターゲットクライアントがこの設定をサポートしていることを確認する必要があります。

   NFSのその他の機能を有効にするには、コマンドを使用し `vserver nfs modify`ます。

3. NFSが実行されていることを確認します。

   ```
   vserver nfs status -vserver vserver_name
   ```

4. NFSが必要に応じて設定されていることを確認します。

   ```
   vserver nfs show -vserver vserver_name
   ```

例

次のコマンドは、 NFSv3 と NFSv4.0 が有効な 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 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

次のコマンドは、vs1という名前の新しいNFSサーバのステータスと設定値を確認します。

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
            NFSv4 ID Mapping Domain: my_domain.com
...
```

LIFの作成

LIFは、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

必要なもの

- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

- LIFで処理されるトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9 .5以前では、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- Kerberos認証を使用する場合は、複数のLIFでKerberosを有効にします。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。
- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、同じサブネットにすでに設定されている他のLIFと同じブロードキャストドメイン内の指定したホームノード上の任意のポートを自動的に選択します。

ONTAP 9 .4以降では、FC-NVMeがサポートされます。FC-NVMe LIFを作成する場合は、次の点に注意してください。

- LIFを作成するFCアダプタでNVMeプロトコルがサポートされている必要があります。
- データLIFで使用できるデータプロトコルはFC-NVMeのみです。
- SANをサポートするStorage Virtual Machine（SVM）ごとに、管理トラフィックを処理するLIFを1つ設定する必要があります。
- NVMe LIFとネームスペースは同じノードでホストされている必要があります。
- データトラフィックを処理するNVMe LIFは、SVMごとに1つだけ設定できます。

手順

1. LIFを作成します。

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

オプション	説明
• ONTAP 9.5 以前 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

• ONTAP 9.6 以降 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- `-role`サービスポリシーを使用してLIFを作成する場合（ONTAP 9.6以降）は、パラメータは必要ありません。
- このパラメータは `-data-protocol`LIFの作成時に指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。

  > `-data-protocol`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。

- `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert。

  オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます -auto-revert。

- `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert。
- オプションと -netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address。
- サブネットを使用してIPアドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときに、ゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
- IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。 `network route create`のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- オプションには -firewall-policy、LIFのロールと同じデフォルトを使用し `data`ます。

  必要に応じて、あとからカスタムファイアウォールポリシーを作成して追加できます。

  > ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false。

2. コマンドを使用して、LIFが正常に作成されたことを確認します network interface show。

3. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

4. Kerberosを使用する場合は、手順1~3を繰り返して追加のLIFを作成します。

   これらの各LIFでKerberosを個別に有効にする必要があります。

例

次のコマンドは、LIFを作成し、パラメータと `-netmask`パラメータを使用してIPアドレスとネットワークマスク値を指定し `-address`ます。

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワークマスク値を指定したサブネット（client1_sub）から割り当てます。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

次のコマンドは、サービスポリシーが割り当てられたNASデータLIFを作成する方法を示してい `default-data-files`ます。

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

ホスト名解決のための**DNS**の有効化

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して

解決されます。

必要なもの

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。 `vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。

タスクの内容

SVM での動的 DNS の設定については、『ネットワーク管理ガイド』を参照してください。

手順

1. SVMでDNSを有効にします。

   ```
   vserver services name-service dns create -vserver vserver_name -domains
   domain_name -name-servers ip_addresses -state enabled
   ```

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   ONTAP 9 .2以降では `vserver services name-service dns create`、コマンドによって設定の自動検証が実行され、ONTAPがネームサーバに接続できない場合はエラーメッセージが報告されます。

2. コマンドを使用して、DNSドメイン設定を表示します `vserver services name-service dns show`。

   次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. コマンドを使用して、ネームサーバのステータスを検証し `vserver services name-service dns check`ます。

   この `vserver services name-service dns check`コマンドは、ONTAP 9 .2以降で使用できます。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver            Name Server     Status       Status Details
---------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

ネームサービスを設定する

ネームサービスの設定の概要

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権を提供するために ONTAP でホスト、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ようにする必要があります。この情報を取得するためには、 ONTAP がローカルまたは外部のネームサービスにアクセス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。

NIS や LDAP などのネームサービスは、クライアント認証時の名前検索を容易にするために使用する必要があります。特に NFSv4 以降を導入する際は、セキュリティ強化のために、可能なかぎり LDAP を使用することを推奨します。外部ネームサーバが使用できない場合に備えて、ローカルのユーザとグループも設定する必要があります。

ネームサービス情報は、すべてのソースで同期を維持する必要があります。

ネームサービススイッチテーブルを設定する

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、グループ、ネットグループ、またはネームマッピングの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。

必要なもの

ホスト、ユーザ、グループ、ネットグループ、またはネームマッピングで現在の環境に該当するように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する場合、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 での指定どおりに短縮および圧縮されている必要があります。

タスクの内容

使用されていない情報ソースは含めないでください。たとえば、ご使用の環境でNISが使用されていない場合は、オプションを指定しない `-sources nis`でください。

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`*

   修正する場合は、コマンドまたは `vserver services name-service ns-switch delete`コマンドを使用する必要があります `vserver services name-service ns-switch modify`。

例

次の例は、 SVM vs1 がローカルネットグループファイルを使用し、外部 NIS サーバがネットグループ情報をこの順序で検索するように、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ます。

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

終了後

- データアクセスを提供するには、 SVM 用に指定したネームサービスを設定する必要があります。
- SVM 用のネームサービスを削除する場合は、ネームサービススイッチテーブルからも削除する必要があります。

  ネームサービススイッチテーブルからネームサービスを削除しないと、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場合があります。

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の設定の概要

SVM 上で、認証およびネームマッピングにローカル UNIX ユーザおよびグループを使用できます。UNIX ユーザおよびグループは、手動で作成することも、 Uniform Resource Identifier （ URI ）から UNIX ユーザまたはグループを含むファイルをロードすることもできます。

クラスタ内のローカル UNIX ユーザ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。

ローカル**UNIX**ユーザを作成する

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 `vserver services name-service unix-user create`。ローカル UNIX ユーザは、 SVM 上に UNIX ネームサービスオプションとして作成し、ネームマッピングの処理で使用する UNIX ユーザです。

ステップ

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
   ```

   `-user *user_name*`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*`割り当てるユーザIDを指定します。

   `-primary-gid *integer*`プライマリグループIDを指定します。これにより、ユーザがプライマリグループに追加されます。ユーザを作成したあと、手動でユーザを目的の追加グループに追加できます。

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vs1というSVM上に作成します。ユーザの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"
```

URIからローカル**UNIX**ユーザをロードします。

SVMで個 々 のローカルUNIXユーザを手動で作成する別の方法として、ローカルUNIXユーザのリストをUniform Resource Identifier（URI；ユニフォームリソース識別子）を使用(`vserver services name-service unix-user load-from-uri`してSVMにロードすることもできます。

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。

   ファイルには、次のUNIX形式でユーザ情報が含まれている必要があり `/etc/passwd`ます。

   ```
   user_name: password: user_ID: group_ID: full_name
   ```

   このコマンドを実行すると、フィールドの値とフィールド(*`home_directory`*の後のフィールドの値が *`full_name`*破棄され *`password`* *`shell`* ます）。

サポートされる最大ファイルサイズは 2.5MB 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。

   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、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから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、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

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}`

   `-overwrite{true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。

例

次のコマンドは、ローカルUNIXユーザのリストを、というURIを使用してvs1というSVM内にロードし`ftp://ftp.example.com/passwd`ます。URI を使用してロードした情報によって SVM 内の既存のユーザが上書きされることはありません。

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

ローカル**UNIX**グループを作成する

コマンドを使用すると、SVMに対してローカルなUNIXグループを作成できます `vserver services name-service unix-group create`。ローカル UNIX グループはローカル UNIX ユーザとともに使用されます。

ステップ

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`*

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

   `-id` *`integer`*`割り当てるグループ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
```

ローカル**UNIX**グループにユーザを追加する

コマンドを使用すると、SVMに対してローカルなUNIXグループにユーザを追加できます `vserver services name-service unix-group adduser`。

ステップ

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`*

`-name` `*group_name*`ユーザのプライマリグループに加えて、ユーザを追加するUNIXグループの名前を指定します。

例

次のコマンドは、 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します。

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

URIからローカル**UNIX**グループをロードする

個 々 のローカルUNIXグループを手動で作成する別の方法として、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）からSVMにロードすることができます `vserver services name-service unix-group load-from-uri`。

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。

   ファイルには、UNIX形式のグループ情報が含まれている必要があり `/etc/group`ます。

   `group_name: password: group_ID: comma_separated_list_of_users`

   このコマンドを実行すると、フィールドの値が破棄され `*password*`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。

   重複するエントリがリストに含まれていてはいけません。含まれていると、リストのロードに失敗します。SVMにすでにエントリがある場合は、パラメータをに `true`設定して既存のエントリをすべて新しいファイルで上書きするか、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ないようにする必要があります `-overwrite`。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから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、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

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}`

   `-overwrite true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。このパラメータをに指定する `true`と、ONTAPは、指定した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の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、というURIを使用してvs1というSVM内にロードし `ftp://ftp.example.com/group`ます。URI を使用してロードした情報によって SVM 内の既存のグループが上書きされることはありません。

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

ネットグループの使用

ネットグループの使用の概要

ネットグループは、ユーザ認証に使用したり、エクスポートポリシールールでクライアントを照合したりするために使用できます。外部ネームサーバ（LDAPまたはNIS）からネットグループへのアクセスを提供することも、コマンドを使用してUniform Resource Identifier（URI）からSVMへネットグループをロードすることもできます `vserver services name-service netgroup load`。

必要なもの

ネットグループを使用する前に、次の条件を満たしていることを確認する必要があります。

- ネットグループ内のすべてのホストは、ソース（NIS、LDAP、またはローカルファイル）に関係なく、フォワードおよびリバースDNSルックアップの一貫性を提供するために、フォワード（A）およびリバース（PTR）の両方のDNSレコードを持つ必要があります。

  さらに、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、それらのホスト名はすべてネットグループのメンバーであり、対応するAレコードを持っている必要があります。

- ソース（NIS、LDAP、またはローカルファイル）に関係なく、ネットグループ内のすべてのホストの名前のスペルが正しく、大文字と小文字が正しい必要があります。ネットグループで使用されているホスト名に大文字と小文字の不一致があると、予期しない動作（エクスポートチェックの失敗など）が発生する可能性があります。
- ネットグループに指定されているすべてのIPv6アドレスは、RFC 5952の指定に従って短縮および圧縮する必要があります。

  たとえば、 2011 ： hu9 ： 0 ： 0 ： 0 ： 0 ： 3 ： 1 は 2011 ： hu9 ： 3 ： 1 に短縮する必要があります。

タスクの内容

ネットグループについては次の処理を実行できます。

- 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 `vserver export-policy netgroup check-membership`。
- コマンドを使用すると、クライアントがネットグループの一部であるかどうかを確認できます `vserver services name-service getxxbyyy netgrp`。

  検索を実行するための基盤となるサービスは、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選択されます。

ネットグループを**SVM**にロードする

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 つは、ネットグループにリストされているホストを使用することです。ネットグループは、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代わりに、Uniform Resource Identifier（URI）を使用(`vserver services name-service netgroup load`してSVMにロードできます。

必要なもの

ネットグループファイルは、 SVM にロードする前に、次の要件を満たしている必要があります。

- ファイルは、 NIS の設定に使用されるのと同じ適切なネットグループテキストファイル形式を使用する必要があります。

  ONTAP は、ロードを行う前にネットグループテキストファイル形式をチェックします。ファイルにエラーが含まれている場合、ファイルはロードされず、ファイルで実行する必要のある修正を示すメッセージが表示されます。エラーを修正後に、ネットグループファイルを指定した SVM に再ロードできます。

- ネットグループファイル内のホスト名に含まれる英文字は、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 1000 です。
- ネットグループファイルでホスト名を定義する際に使用できるのは、プライマリ DNS ホスト名のみです。

  エクスポートへのアクセスに関する問題を回避するために、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。

- ネットグループファイル内の 3 つの値のうちユーザおよびドメインの部分は、 ONTAP でサポートされていないので空にしておく必要があります。

  ホスト / IP の部分のみがサポートされます。

タスクの内容

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したあと、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 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。

ステップ

1. URI から SVM にネットグループをロードします。

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

   ネットグループファイルのロードとnetgroup.byhostマップの構築には数分かかることがあります。

   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`http://intranet/downloads/corp-netgroup`ます。

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

ネットグループの定義のステータスを確認する

SVMにネットグループをロードしたら、コマンドを使用してネットグループの定義のステータスを確認できます `vserver services name-service netgroup status`。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た状態になっ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ステータスを確認します。

```
vserver services name-service netgroup status
```

追加情報をより詳細なビューで表示できます。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

権限レベルを設定したあと、次のコマンドを実行すると、すべての SVM のネットグループのステータスが表示されます。

```
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
```

NISドメイン設定を作成する

環境でNetwork Information Service（NIS；ネットワーク情報サービス）がネームサービスに使用されている場合は、コマンドを使用して、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`。

開始する前に

SVMにNISドメインを設定するには、設定済みのすべてのNISサーバが使用可能で到達可能である必要があり

ます。

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。この制限に従っていないNISサーバを指定しないでください。そうしないと、NISエントリに依存するクライアントアクセスが失敗する可能性があります。

タスクの内容

NISデータベースにマップが含まれている場合 `netgroup.byhost`、ONTAPはこのマップを使用して検索を高速化できます。 `netgroup.byhost`ディレクトリ内のマップと `netgroup`マップは、クライアントアクセスに関する問題を回避するために、常に同期されている必要があります。nis.7以降では、コマンドを使用してONTAP 9 `netgroup.byhost`エントリをキャッシュでき `vserver services name-service nis-domain netgroup-database`ます。

ホスト名解決にNISを使用することはサポートされていません。

手順

1. NISドメイン設定を作成します。

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   最大10台のNISサーバを指定できます。

   > ONTAP 9 .2以降では、 `-nis-servers`フィールドがフィールドに置き換わります `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

2. ドメインが作成されたことを確認します。

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

例

次のコマンドは、という名前のSVM上に、IPアドレスのNISサーバを使用して `192.0.2.180`、という名前の`vs1`NISドメインのNISドメイン設定を作成し `nisdomain`ます。

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

LDAPを使用

LDAPノシヨウホウホウノカイヨウ

現在の環境でLDAPがネームサービスに使用されている場合は、LDAP管理者と協力して要件と適切なストレージシステム構成を決定し、SVMをLDAPクライアントとして有効にする必要があります。

10.1以降では、チャネルバインドが**ONTAP 9**接続とネームサービス**LDAP**接続の両方でデフォルトでサポートされます。**ONTAP**は、**Start-TLS**または**LDAPS**が有効で、セッションセキュリティが署名または封印のいずれかに設定されている場合にのみ、**LDAP**接続でチャネルバインディングを試行します。ネームサーバとの**LDAP**チャネルバイ

ンドを無効または再度有効にするには、コマンドでパラメータを `**ldap client modify**`使用し `**-try-channel-binding**`ます。

詳細については、を参照してください "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"。

- ONTAP用にLDAPを設定する前に、サイト環境がLDAPサーバとクライアントの設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAPサーバのドメイン名がLDAPクライアントのエントリと一致している必要があります。
  - LDAPサーバでサポートされるLDAPユーザパスワードのハッシュタイプには、ONTAPでサポートされるハッシュタイプが含まれている必要があります。
    - Crypt（すべてのタイプ）およびSHA-1（SHA、SSHA）。
    - ONTAP 9 .8以降では、SHA-2ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384、およびSSHA-512）もサポートされます。
  - LDAPサーバでセッションセキュリティ対策が必要な場合は、LDAPクライアントで設定する必要があります。

    次のセッションセキュリティオプションを使用できます。

    - LDAP署名（データ整合性チェックを提供）およびLDAP署名と封印（データ整合性チェックと暗号化を提供）
    - START TLS
    - LDAPS （ LDAP over TLS または SSL ）
  - 署名および封印されたLDAPクエリを有効にするには、次のサービスを設定する必要があります。
    - LDAPサーバは、GSSAPI（Kerberos）SASLメカニズムをサポートしている必要があります。
    - LDAPサーバには、DNS A/AAAAレコードと、DNSサーバで設定されたPTRレコードが必要です。
    - Kerberosサーバには、DNSサーバ上にSRVレコードが存在する必要があります。
  - START TLSまたはLDAPSを有効にするには、次の点を考慮する必要があります。
    - NetAppでは、LDAPSではなくStart TLSを使用することを推奨します。
    - LDAPSを使用する場合は、ONTAP 9 .5以降で、TLSまたはSSLに対してLDAPサーバが有効になっている必要があります。ONTAP 9ではSSLはサポートされていません。0-9.4
    - 証明書サーバがドメインで設定済みである必要があります。
  - LDAPリファーラル追跡を有効にするには（ONTAP 9 .5以降で）、次の条件を満たす必要があります。
    - 両方のドメインに次のいずれかの信頼関係を設定する必要があります。
      - 双方向
      - 一方向（プライマリがリファーラルドメインを信頼する場合）
      - 親子
    - 参照されるすべてのサーバ名を解決するようにDNSを設定する必要があります。
    - bind-as-cifs-server が true に設定されている場合、認証には両ドメインのパスワードが同じであることが必要です。

次の設定はLDAPリファーラル追跡ではサポートされていません。

- すべてのONTAPバージョン：
  - 管理 SVM 上の LDAP クライアント
- ONTAP 9.8 以前では（ 9.9.1 以降でサポートされています）：
  - LDAPの署名と封印（ `-session-security`オプション）
  - 暗号化されたTLS接続（ `-use-start-tls`オプション）
  - LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap`オプション）

- SVMでLDAPクライアントを設定するときは、LDAPスキーマを入力する必要があります。

  ほとんどの場合、デフォルトのONTAPスキーマのいずれかが適切です。ただし、環境で使用するLDAPスキーマがこれらと異なる場合は、LDAPクライアントを作成する前に、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。環境の要件については、LDAP管理者にお問い合わせください。

- ホスト名解決にLDAPを使用することはサポートされていません。

詳細情報

- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"
- "自己署名ルートCA証明書をSVMにインストールする"

新しい**LDAP**クライアントスキーマを作成する

環境で使用するLDAPスキーマがONTAPのデフォルトと異なる場合は、LDAPクライアント設定を作成する前に、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。

タスクの内容

ほとんどのLDAPサーバでは、ONTAPが提供するデフォルトスキーマを使用できます。

- MS-AD-BIS（Windows Server 2012以降のほとんどのADサーバで推奨されるスキーマ）
- AD-IDMU（Windows 2008、Windows Server 2012、およびそれ以降のADサーバ）
- AD-SFU（Windows 2003以前のADサーバ）
- RFC-2307（UNIX LDAPサーバ）

デフォルト以外のLDAPスキーマを使用する必要がある場合は、LDAPクライアント設定を作成する前にスキーマを作成する必要があります。新しいスキーマを作成する前に、LDAP管理者に問い合わせてください。

ONTAPが提供するデフォルトの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、それに応じてコピーを変更します。

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. 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。

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

5. admin権限レベルに戻ります。

```
set -privilege admin
```

LDAPクライアント設定を作成する

環境内の外部LDAPサービスまたはActive DirectoryサービスにONTAPからアクセスする場合は、まずストレージシステム上にLDAPクライアントを設定する必要があります。

必要なもの

Active Directoryドメイン解決リストの最初の3つのサーバのいずれかが稼働し、データを提供している必要があります。そうしないと、このタスクは失敗します。

複数のサーバがあり、そのうちどの時点でも3台以上のサーバがダウンしています。

手順

1. LDAP管理者に問い合わせて、このコマンドの適切な設定値を確認し `vserver services name-service ldap client create`ます。

   a. LDAPサーバへのドメインベースまたはアドレスベースの接続を指定します。

   `-ad-domain`オプションと `-servers`オプションを同時に指定することはできません。

   - オプションを使用し `-ad-domain`て、Active DirectoryドメインでLDAPサーバ検出を有効にします。
     - オプションを使用すると `-restrict-discovery-to-site`、LDAPサーバ検出を、指定したドメインのCIFSデフォルトサイトに制限できます。このオプションを使用する場合は、でCIFSのデフォルトサイトを指定する必要もあり `-default-site`ます。
   - オプションを使用すると、優先されるActive Directoryサーバをカンマで区切ってIPアドレスで指定できます `-preferred-ad-servers`。クライアントが作成されたら、コマンドを使用してこのリストを変更できます `vserver services name-service ldap client modify`。

- オプションを使用する `-servers`と、1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）をIPアドレスでカンマで区切って指定できます。

> `-servers`オプションはONTAP 9で廃止されました。2.ONTAP 9.2以降では、 `-ldap-servers`フィールドがフィールドに置き換わります `-servers`。このフィールドには、LDAPサーバのホスト名またはIPアドレスを指定できます。

b. デフォルトまたはカスタムのLDAPスキーマを指定します。

ほとんどのLDAPサーバでは、ONTAPが提供するデフォルトの読み取り専用スキーマを使用できます。他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。他のスキーマを使用する場合は、デフォルトのスキーマ（読み取り専用）をコピーし、コピーを変更することによって、独自のスキーマを作成できます。

デフォルトのスキーマ：

- MS-AD-BIS

  RFC-2307bisに基づいて、Windows Server 2012以降のほとんどの標準的なLDAP環境で推奨されるLDAPスキーマです。

- AD-IDMU

  Active Directory Identity Management for UNIXに基づいて、このスキーマはWindows 2008、Windows 2012、およびそれ以降のほとんどのADサーバに適しています。

- AD-SFU

  Active Directory Services for UNIXに基づいて、このスキーマはWindows 2003以前のほとんどのADサーバに適しています。

- RFC-2307

  RFC-2307 （ネットワーク情報サービスとして LDAP を使用するためのアプローチ）に基づいて、このスキーマはほとんどの UNIX AD サーバに適しています。

c. バインド値を選択します。

- `-min-bind-level {anonymous|simple|sasl}`最小バインド認証レベルを指定します。

  デフォルト値はです **anonymous**。

- `-bind-dn *LDAP_DN*`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する必要があります。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する必要があります。

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

d. 必要に応じて、セッションセキュリティオプションを選択します。

LDAPの署名と封印、またはLDAP over TLS（LDAPサーバで必要な場合）を有効にすることができます。

- `--session-security {none|sign|seal}`

  署名(`sign`、データ整合性）、署名と封印(`seal`、データの整合性と暗号化を有効にすることができます。また、 `none`署名と封印のどちらも有効にしないことも可能です。デフォルト値はです `none`。

  {`sasl`バインド認証をにフォールバックする場合、または `**simple**`署名と封印のバインドが失敗した場合以外は、} `**anonymous**`も設定する必要があります `-min-bind-level`。

- `-use-start-tls{true|false}`

  に設定し、LDAPサーバでサポートされている場合、 **`true`**`LDAP`クライアントはサーバへの暗号化された`TLS`接続を使用します。デフォルト値はです **`false`**。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。

> Storage VMにSMBサーバがドメインに追加されていて、LDAPサーバがSMBサーバのホームドメインのドメインコントローラの1つである場合は、コマンドを使用してオプションを `vserver cifs security modify`変更できます `-session-security-for-ad-ldap`。

e. ポート、クエリ、およびベースの値を選択します。

デフォルト値を推奨しますが、実際の環境に適しているかどうかをLDAP管理者に確認する必要があります。

- `-port *port*`LDAPサーバポートを指定します。

  デフォルト値はです `389`。

Start TLSを使用してLDAP接続を保護する場合は、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TLS接続にアップグレードされます。ポートを変更すると、Start TLSが失敗します。

- `-query-timeout *integer*`クエリータイムアウトを秒単位で指定します。

  指定できる範囲は1～10秒です。デフォルト値は秒です `3`。

- `-base-dn *LDAP_DN*`ベースDNを指定します。

  必要に応じて複数の値を入力できます（LDAPリファーラル追跡が有効な場合など）。デフォルト値は（root）です `""`。

- `-base-scope{base|onelevel|subtree}` は、ベース検索範囲を指定します。

  デフォルト値はです `subtree`。

- `-referral-enabled{true|false}` LDAPリファーラル追跡を有効にするかどうかを指定しま

す。

ONTAP 9 .5以降では、必要なレコードが参照先のLDAPサーバに存在することを示すLDAPリファーラル応答がプライマリLDAPサーバから返された場合に、ONTAP LDAPクライアントが他のLDAPサーバへのルックアップ要求を参照できるようになりました。デフォルト値はです **false**。

参照されたLDAPサーバに存在するレコードを検索するには、参照されたレコードのベースDNをLDAPクライアント設定の一部としてベースDNに追加する必要があります。

2. Storage VMに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 -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

LDAPクライアント設定を作成するときは、Storage VM名を指定する必要があります。

3. 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、Storage VM 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 -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
```

次のコマンドでは、署名と封印が必要なLDAPのActive Directoryサーバと連携するために、Storage VM 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。また、LDAPサーバ検出は指定したドメインの特定サイトに制限されます。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

次のコマンドでは、LDAPリファーラル追跡が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1に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 -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

次のコマンドでは、ベースDNを指定することで、Storage VM 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
```

次のコマンドでは、リファーラル追跡を有効にすることで、Storage VM vs1の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 "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

LDAPクライアント設定を**SVM**に関連付ける

SVMでLDAPを有効にするには、コマンドを使用してLDAPクライアント設定をSVMに関連付ける必要があります `vserver services name-service ldap create`。

必要なもの

- LDAPドメインがネットワーク内にすでに存在し、SVMが配置されているクラスタからアクセスできる必要があります。
- 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
   ```

   ONTAP 9 .2以降では `vserver services name-service ldap create`、コマンドによって設定の自動検証が実行され、ONTAPがネームサーバに接続できない場合はエラーメッセージが報告されます。

   次のコマンドは、「vs1」SVMでLDAPを有効にし、「ldap1」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
```

2. vserver services name-service ldap checkコマンドを使用して、ネームサーバのステータスを検証します。

次のコマンドは、SVM vs1のLDAPサーバを検証します。

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

ネーム サービスのチェック コマンドはONTAP 9.2以降で使用できます。

ネームサービススイッチテーブルで**LDAP**ソースを確認

ネームサービスのLDAPソースがSVMのネームサービススイッチテーブルに正しく表示されていることを確認する必要があります。

手順

1. 現在のネームサービススイッチテーブルの内容を表示します。

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

次のコマンドは、 SVM My_SVM の結果を表示します。

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
My_SVM          hosts          files,
                               dns
My_SVM          group          files,ldap
My_SVM          passwd         files,ldap
My_SVM          netgroup       files
My_SVM          namemap        files
5 entries were displayed.
```

`namemap`ネームマッピング情報を検索する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。

2. 必要に応じてエントリを更新し `ns-switch`ます。

ns-switch エントリの更新対象	入力するコマンド
ユーザ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
グループ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
ネットグループ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

NFSでKerberosを使用してセキュリティを強化

NFSでのKerberos使用によるセキュリティ強化の概要

ご使用の環境でKerberosが強力な認証に使用されている場合は、Kerberos管理者と協力して要件および適切なストレージシステム構成を決定し、SVMをKerberosクライアントとして有効にする必要があります。

環境が次のガイドラインを満たしている必要があります。

- ONTAP で Kerberos を設定するには、 Kerberos のサーバとクライアントの設定に適したベストプラクティスに従ってサイトが導入されている必要があります。
- Kerberos 認証を必須とする場合は、可能であれば NFSv4 以降を使用します。

  NFSv3 でも Kerberos を使用できますが、Kerberos の高度なセキュリティ機能をフルに活用するには、ONTAP を NFSv4 以降に導入する必要があります。

- サーバアクセスの冗長化を促すため、同じ SPN を使ってクラスタ内の複数のノードのデータ LIF で Kerberos を有効にする必要があります。
- Kerberos を SVM で有効にする場合は、 NFS クライアントの設定に応じて、次のいずれかのセキュリティ方式をボリュームまたは qtree のエクスポートルールに指定する必要があります。
  - `krb5`（Kerberos v5プロトコル）
  - `krb5i`（Kerberos v5プロトコルとチェックサムによる整合性チェック）
  - `krb5p`（Kerberos v5プロトコルとプライバシーサービス）

Kerberos のサーバとクライアントのほかに、次の外部サービスを Kerberos を使用する ONTAP 用に設定する必要があります。

- ディレクトリサービス

  Active Directory や OpenLDAP などの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 を使用するように設定してください。NIS を使用すると、要求がクリアテキストで送信されセキュアではないため、 NIS は使用しないでください。

- NTP

  NTPを実行している稼働中のタイムサーバが必要です。これは、時間のずれによるKerberos認証の失敗を防ぐために必要です。

- ドメイン名解決（DNS）

  各UNIXクライアントおよび各SVM LIFについて、KDCのフォワードルックアップゾーンとリバースルックアップ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。すべての参加者は、DNSを介して適切に解決できる必要があります。

Kerberos設定の権限の確認

Kerberos では、特定の UNIX 権限が SVM ルートボリューム用およびローカルのユーザおよびグループ用に設定されている必要があります。

手順

1. SVM ルートボリュームについて、関連する権限を表示します。

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   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
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	755

   これらの値が表示されない場合は、コマンドを使用し `volume modify`て更新します。

2. ローカル UNIX ユーザを表示します。

   `vserver services name-service unix-user show -vserver vserver_name`

   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。 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。
root	0	0	マウントに必要。

これらの値が表示されていない場合は、コマンドを使用して更新できます `vserver services name-service unix-user modify`。

3. ローカル UNIX グループを表示します。

   `vserver services name-service unix-group show -vserver vserver _name`

   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
デーモン	1
root	0

これらの値が表示されていない場合は、コマンドを使用して更新できます `vserver services name-service unix-group modify`。

NFS Kerberos Realmの設定を作成します。

環境で ONTAP から外部 Kerberos サーバにアクセスする場合は、まず既存の Kerberos Realm を使用するように SVM を設定する必要があります。そのためには、Kerberos KDCサーバの設定値を収集し、コマンドを使用してSVMにKerberos Realm設定を作成する必要があり `vserver nfs kerberos realm create`ます。

必要なもの

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の時間差（クロックスキュー）は、認証エラーの一般的な原因です。

手順

1. Kerberos管理者に問い合わせて、コマンドで指定する適切な設定値を決定し `vserver nfs kerberos realm create`ます。
2. SVM で Kerberos Realm の設定を作成します。

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. Kerberos Realmの設定が正常に作成されたことを確認します。

   ```
   vserver nfs kerberos realm show
   ```

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"
```

NFS Kerberosで許可される暗号化タイプの設定

デフォルトでは、 ONTAP は、 DES 、 3DES 、 AES-128 、および AES-256 の暗号化タイプをサポートします。コマンドでパラメータを指定する `-permitted-enc -types`と、SVMごとに許可される暗号化タイプを、特定の環境のセキュリティ要件に合わせて設定できます `vserver nfs modify`。

タスクの内容

クライアントの互換性を最大限に高めるために、ONTAPはデフォルトで弱いDES暗号化と強いAES暗号化の両方をサポートしています。つまり、たとえば、セキュリティを強化する必要があり、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、クライアントにAES暗号化のみの使用を要求できます。

使用可能な最も強力な暗号化を使用する必要があります。ONTAP の場合は AES-256 です。この暗号化レベルが環境でサポートされていることを、 KDC 管理者に確認する必要があります。

- SVMでAES全体（AES-128とAES-256の両方）を有効または無効にすると、システムが停止します。元のDESプリンシパル/ keytabファイルが削除され、SVMのすべてのLIFでKerberos設定を無効にする必要があるためです。

  この変更を行う前に、SVMでNFSクライアントがAES暗号化を使用していないことを確認する必要があります。

- 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。

ステップ

1. 許可されている暗号化タイプを有効または無効にします。

有効または無効にする対象	実行する手順
DES または 3DES	a. SVMのNFS Kerberosで許可されている暗号化タイプを設定します。+ `vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types` 暗号化タイプが複数ある場合はカンマで区切ります。 b. 変更が成功したことを確認します。+ `vserver nfs show -vserver vserver_name -fields permitted-enc-types`

有効または無効にする対象	実行する手順

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. 変更対象のNFS Kerberosで許可されている暗号化タイプが設定されている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で許可されている暗号化タイプを設定します。+
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	暗号化タイプが複数ある場合はカンマで区切ります。
	d. 変更が成功し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を再度有効にします。+
	`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`

データ**LIF**で**Kerberos**を有効にする

コマンドを使用すると、データLIFでKerberosを有効にできます `vserver nfs kerberos interface enable`。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。

タスクの内容

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。

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
```

ONTAP で Kerberos インターフェイスを有効にするには、 KDC の SPN 用のシークレットキーが必要です。

Microsoft KDC の場合、 KDC に接続があると、シークレットキーを取得するためのユーザ名とパスワードのプロンプトが CLI で発行されます。Kerberos Realmの別のOUでSPNを作成する必要がある場合は、オプションのパラメータを指定できます `-ou`。

Microsoft 以外の KDC の場合は、次の 2 つのうちいずれかの方法を使用してシークレットキーを取得できます。

状況	コマンドとともに含める必要のあるパラメータ
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必要です	`-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

2. LIFでKerberosが有効になったことを確認します。

   `vserver nfs kerberos-config show`

3. 複数の LIF で Kerberos を有効にするには、手順 1 と 2 を繰り返します。

例

次のコマンドは、 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、 ves03-d1 という論理インターフェイス ves03-d1 に対して作成して検証します。

```
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"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- ------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

NFSでTLSを使用したセキュリティ強化

NFSでのTLSを使用したセキュリティ強化の概要

TLSを使用すると、暗号化されたネットワーク通信をKerberosやIPsecと同等のセキュリ

ティで実現でき、複雑さも軽減されます。管理者は、System Manager、ONTAP CLI、またはONTAP REST APIを使用して、NFSv3およびNFSv4.x接続でのセキュリティを強化するためのTLSの有効化、設定、および無効化を行うことができます。

> ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

ONTAPでは、TLS経由のNFS接続にTLS 1.3が使用されます。

要件

NFS over TLSにはX.509証明書が必要です。CA署名済みサーバ証明書を作成してONTAPクラスタにインストールするか、NFSサービスが直接使用する証明書をインストールできます。証明書は次のガイドラインに従っている必要があります。

- 各証明書の共通名（CN）には、TLSを有効にするデータLIFのFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を設定する必要があります。
- 各証明書のサブジェクト代替名（SAN）に、TLSを有効にするデータLIFのIPアドレスを設定する必要があります。必要に応じて、データLIFのIPアドレスとFQDNの両方を使用してSANを設定できます。IPアドレスとFQDNの両方が設定されている場合、NFSクライアントはIPアドレスまたはFQDNを使用して接続できます。
- 同じLIFに複数のNFSサービス証明書をインストールすることができますが、NFS TLS設定で一度に使用できるのはそのうちの1つだけです。

ONTAPでの**NFS**クライアントに対する**TLS**の有効化または無効化

NFSクライアント用のデータLIFでTLSを有効または無効にすることができます。NFS over TLSを有効にすると、SVMはTLSを使用して、ネットワーク経由でNFSクライアントとONTAPの間で送信されるすべてのデータを暗号化します。これにより、NFS接続のセキュリティが向上します。

> ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

TLSを有効にする

NFSクライアントに対してTLS暗号化を有効にすると、転送中のデータのセキュリティを強化できます。

開始する前に

- 作業を開始する前に、『for NFS over TLS』を参照してください"要件"。
- コマンドの詳細については "SVM NFS TLSインターフェイス有効"、ONTAPコマンドリファレンスを参照してください。

手順

1. TLSを有効にするStorage VMと論理インターフェイス（LIF）を選択してください。

2. そのStorage VMおよびインターフェイスのNFS接続に対してTLSを有効にします。括弧<>の値は、環境の情報で置き換えます。

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. コマンドを使用し `vserver nfs tls interface show`て結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、Storage VMのLIF `vs1`でNFS over TLSを有効にし `data1`ます。

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address          TLS Status TLS Certificate
Name
-------------- ------------- ---------------- ----------
-----------------------
vs1            data1         10.0.1.1         enabled    cert_vs1
vs2            data2         10.0.1.2         disabled   -
2 entries were displayed.
```

TLSの無効化

転送中データのセキュリティ強化が必要なくなった場合は、NFSクライアントのTLSを無効にできます。

NFS over TLSを無効にすると、NFS接続に使用されているTLS証明書が削除されます。今後NFS over TLSを有効にする必要がある場合は、有効化時に証明書名を再度指定する必要があります。

開始する前に

コマンドの詳細については "SVM NFS TLSインターフェイスの無効化"、ONTAPコマンドリファレンスを参照してください。

手順

1. TLSを無効にするStorage VMと論理インターフェイス（LIF）を選択してください。

2. そのStorage VMおよびインターフェイスのNFS接続に対するTLSを無効にします。括弧<>の値は、環境の情報で置き換えます。

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. コマンドを使用し `vserver nfs tls interface show`て結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、Storage VMのLIF `vs1`でNFS over TLSを無効にし `data1`ます。

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address          TLS Status TLS Certificate
Name
-------------- ------------- ---------------- ----------
------------------------
vs1            data1         10.0.1.1         disabled   -
vs2            data2         10.0.1.2         disabled   -
2 entries were displayed.
```

TLS設定の編集

既存のNFS over TLS設定を変更できます。たとえば、この手順を使用してTLS証明書を更新できます。

開始する前に

コマンドの詳細については "vserver nfs tls interface modify"、ONTAPコマンドリファレンスを参照してください。

手順

1. NFSクライアントのTLS設定を変更するStorage VMと論理インターフェイス（LIF）を選択してください。
2. 設定を変更します。を指定する場合は `status enable`、パラメータも指定する必要があり `certificate-name`ます。括弧<>の値は、環境の情報で置き換えます。

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. コマンドを使用し `vserver nfs tls interface show`て結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、Storage VMのLIFの `vs2`NFS over TLSの設定を変更します `data2。

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address          TLS Status TLS Certificate
Name
-------------- ------------- ---------------- ----------
-----------------------
vs1            data1         10.0.1.1         disabled   -
vs2            data2         10.0.1.2         enabled    new_cert
2 entries were displayed.
```

NFS対応SVMにストレージ容量を追加する

NFS対応SVMへのストレージ容量の追加の概要

NFS 対応 SVM にストレージ容量を追加するには、ストレージコンテナを提供するボリュームまたは qtree を作成し、そのコンテナのエクスポートポリシーを作成または変更する必要があります。その後、クラスタからの NFS クライアントアクセスを確認し、クライアントシステムからのアクセスをテストできます。

必要なもの

- SVMでNFSの設定が完了している必要があります。
- SVM 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に、すべてのクライアントへのアクセスを許可するルールが含まれている必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Kerberos 設定への追加または変更が完了している必要があります。

エクスポートポリシーを作成する

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。エクスポートポリシーは、コマンドを使用して作成できます `vserver export-policy create`。

手順

1. エクスポートポリシーを作成します。

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

   ポリシー名の最大文字数は256文字です。

2. エクスポートポリシーが作成されたことを確認します。

   ```
   vserver export-policy show -policyname policy_name
   ```

例

次のコマンドは、 vs1 という SVM で、 exp1 という名前のエクスポートポリシーを作成し、作成を確認します。

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

エクスポートポリシーにルールを追加する

エクスポートポリシーにルールがないと、クライアントはデータにアクセスできません。新しいエクスポートルールを作成するには、クライアントを特定してクライアント照合形式を選択し、アクセスとセキュリティのタイプを選択し、匿名ユーザIDマッピングを指定し、ルールインデックス番号を選択して、アクセスプロトコルを選択する必要があります。その後、コマンドを使用して、新しいルールをエクスポートポリシーに追加できます `vserver export-policy rule create`。

必要なもの

- 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。
- データ SVM で DNS が正しく設定されている必要があり、 DNS サーバに NFS クライアント用の正しいエントリが存在する必要があります。

  その理由は、特定のクライアント照合形式で 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することと、エクスポートポリシールールの照合が失敗するとクライアントがデータにアクセスできなくなる可能性があることです。

- Kerberosで認証する場合は、NFSクライアントで次のいずれのセキュリティ方式が使用されているかを確認しておく必要があります。
  - `krb5`（Kerberos v5プロトコル）
  - `krb5i`（Kerberos v5プロトコルとチェックサムによる整合性チェック）
  - `krb5p`（Kerberos v5プロトコルとプライバシーサービス）

タスクの内容

エクスポートポリシーの既存のルールがクライアント一致とアクセスの要件を満たしている場合は、新しいルールを作成する必要はありません。

Kerberosで認証する場合に、SVMのすべてのボリュームにKerberos経由でアクセスできる場合は `-superuser`、 `krb5i`ルートボリュームのエクスポートルールオプション、 `-rwrule`、、を、または `krb5p`に `krb5`設定できます `-rorule`。

手順

1. 新しいルールのクライアントとクライアント照合形式を特定します。

   オプションは `-clientmatch`、ルールを適用するクライアントを指定します。クライアント一致の値は1つまたは複数指定できます。複数の値を指定する場合はカンマで区切る必要があります。次のいずれかの形式で指定できます。

クライアント照合形式	例
先頭に文字が付いたドメイン名	`.example.com`または `.example.com,.example.net,...`
ホスト名	`host1`または `host1,host2, ...`
IPv4アドレス	`10.1.12.24`または `10.1.12.24,10.1.12.25, ...`
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`または `10.1.12.10/4,10.1.12.11/4,...`
IPv4アドレスとネットワークマスク	`10.1.16.0/255.255.255.0`または `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
ドット付き形式のIPv6アドレス	`::1.2.3.4`または `::1.2.3.4,::1.2.3.5,...`
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`または `ff::00/32,ff::01/32,...`
先頭に@文字が付いた単一のネットグループ	`@netgroup1`または `@netgroup1,@netgroup2,...`

クライアント定義のタイプを組み合わせることもできます（例：） `.example.com,@netgroup1`。

IPアドレスを指定する場合は、次の点に注意してください。

- 10.1.12.10-10.1.12.70などのIPアドレス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。

- クライアントアクセスのきめ細かな管理のためにエクスポートルールで個々の IP アドレスを指定する際には、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。

  そうしないと、IPアドレスが変更されると、クライアントはアクセスを失います。

- 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。

2. クライアント一致のアクセスタイプとセキュリティタイプを選択します。

   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は、次のアクセスモードを1つ以上指定できます。

   - `-rorule`（読み取り専用アクセス）
   - `-rwrule`（読み取り/書き込みアクセス）
   - `-superuser`（ルートアクセス）

   > ⓘ 特定のセキュリティタイプの読み取り/書き込みアクセスは、エクスポートルールでそのセキュリティタイプの読み取り専用アクセスも許可されている場合にのみ許可されます。読み取り専用パラメータで読み取り/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すると、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。スーパーユーザアクセスについても同様です。

   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またはを `never`指定する場合は `any`、他のセキュリティタイプは指定しないでください。次の有効なセキュリティタイプから選択します。

セキュリティタイプの設定	一致するクライアントからエクスポートされたデータへのアクセス
`any`	受信セキュリティタイプに関係なく、常に。
`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すると、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`	受信セキュリティタイプに関係なく、なし。

セキュリティタイプの設定	一致するクライアントからエクスポートされたデータへのアクセス
krb5	Kerberos 5によって認証されます。認証のみ：各要求および応答のヘッダーが署名されます。
krb5i	Kerberos 5iによって認証されます。認証および整合性：各要求および応答のヘッダーと本文が署名されます。
krb5p	Kerberos 5pによって認証されます。認証、整合性、およびプライバシー：各要求および応答のヘッダーと本文が署名され、 NFS データペイロードが暗号化されます。
ntlm	CIFS NTLMによって認証されます。
sys	NFS AUTH_SYSで認証されます。

推奨されるセキュリティタイプは sys、または（Kerberosを使用する場合） krb5、、 krb5i、、または `krb5p`です。

NFSv3でKerberosを使用している場合は -rwrule、に加えて krb5`エクスポートポリシールールでアクセスを `sys`許可する必要があります `-rorule。これは、Network Lock Manager（NLM）によるエクスポートへのアクセスを許可する必要があるためです。

3. 匿名ユーザIDマッピングを指定します。

`-anon`オプションは、ユーザIDが0（ゼロ）で到着するクライアント要求にマッピングされる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に関連付けられています。デフォルト値はです `65534`。NFS クライアントは通常、ユーザ ID 65534 をユーザ名 nobody と関連付けます（ _root squashing_ ） 。ONTAPでは、このユーザIDはユーザ pcuser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無効にするには、の値を指定し `65535`ます。

4. ルールインデックスの順序を選択します。

オプションは -ruleindex、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内の順序に従って評価され、インデックス番号が小さいルールが最初に評価されます。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。

追加対象	そしたら...。
エクスポートポリシーへの最初のルール	と入力し `1`ます。

追加対象	そしたら...。
追加のルールをエクスポートポリシーに	a. ポリシー内の既存のルールを表示します。+ `vserver export-policy rule show -instance -policyname your_policy` b. 評価する順序に応じて、新しいルールのインデックス番号を選択します。

5. 該当するNFSアクセス値を選択します{nfs|nfs3|nfs4：}。

   nfs`任意のバージョンに一致し `nfs3、 `nfs4`特定のバージョンだけに一致します。

6. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. エクスポートポリシーのルールを表示して、新しいルールが存在することを確認します。

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   このコマンドは、エクスポートポリシーに適用されているルールのリストを含む、エクスポートポリシーの概要を表示します。ONTAPは、各ルールにルールインデックス番号を割り当てます。ルールインデックス番号を確認したら、その番号を使用して、指定したエクスポートルールに関する詳細情報を表示できます。

8. エクスポートポリシーに適用されたルールが正しく設定されていることを確認します。

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

例

次のコマンドは、 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し、作成を確認します。このルールのインデックス番号は1です。このルールは、ドメインeng.company.comおよびネットグループ@netgroup1内のすべてのクライアントに一致します。このルールは、すべてのNFSアクセスを有効にします。AUTH_SYSで認証されたユーザに対する読み取り専用アクセスと読み取り/書き込みアクセスを有効にします。UNIXユーザIDが0（ゼロ）のクライアントは、Kerberosで認証されないかぎり匿名化されます。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

次のコマンドは、 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し、作成を確認します。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。このルールは、すべてのNFSアクセスを有効にします。AUTH_SYSで認証されたユーザの読み取り専用アクセスを有効にし、読み取り/書き込みアクセスとrootアクセスにはKerberos認証を必要とします。UNIXユーザIDが0（ゼロ）のクライアントは、Kerberos以外で認証されないかぎり、ルートアクセスを拒否されます。

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                  Vserver: vs2
                              Policy Name: expol2
                               Rule Index: 21
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                           @dev_netgroup_main
                            RO Access Rule: sys
                            RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

ボリュームまたは**qtree**のストレージコンテナを作成する

ボリュームの作成

コマンドを使用すると、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create`。

タスクの内容

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームの作成時に指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、コマンドを使用して、SVMネームスペースでボリュームを_mount_theにする必要があります `volume mount`。

開始する前に

- NFSがセットアップされ、実行されている必要があります。
- SVMのセキュリティ形式がUNIXである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する

`volume create`か、 `-activity-tracking-state`に設定します `on。

容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。

手順

1. ジャンクションポイントを設定してボリュームを作成します。

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path [-policy
   export_policy_name]
   ```

   の選択肢は `-junction-path`次のとおりです。

   - ルートの直下。例： */new_vol*

     新しいボリュームを作成し、 SVM のルートボリュームに直接マウントされるように指定することができます。

   - 既存のディレクトリの下（例： */existing_dir/new_vol*

     新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

     たとえば、新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は */new_dir/new_vol*、SVMのルートボリュームにジャンクションされている新しい親ボリュームを最初に作成する必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

   + 既存のエクスポートポリシーを使用する場合は、ボリュームの作成時に指定できます。エクスポートポリシーは、あとからコマンドを使用して追加することもできます `volume modify`。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

   ```
   volume show -vserver svm_name -volume volume_name -junction
   ```

例

次のコマンドは、 SVM vs1.example.com およびアグリゲート aggr1 上に、 users1 という名前の新しいボリュームを作成します。新しいボリュームは、で使用でき `/users`ます。ボリュームのサイズは750GBで、ボリュームギャランティのタイプはvolume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

次のコマンドは、SVM「vs1.example.com」とアグリゲート「aggr1」に「home4」という名前の新しいボリュームを作成します。ディレクトリは /eng/`vs1 SVMのネームスペース内にすでに存在し、新しいボリュームがで使用可能になります `/eng/home。これがネームスペースのホームディレクトリになります。/eng/`ボリュームのサイズは750GBで、ボリュームギャランティのタイプは（デフォルト）です `volume。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

qtreeを作成する

コマンドを使用すると、データを含むqtreeを作成し、そのプロパティを指定できます volume qtree create。

必要なもの

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVMのセキュリティ形式がUNIXで、NFSが設定されて実行されている必要があります。

手順

1. qtree を作成します。

   ```
   volume qtree create -vserver vserver_name { -volume volume_name -qtree
   qtree_name | -qtree-path qtree path } -security-style unix [-policy
   export_policy_name]
   ```

   ボリュームとqtreeを別 々 の引数として指定するか、の形式でqtreeパスの引数を指定できます /vol/volume_name/_qtree_name。

デフォルトでは、 qtree は親ボリュームのエクスポートポリシーを継承しますが、独自のものを使用するように設定することもできます。既存のエクスポートポリシーを使用する場合は、 qtree の作成時にポリシーを指定できます。エクスポートポリシーは、あとからコマンドを使用して追加することもできます `volume qtree modify`。

2. qtree が必要なジャンクションパスで作成されたことを確認します。

   ```
   volume qtree show -vserver vserver_name { -volume volume_name -qtree
   qtree_name | -qtree-path qtree path }
   ```

例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成し`/vol/data1`ます。

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

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と、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できます。新しいストレージをプロビジョニングする際に、既存のポリシーとルールを使用するか、既存のポリシーにルールを追加するか、新しいポリシーとルールを作成できます。エクスポートポリシーの設定も確認できます。

ONTAP 9 .3以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にして、すべてのルール違反をエラールールリストに記録できます。 `vserver export-policy config-checker`コマンドはチェッカーを呼び出して結果を表示します。この結果を使用して、設定を検証し、エラーのあるルールをポリシーから削除できます。このコマンドで検証されるのは、ホスト名、ネットグループ、匿名ユーザのエクスポート設定のみです。

エクスポートルールの処理順序を管理します。

コマンドを使用すると、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できます `vserver export-policy rule setindex`。これにより、 ONTAP がクライアント要求に対してエクスポートルールを適用する優先順位を指定できます。

タスクの内容

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、指定した場所にルールが挿入され、それに応じてリストの順序が変更されます。

ステップ

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します。

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

例

次のコマンドは、 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 に変更します。

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

ボリュームへのエクスポートポリシーの割り当て

SVM内の各ボリュームには、クライアントがボリューム内のデータに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。

タスクの内容

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 つのボリュームに関連付けることができるのは 1 つのエクスポートポリシーだけですが、 1 つのポリシーを多数のボリュームに関連付けることができます。

手順

1. ボリュームの作成時にエクスポートポリシーを指定しなかった場合は、ボリュームにエクスポートポリシーを割り当てます。

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. ポリシーがボリュームに割り当てられたことを確認します。

```
volume show -volume volume_name -fields policy
```

例

次のコマンドは、エクスポートポリシー nfs_policy を vs1 という SVM 上のボリューム vol1 に割り当てて、割り当てを確認します。

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

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 の変更によって行うこともできます。

必要なもの

エクスポートポリシーが存在している必要があります。

タスクの内容

qtree では、作成時に指定しなかった場合、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継承されます。

エクスポートポリシーは、 qtree の作成時、または qtree の作成後にいつでも、 qtree に関連付けることができます。1 つの qtree に関連付けることができるのは 1 つのエクスポートポリシーだけですが、 1 つのポリシーを多数の qtree と関連付けることができます。

手順

1. qtree の作成時にエクスポートポリシーを指定しなかった場合は、 qtree にエクスポートポリシーを割り当てます。

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. ポリシーが qtree に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、エクスポートポリシー nfs_policy を vs1 という SVM 上の qtree qt1 に割り当てて、割り当てを確認します。

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

クラスタからの**NFS**クライアントアクセスの確認

UNIX 管理ホストで UNIX ファイル権限を設定することにより、選択したクライアントに共有へのアクセスを許可できます。クライアントアクセスを確認するには、コマンドを使用し `vserver export-policy check-access`、必要に応じてエクスポートルールを調整します。

手順

1. クラスタで、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確認します `vserver export-policy check-access`。

   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 home2 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、ボリュームでエクスポートポリシーが使用されていること、およびアクセスが拒否されたことが示されています `exp-home-dir`。

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
   -type read-write
                                        Policy    Policy     Rule
   Path                    Policy       Owner     Owner Type Index  Access
   ----------------------- ------------ --------- ---------- ------
   ----------
   /                       default      vs1_root  volume          1 read
   /eng                    default      vs1_root  volume          1 read
   /eng/home2              exp-home-dir home2     volume          1 denied

   3 entries were displayed.
   ```

2. 出力を確認して、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、結果としてクライアントが行ったアクセスのタイプを確認する必要があります。

3. 必要に応じて、エクスポートポリシールールを再設定します。

新しいストレージオブジェクトに対する NFS アクセスの確認が完了したら、設定をテストする必要があります。設定をテストするには、 NFS 管理ホストにログインし、 SVM に対するデータの読み取りと書き込みが可能かどうかを確認します。その後、 root 以外のユーザとしてクライアントシステム上で処理を繰り返します。

必要なもの

- クライアントシステムに、前に指定したエクスポートルールで許可されている IP アドレスが割り当てられている必要があります。
- root ユーザのログイン情報が必要です。

手順

1. クラスタで、新しいボリュームをホストしている LIF の IP アドレスを確認します。

   ```
   network interface show –vserver svm_name
   ```

2. 管理ホストクライアントシステムに root ユーザとしてログインします。
3. ディレクトリをマウントフォルダに変更します。

   ```
   cd /mnt/
   ```

4. 新しいフォルダを作成し、 SVM の IP アドレスを使用してマウントします。

   a. 新しいフォルダの作成：+
   `mkdir /mnt/folder`

   b. この新しいディレクトリに新しいボリュームをマウントします。+
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. ディレクトリを新しいフォルダに変更します。+
   `cd folder`

   次のコマンドでは、 test1 という名前のフォルダを作成し、 IP アドレス 192.0.2.130 のボリューム vol1 をマウントフォルダ test1 にマウントして、ディレクトリを新しい test1 に変更しています。

   ```
   host# mkdir /mnt/test1
   host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
   host# cd /mnt/test1
   ```

5. 新しいファイルを作成し、そのファイルが存在することを確認して、テキストを書き込みます。

   a. テストファイルを作成します。+
   `touch filename`

   b. ファイルが存在することを確認します。:+
   `ls -l filename`

   c. 入力：+
   `cat > filename`

テキストを入力してから Ctrl+D を押してテストファイルにテキストを書き込みます。

d. テストファイルの内容を表示します。+
`cat filename`

e. テストファイルを削除します。+
`rm filename`

f. 親ディレクトリに戻ります。+
`cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. root として、マウントされたボリュームに対する必要な UNIX の所有権と権限を設定します。
7. エクスポートルールで特定されている UNIX クライアントシステムで、新しいボリュームへのアクセス権を持つ許可されたユーザとしてログインし、手順 3 ~ 5 を繰り返して、ボリュームのマウントとファイルの作成が可能なことを確認します。

詳細情報の入手方法

NFSクライアントアクセスをテストしたあと、NFSの追加設定を行ったり、SANアクセスを追加したりできます。プロトコルアクセスが完了したら、Storage Virtual Machine（SVM）のルートボリュームを保護する必要があります。

NFSの設定

NFSアクセスについてさらに詳しく設定するには、次の情報やテクニカルレポートを参照してください。

- "NFSの管理"

  NFSを使用したファイルアクセスを設定および管理する方法について説明します。

- "NetAppテクニカルレポート4067：『NFS Best Practice and Implementation Guide』"

  NFSv3およびNFSv4の運用ガイドであり、NFSv4を中心にONTAPオペレーティングシステムの概要を説明しています。

- "NetAppテクニカルレポート4073：『Secure Unified Authentication』"

  NFSストレージ認証用にUNIXベースのKerberosバージョン5（krb5）サーバを使用し、KDCおよびLightweight Directory Access Protocol（LDAP）のアイデンティティプロバイダとしてWindows Server

Active Directory（AD）を使用するようにONTAPを設定する方法について説明します。

- "NetAppテクニカルレポート3580：『NFSv4の拡張機能とベストプラクティスガイド：Data ONTAPでの実装』"

  ONTAPを実行するシステムに接続されたAIX、Linux、またはSolarisクライアントにに NFSv4のコンポーネントを実装する際のベストプラクティスを紹介しています。

ネットワーク構成

ネットワーク機能とネームサービスについてさらに詳しく設定するには、次の情報およびテクニカルレポートを参照してください。

- "NFSの管理"

  ONTAPネットワークを設定および管理する方法について説明します。

- "NetAppテクニカルレポート4182：『clustered Data ONTAP構成でのイーサネットストレージの設計時の考慮事項とベストプラクティス』"

  ONTAPネットワーク構成の実装について説明し、一般的なネットワーク導入シナリオとベストプラクティスの推奨事項を提供します。

- "NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

  認証用にLDAP、NIS、DNS、およびローカルファイルを設定する方法について説明します。

SANプロトコルの設定

新しいSVMに対するSANアクセスを提供または変更する場合は、FCまたはiSCSIの設定情報を使用します。この情報は、複数のホストオペレーティングシステムに関するものです。

ルートボリュームの保護

SVMでプロトコルを設定したら、ルートボリュームを保護してください。

- "データ保護"

  負荷共有ミラーを作成してSVMルートボリュームを保護する方法について説明しています。これは、NAS対応のSVMに対するNetAppのベストプラクティスです。また、SVMルートボリュームを負荷共有ミラーから昇格させてボリュームの障害や損失からリカバリする簡単な方法についても説明しています。

ONTAPエクスポートと7-Modeエクスポートの違い

ONTAPエクスポートと**7-Mode**エクスポートの違い

ONTAPでNFSエクスポートを実装する方法に精通していない場合は、7-ModeとONTAPのエクスポート設定ツールを比較したり、サンプルの7-Modeファイルをクラスタ化されたポリシーやルールと比較し `/etc/exports` たりできます。

ONTAPにはファイルもコマンドもあり `exportfs`ませ `/etc/exports`ん。代わりに、エクスポートポリシーを定義する必要があります。エクスポートポリシーを使用すると、7-Modeとほぼ同じ方法でクライアントアクセスを制御できますが、同じエクスポートポリシーを複数のボリュームで再利用するなどの機能が追加されています。

関連情報

"NFSの管理"

"NetAppテクニカルレポート4067：『NFS Best Practice and Implementation Guide』"

7-Modeト**ONTAP**テノエクスホオトノヒカク

ONTAPでのエクスポートの定義と使用方法は、7-Mode環境とは異なります。

相違点	7-Mode	ONTAP
エクスポートの定義方法	エクスポートはファイルで定義され `/etc/exports`ます。	エクスポートは、SVM内でエクスポートポリシーを作成することによって定義されます。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。
エクスポートの範囲	• エクスポートは指定したファイルパスまたはqtreeに適用されます。 • ファイルパスまたはqtreeごとに、に個別のエントリを作成する必要があります `/etc/exports`。 • エクスポートは、ファイルに定義されている場合にのみ保持され `/etc/exports`ます。	• エクスポートポリシーは、ボリューム内のすべてのファイルパスとqtreeを含むボリューム全体に適用されます。 • エクスポートポリシーは、必要に応じて複数のボリュームに適用できます。 • すべてのエクスポートポリシーは、システムの再起動後も維持されます。
フェンシング（特定のクライアントに対して同じリソースへの別のアクセスを指定すること）	特定のクライアントに単一のエクスポートされたリソースへの異なるアクセスを提供するには、各クライアントとその許可されているアクセスをファイル内でリストする必要が `/etc/exports`あります。	エクスポートポリシーは、複数のエクスポートルールで構成されています。各エクスポートルールでは、リソースに対する特定のアクセス権限が定義され、その権限を持つクライアントがリストされます。特定のクライアントに対して異なるアクセスを指定するには、アクセス権限の特定のセットごとにエクスポートルールを作成し、それらの権限を持つクライアントをリストして、エクスポートポリシーにルールを追加する必要があります。

名前のエイリアス設定	エクスポートを定義するときに、エクスポートの名前をファイルパスの名前とは別の名前にすることができます。このようなエクスポートをファイルで定義する場合は、パラメータを `/etc/exports` 使用する必要があります `-actual`。	エクスポートされたボリュームの名前として、実際のボリューム名とは異なる名前を選択できます。そのためには、カスタムジャンクションパス名を持つボリュームをSVMネームスペース内でマウントする必要があります。 デフォルトでは、ボリュームはそのボリューム名でマウントされます。ボリュームのジャンクションパス名をカスタマイズするには、アンマウントし、名前を変更してから再マウントする必要があります。

ONTAPエクスポートポリシーの例

エクスポートポリシーの例を確認すると、 ONTAP でのエクスポートポリシーの動作について理解を深めることができます。

7-Mode エクスポートの ONTAP 実装例

次の例は、ファイルに出力されている7-Modeエクスポートを示してい `/etc/export` ます。

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

このエクスポートをクラスタエクスポートポリシーとして再現するには、 3 つのエクスポートルールを含むエクスポートポリシーを作成し、そのエクスポートポリシーをボリューム vol1 に割り当てる必要があります。

ルール	要素	値
ルール1	`-clientmatch`（クライアント仕様）	`@readonly_netgroup`
`-ruleindex`（ルールリスト内でのエクスポートルールの位置）	`1`	`-protocol`
`nfs`	`-rorule`（読み取り専用アクセスを許可）	`sys`（クライアントはAUTH_SYSで認証されます）

ルール	要素	値
-rwrule（読み取り/書き込みアクセスを許可）	never	-superuser（スーパーユーザアクセスを許可）
none（root_squashed_to anon）	ルール2	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	ルール3
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. exp_vol1というエクスポートポリシーを作成します。

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. 基本コマンドに対して、次のパラメータを指定して 3 つのルールを作成します。
   - 基本コマンド：+
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - ルールパラメータ：
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none+ -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`
3. ボリュームvol1にポリシーを割り当てます。

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

7-Mode エクスポートの統合の例

次の例は、qtree 10個につき1行で構成された7-Modeのファイルを示してい `/etc/export`ます。

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

ONTAPでは、qtreeごとに、を含むルールが設定されたポリシーとを含むルールが設定 `-clientmatch host2057s`されたポリシーのどちらかが必要です。 `-clientmatch host1519s`

1. exp_vol1q1 と exp_vol1q2 という 2 つのエクスポートポリシーを作成します。
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. 各ポリシーのルールを作成します。
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. ポリシーを qtree に適用します。
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [続く 4 つの qtree …]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [続く 4 つの qtree …]

これらのホスト用に qtree をあとから追加する必要がある場合は、同じエクスポートポリシーを使用します。

CLIを使用したNFSの管理

NFSリファレンスの概要

ONTAPには、NFSプロトコルで使用できるファイルアクセス機能があります。NFSサーバを有効にし、ボリュームまたはqtreeをエクスポートできます。

これらの手順は、次の状況で実行します。

- ONTAP NFSプロトコルの機能の範囲について理解する必要がある。

- NFSの基本的な設定ではなく、あまり一般的でない設定タスクとメンテナンスタスクを実行する。
- System Managerや自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

NASファイルアクセスについて理解する

ネームスペースとジャンクションポイント

ネームスペースとジャンクションポイントの概要

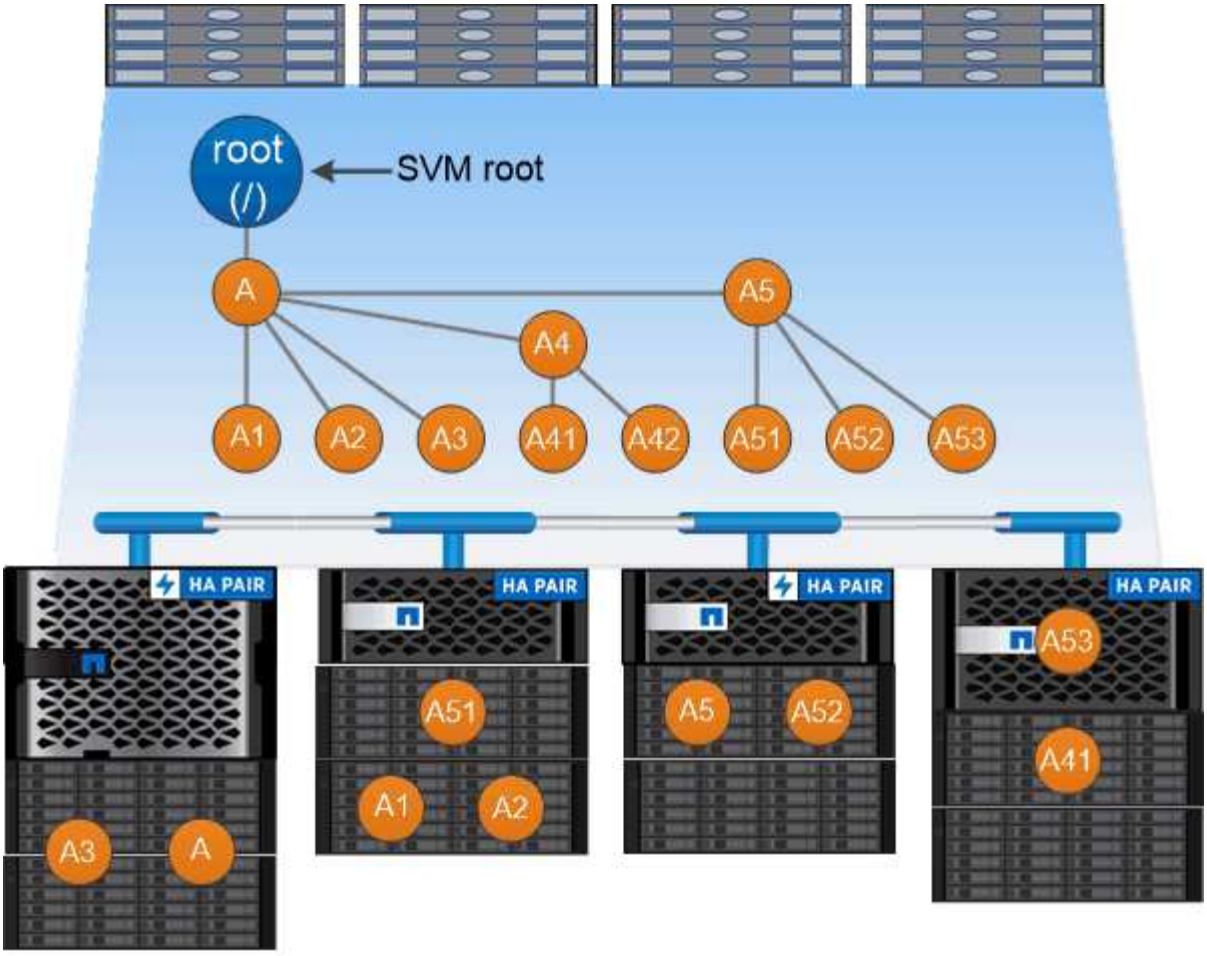
nas_namespace _ は、 _junction points_to によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限があるクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

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

ネームスペースには必要に応じてボリュームを追加できます。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。「vol3」という名前のボリュームのボリュームジャンクションへのパスは、またはの `/vol1/dir2/vol3`ようになります `/vol1/vol2/vol3 /dir1/dir2/vol3`。このパスのことを _junction パスと呼びます。 _

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

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



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

例

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

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

一般的な**NAS**ネームスペースアーキテクチャとは

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。ビジネスやワークフローのニーズに合ったネームスペースアーキテクチャを選択できます。

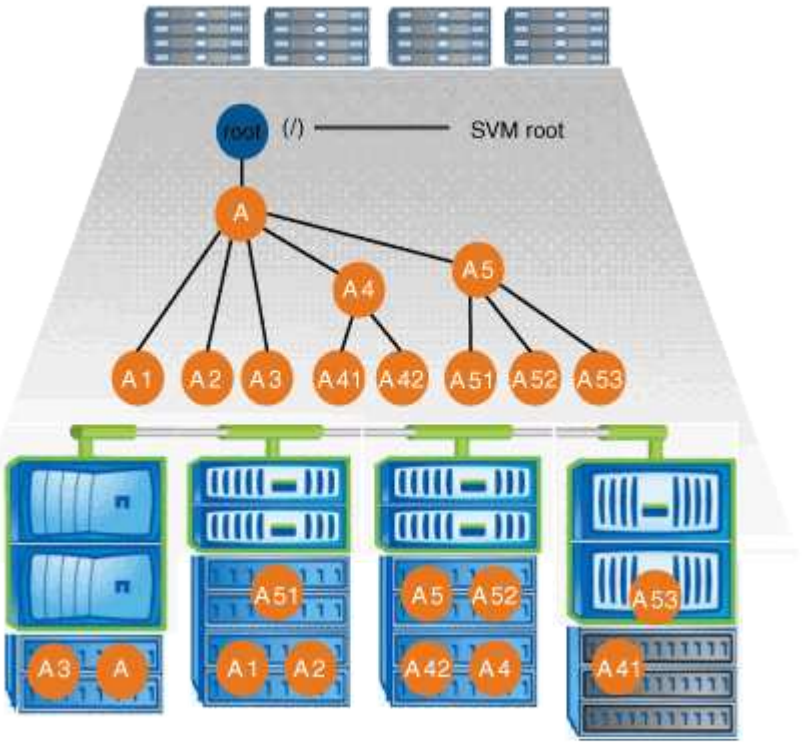
ネームスペースの最上位は常にルートボリュームで、スラッシュ（/）で表されます。ルートの下のネームスペースアーキテクチャは、次の3つの基本カテゴリに分類されます。

- ネームスペースのルートへのジャンクションが1つだけの単一分岐ツリー

- 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分岐ツリー
- 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を持つ複数のスタンドアロンボリューム

単一分岐ツリーを使用するネームスペース

単一分岐のツリーを使用するアーキテクチャには、 SVM ネームスペースのルートへの単一の挿入ポイントがあります。単一の挿入ポイントには、ジャンクションされたボリュームまたはルート直下のディレクトリを指定できます。他のすべてのボリュームは、単一の挿入ポイント（ボリュームまたはディレクトリ）の下のジャンクションポイントでマウントされます。

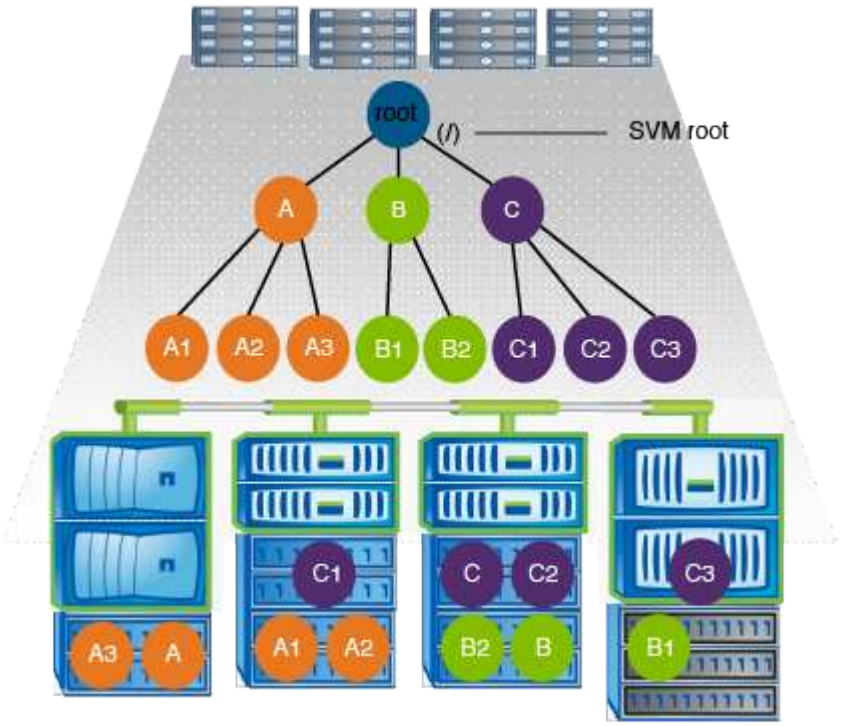


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、すべてのボリュームが単一の挿入ポイントの下で結合された以下のような構成になります。これは「 `d ATA` 」というディレクトリです。

```
                    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    -        /                      -
```

複数分岐ツリーを使用するネームスペース

複数分岐のツリーを使用するネームスペースには、 SVM ネームスペースのルートへの複数の挿入ポイントがあります。挿入ポイントは、ルートの下に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いずれかです。他のすべてのボリュームは、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。

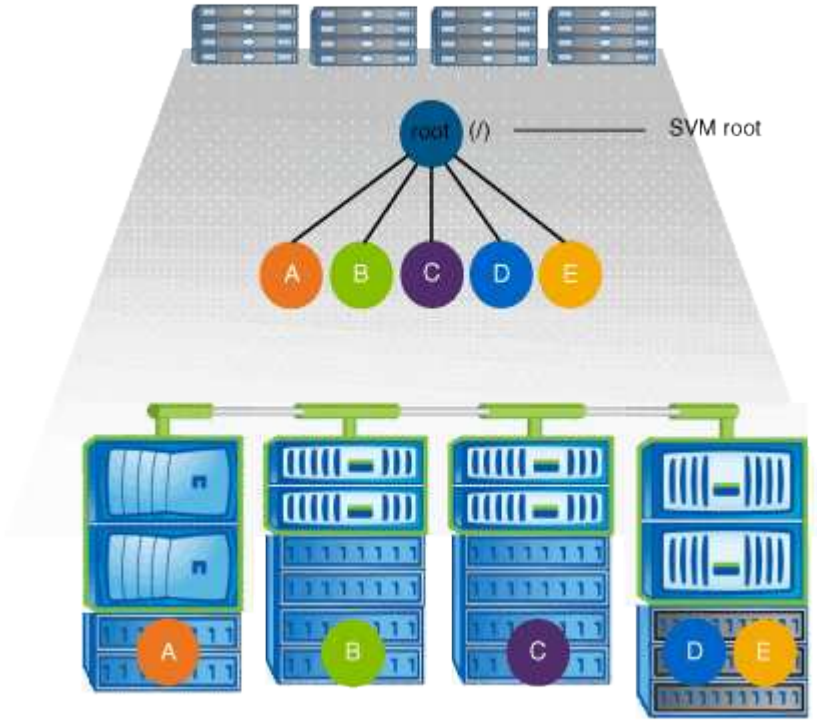


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、 SVM のルートボリュームへの 3 つの挿入ポイントがある以下のような構成になります。2 つの挿入ポイントは、「 `d ata" 」と「 projects' 」という名前のディレクトリです。挿入ポイントの 1 つは「 audit 」という名前の結合されたボリュームです。

```
                    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を使用するネームスペース

スタンドアロンボリュームを使用する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、それらの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ません。各ボリュームには一意のパスがあり、ルート直下でジャンクションされるか、ルートより下のディレクトリでジャンクションされます。



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 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    -        /                      -
```

ONTAPによるファイルアクセスの制御方法

ONTAPによるファイルアクセスの制御方法の概要

ONTAP 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、ファイルアクセスを制御します。

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、 ONTAP は 2 つのタスクを実行する必要があります。

- 認証

  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

  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設定されている権限を比較し、提供するアクセスのタイプ（ある場合）を判別することで、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、 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、 ONTAP の環境に応じて、サービスを適切に設定する必要があります。

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。

ONTAP は、 UNIX サーバおよび Windows サーバの両方からの Kerberos 認証をサポートします。

ファイルベースの制限

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

どのストレージオブジェクトにも、最大 3 種類のセキュリティレイヤを含めることができます。

- エクスポート（NFS）および共有（SMB）セキュリティ

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

- ストレージレベルのアクセス保護のファイルとディレクトリのセキュリティ

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

  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セキュリティは表示されません。システム（WindowsまたはUNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。

- NTFS、UNIX、およびNFSv4の標準のファイルレベルセキュリティ

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

ONTAPによる**NFS**クライアント認証の処理

ONTAPによる**NFS**クライアント認証の処理の概要

NFSクライアントからSVM上のデータにアクセスするには、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。ONTAP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、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、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することで、そのユーザのUNIXクレデンシャルを取得します。ONTAPでは、ローカル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をチェックできます。ONTAPがユーザを正常に認証できるように、これらのうち少なくとも1つを設定する必要があります。複数のネームサービスと、ONTAPによる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を使用する純粋なNFS環境では、この設定だけでNFSクライアントから接続してい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。

mixed、NTFS、またはunifiedのボリュームセキュリティ形式を使用している場合、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SMBユーザ名を取得する必要があります。これには、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SMBユーザを使用します。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ことも、デフォルトのSMBユーザを指定することもできます。

ONTAPでのネームサービスの使用方法

ONTAPは、ネームサービスを使用してユーザとクライアントに関する情報を取得します。ONTAPは、この情報を使用して、ストレージシステム上で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を設定する場合は、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。ONTAP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（ファイル）
- 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をSVMで設定するには、コマンドファミリーを使用し `vserver services name-service ns-switch`ます。これらのコマンドは、UNIXシステムのファイルと同等の機能を提供し `/etc/nsswitch.conf`ます。

NFS クライアントが SVM に接続すると、 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、ONTAPがUNIXクレデンシャルを取得できる場合、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、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。ONTAPでユーザクレデンシャルが適切にマッピングされるようにするには、環境のネームサービスを適切に設定する必要があります。

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管理ユーザの詳細については、を参照してください"カンリシヤニンシヨウトRBAC"。

ONTAPニヨル**NFS**クライアントカラノ**SMB**ファイルアクセスノキョカホウホウ

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 アクセス権による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。

ONTAPでは、ユーザのUNIXユーザID（UID）をSMBクレデンシャルに変換し、そのクレデンシャルを使用してユーザにファイルへのアクセス権があることを確認します。SMBクレデンシャルは、プライマリのSecurity Identifier（SID；セキュリティ識別子）（通常はユーザのWindowsユーザ名）と、ユーザが属しているWindowsグループに対応する1つ以上のグループSIDで構成されます。

ONTAPがUNIX UIDをSMBクレデンシャルに変換するのにかかる時間は、数十ミリ秒から数百ミリ秒です。これは、この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。ONTAPはUIDをSMBクレデンシャルにマッピングし、クレデンシャルキャッシュにマッピングを入力して変換によって発生する検証時間を短縮します。

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、

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。ONTAPは、後で参照できるように、これらのクレデンシャルを内部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することで、パフォーマンスや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いと、 ONTAP ユーザは 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を照会しなければなりません。多数のユーザがアクセスする使用頻度の高いストレージシステムでは、こうした状況がすぐに深刻なパフォーマンス上の問題につながり、不必要な遅延や、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、 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簡単にアクセスすることができます。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）への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。
- ユーザが認証される前に外部ソースからクレデンシャルを取得するための待機時間をなくすことで、ユーザアクセスを高速化します。

ONTAP は、受理されたクレデンシャルと拒否されたクレデンシャルの両方をクレデン受理されたクレデンシャルとは、ユーザが認証されてアクセス権を付与されたこと拒否されたクレデンシャルとは、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、ONTAPは受理されたクレデンシャルを24時間保存します。つまり、ユーザの初回認証後、ONTAPはそのユーザからのすべてのアクセス要求に対してキャッシュされたクレデンシャルを24時間使用します。24 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 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。それまでの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、ONTAPは更新されたクレデンシャルをキャッシュして、次の24時間で使用できるようにします。

デフォルトでは、ONTAPは拒否されたクレデンシャルを2時間保存します。つまり、ユーザへのアクセスを最初に拒否したあと、ONTAPはそのユーザからのすべてのアクセス要求を2時間拒否し続けます。2 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 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。過去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、ONTAPは次の2時間で使用できるように、更新されたクレデンシャルをキャッシュします。

NASネームスペースでのデータボリュームの作成と管理

ジャンクションポイントを指定してデータボリュームを作成する

ジャンクションポイントは、データボリュームの作成時に指定できます。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。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量

またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。

ジャンクションパスに次の文字を使用することはできません。 * # <> < | ?\

+また、ジャンクションパスの長さは255文字以下にする必要があります。

手順

1. ジャンクションポイントを設定して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、ディレクトリと結合されたボリュームの両方を含めることができます。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任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリューム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適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、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が区別されません。はと同じ `/eng`です。 `/ENG`CIFS共有を作成する場合、Windowsではジャンクションパスは大文字と小文字が区別されるかのように扱われます。たとえば、ジャンクションがの場合、 `/ENG`SMB共有のパスははではなくで `/eng`始まる必要があります `/ENG`。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。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 `volume create`ください。

2. 目的のジャンクションポイントで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である「home4」という名前のボリュームをSVM vs1上に作成し `/eng/home`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を指定せずにデータボリュームを作成する

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アクセス用に設定することもできません。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、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。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。

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任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリューム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適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、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。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。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 `volume create`ください。

2. ボリュームがジャンクションポイントなしで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ネームスペースで既存のボリュームをマウントまたはアンマウントする

Storage Virtual Machine（SVM）ボリュームに格納されたデータへのNASクライアントから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。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームをアンマウントすることもできます。

タスクの内容

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、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。

ボリュームへのNASクライアントアクセスを中止するには、ボリュームをアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次の技術情報アーティクルを参照してください。

"ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"

ボリュームをアンマウントしてオフラインにしても、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と、ボリュームまたはディレクトリに作成された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は保持されます。アンマウントしたボリュームを再マウントすると、NASクライアント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に格納されているデータにアクセスできます。

手順

1. 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 svm_name -volume volume_name -junction-path junction_path`

ボリュームのアンマウント	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例は、SVM「vs1」にある「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」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

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の情報を表示します。

Storage Virtual Machine（SVM）のマウントボリューム、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。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ネームスペースを理解し、管理することができます。

ステップ

1. 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のマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver` *`vserver_name`* `-junction`
SVM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に関する詳細情報	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`

SVM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に関する特定の情報	a. 必要に応じて、次のコマンドを使用してパラメータの有効なフィールドを表示できます `-fields`。
	`volume show -fields ?`
	b. パラメータを使用して、必要な情報を表示し `-fields`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
```

次の例は、SVM vs2上に配置された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
```

セキュリティ形式の設定

セキュリティ形式がデータアクセスに与える影響

セキュリティ形式とその影響

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式によって、データに対する権限の処理方法が異なります。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、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、ONTAPはマルチプロトコルに対応しているため、SMBクライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAPでは、UNIXクライアントのみが標準のツールを使用して変更できるUNIX権限が使用されます。

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		
NTFS	SMB	NTFS ACL	NTFS	
mixed	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
unified （ Infinite Volume のみ、ONTAP 9.4 以前のリリース）	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVolでは、UNIX、NTFS、およびmixedのセキュリティ形式がサポートされます。セキュリティ形式がmixedまたはunifiedの場合、ユーザはセキュリティ形式を個別に設定するため、権限を最後に変更したクライアントのタイプによって有効な権限が異なります。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。

unifiedセキュリティ形式は、Infinite Volumeでのみ使用できます。Infinite Volumeは、ONTAP 9 .5以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

Windows.2以降では、コマンドのパラメータを `vserver security file-directory`使用して、指定したファイルまたはフォルダパスでONTAP 9 `show-effective-permissions`ユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータを `-share-name`使用すると、有効な共有権限を表示できます。

ONTAPは、最初に一部のデフォルトのファイル権限を設定します。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は、セキュリティ形式はUNIXになり、アクセス権のタイプはUNIXモードビット（特に指定がないかぎり0755）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るようにクライアントによって設定されるまでの間です。デフォルトでは、NTFSセキュリティ形式のボリューム内のすべてのデータに対するセキュリティ形式はNTFSになり、すべてのユーザにフルコントロールを許可するACLが割り当てられます。

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両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

SVMで使用するセキュリティ形式を決定する

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。主な要因は、ファイルシステムを管理する管理者のタイプです。2番目の要因

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。

ボリュームでセキュリティ形式を設定する場合は、最適なセキュリティ形式を選択し、権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定には、次の考慮事項が役立ちます。

セキュリティ形式	以下の場合に選択
UNIX	• ファイルシステムはUNIX管理者によって管理されます。 • 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は、UNIXユーザをサービスアカウントとして使用します。
NTFS	• ファイルシステムはWindows管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションでは、Windowsユーザをサービスアカウントとして使用します。
mixed	• ファイルシステムはUNIX管理者とWindows管理者の両方によって管理され、ユーザはNFSクライアントとSMBクライアントの両方で構成されます。

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さまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む 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 ボリューム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 ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAPによる**UNIX**アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、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、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれ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できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 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できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限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 アクセス権を NTFS アクセス権に変更しています

  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のセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの 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。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式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。

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、コマンドで `-rootvolume-security-style`パラメータを使用し `vserver create`ます。

   ルートボリュームのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

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ボリューム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 volume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 ボリュームの状況	使用するコマンド
まだ存在しません	`volume create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

FlexVol volumeセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

FlexVol volume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。

コマンドまたは `volume modify`コマンドの詳細については `volume create`、を参照してください"論理ストレージ管理"。

2. 作成したFlexVol volume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ボリューム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
まだ存在しません	`volume qtree create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume qtree modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

qtreeのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

コマンドまたは `volume qtree modify`コマンドの詳細については `volume qtree create`、を参照してください"論理ストレージ管理"。

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を使用したファイルアクセスの設定

NFSを使用したファイルアクセスの設定の概要

クライアントがNFSを使用してStorage Virtual Machine（SVM）上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。環境の現在の構成に応じて、追加の手順がいくつかあります。

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、次のタスクを実行する必要があります。

1. SVMでNFSプロトコルを有効にします。

   クライアントからNFS経由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にNFSサーバを作成

   NFSサーバは、NFS経由でファイルを提供できるようにするSVM上の論理エンティティです。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. ネットワークやストレージの環境に応じて、適切なセキュリティ設定やその他の設定でNFSサーバを構成します。

   この手順には、Kerberos"TLS経由のNFS"、LDAP、NIS、ネームマッピング、およびローカルユーザの設定が含まれます。

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 1 つ以上の _ エクスポートルール _ が含まれています。このプロセスの結果、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まります。クライアントがデータにアクセスするためには、エクスポートルールを含むエクスポートポリシーがStorage Virtual Machine（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ポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントが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、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、 ONTAP を実行しているシステム上で動的に変更できます。

SVMのデフォルトのエクスポートポリシー

各 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ます。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。

SVMを作成すると、SVMのルートボリュームに対してという名前の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 `default`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。

SVM 内に FlexVol ボリュームを作成すると、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。複数のボリュームを同じエクスポートポリシーに関連付けることができます。

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、ボリュームへのクライアントアクセス要求が設定した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、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。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序で処理されます。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した場合、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用してクライアントアクセス権限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）。

  フィールドの最大サイズ `-clientmatch`は4096文字です。

- 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いる場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

> ONTAP 9 .3以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にして、すべてのルール違反をエラールールリストに記録できます。 `vserver export-policy config-checker`コマンドを実行するとチェックが呼び出されて結果が表示され、設定を確認したり、誤ったルールをポリシーから削除したりできます。
>
> このコマンドで検証されるのは、エクスポート設定のホスト名、ネットグループ、匿名ユーザのみです。

例

エクスポートポリシーには、次のパラメータを持つ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が一致していても、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サブネットとは異なるサブネットに属しています。そのため、クライアント一致は失敗し、このルールはこのクライアントには適用されません。

例

エクスポートポリシーには、次のパラメータを持つ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アドレスが指定したサブネットにあります。したがって、クライアント一致は成功し、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は、次のパラメータを持つ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。

両方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アドレスが一致している。読み取り専用パラメータでは、認証に使用し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が許可されます。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クライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

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を管理します。

エクスポートルールのアクセスパラメータに指定されていない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は、アクセスパラメータのオプションを使用して、クライアントへのアクセスを拒否するか、クライアントを匿名ユーザIDにマッピングするかを選択できます。 `none`

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）という理由で、アクセスパラメータに指定されていないセキュリティタイプを使用している可能性があります。デフォルトでは、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はオプションを追加できます `none`。このため、リストにないセキュリティ形式を使用するクライアントは、代わりに匿名ユーザIDにマッピングされます。パラメータは `-anon`、これらのクライアントに割り当てるユーザIDを決定します。パラメータに指定するユーザID `-anon`は、匿名ユーザに適していると思われる権限が設定されている有効なユーザである必要があります。

パラメータの有効な値 `-anon`の範囲は `0`~ `65535`です。

割り当てられたユーザ**ID** `-anon`	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、このユーザに設定されている権限に応じてアクセスを取得します。
`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、このユーザに設定されている権限に応じてアクセスできます。これがデフォルトです。
`65535`	すべて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、セキュリティタイプがAUTH_NONEであると拒否されます。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、クライアントが他のセキュリティタイプを使用している場合は拒否されます。

オプションを使用する場合は `none`、最初に読み取り専用パラメータが処理されることを覚えておくことが重要です。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。

読み取り専用インクルード `none`	読み取り/書き込みに含まれるもの `none`	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	拒否されました
いいえ	○	最初に読み取り専用が処理されるため拒否されました
○	いいえ	匿名として読み取り専用
○	○	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は、次のパラメータを持つ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、認証を行わなかった（セキュリティタイプAUTH_NONE）。

3つのクライアントすべてで、クライアントアクセスプロトコルとIPアドレスが一致しています。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。読み取り専用パラメータは、ユーザIDが70の匿名ユーザとして、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読み取り専用アクセスを許可します。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を使用して読み取り/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は、次のパラメータを持つ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、認証を行わなかった（セキュリティタイプAUTH_NONE）。

3つのクライアントすべてで、クライアントアクセスプロトコルとIPアドレスが一致しています。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。読み取り専用パラメータは、ユーザIDが70の匿名ユーザとして、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読み取り専用アクセスを許可します。読み取り/書き込みパラメータでは、読み取り/書き込みアクセスは匿名ユーザとしてのみ許可されます。

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ニヨルクライアントアクセスレベルノケツテイホウホウ

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。

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. superuser （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(`-rorule`専用)

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 / 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`
スーパーユーザの読み取り / 書き込み	読み取り専用(`-rorule`）(`-rwrule`および `-superuser`読み取り/書き込み

これら3つの各アクセスパラメータで有効なセキュリティタイプは次のとおりです。

- `any`
- `none`
- `never`

  このセキュリティタイプは、パラメータでは使用できません `-superuser`。

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

クライアントのセキュリティタイプを 3 つの各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 つが考えられます。

クライアントのセキュリティタイプ	クライアント
アクセスパラメータで指定されたタイプと一致する。	独自のユーザ ID を使用して、そのレベルのアクセス権を取得します。
指定し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が指定されている `none`。	このレベルのアクセス権を取得しますが、パラメータで指定したユーザIDを持つ匿名ユーザとして取得します `-anon`。
指定したタイプと一致しないため、アクセスパラメータにオプションが指定されていません。 `none`	は、そのレベルのアクセス権を取得しません。これは、指定されていない場合でも常にを含むため、パラメータには適用され `-superuser`ません。 `none`

例

エクスポートポリシーには、次のパラメータを持つ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で認証されています。

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ますが、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は、読み取り/書き込みアクセスを、AUTH_SYSまたはKerberos v5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します。superuserパラメータでは、Kerberos v5で認証されたユーザIDが0のクライアントにスーパーユーザアクセスを許可します。

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。

スーパーユーザのアクセス要求を管理します。

エクスポートポリシーを設定する際には、ストレージシステムがユーザ ID が 0 のクライアントアクセス要求をスーパーユーザとして受信し、それに応じてエクスポートルールを設定する場合に必要な処理を考慮する必要があります。

UNIX の世界では、ユーザ ID 0 のユーザがスーパーユーザと呼ばれ、通常は root と呼ばれます。このユーザにはシステム上で無制限のアクセス権が与えられています。スーパーユーザ権限の使用は、システムやデータセキュリティの侵害などのいくつかの理由によってリスクを伴う可能性があります。

デフォルトでは、 ONTAP はユーザ ID が 0 のクライアントを匿名ユーザにマッピングします。ただし、エクスポートルールで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できます `- superuser`。パラメータに有効なオプションは次のとおりです `-superuser`。

- `any`
- `none`

  これは、パラメータを指定しない場合のデフォルト設定 `-superuser`です。

- `krb5`
- `ntlm`
- `sys`

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

`-superuser`パラメータとクライアントのセキュリティタイプ	クライアント
一致	ユーザ ID 0 でスーパーユーザアクセス権を取得します。
一致しません	パラメータで指定したユーザIDと、割り当てられた権限を持つ匿名ユーザとしてアクセスを取得します `-anon`。これは、読み取り専用パラメータと読み取り/書き込みパラメータのどちらでオプションが指定されているかに関係あり `none`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にアクセスするためにユーザID 0を提示し、パラメータがに設定されている `none`場合 `-superuser`、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は、次のパラメータを持つ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で認証されています。

両方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アドレスが一致している。読み取り専用パラメータでは、認証に使用し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が許可されます。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。

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。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 `-superuser`ます。つまり、デフォルトで `none`ユーザID 0が匿名にマッピングされ、自動的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は、次のパラメータを持つ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で認証されています。

両方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アドレスが一致している。読み取り専用パラメータでは、認証に使用し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が許可されます。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

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、読み取り専用パラメータとパラメータのユーザIDおよびセキュリティタイプと一致しているため、スーパーユーザアクセスを取得します。 `-superuser`クライアント#2のセキュリティタイプが読み取り/書き込みパラメータまたはパラメータと一致しないため、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されません。 `-superuser`代わりに、クライアント #2 は匿名ユーザにマッピングされます。この場合、ユーザ ID は 0 です。

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、 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、 ONTAP は外部ソースから情報を取得する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。

NFS エクスポートへのクライアントアクセスを制御するには、エクスポートポリシーを設定します。各エクスポートポリシーにはルールが含まれており、各ルールにはアクセスを要求しているクライアントに対するマッチングを行うパラメータが含まれています。これらのパラメータの一部では、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 ONTAP が DNS サーバや NIS サーバのような外部ソースと通信する必要があります。

外部ソースとの通信には少し時間がかかります。パフォーマンスを向上させるために、 ONTAP は、各ノード上の複数のキャッシュに情報をローカルに格納して、エクスポートポリシールール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	保存される情報のタイプ
アクセス	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
名前	対応する UNIX ユーザ ID への UNIX ユーザ名のマッピング

キャッシュ名	保存される情報のタイプ
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
ホスト	対応する IP アドレスへのホスト名のマッピング
ネットグループ	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

ONTAP が外部ネームサーバ上の情報を取得してローカルに格納したあとに、環境内の外部ネームサーバ上の情報を変更すると、キャッシュ内の情報が古くなる可能性があります。ONTAP は一定期間の経過後に自動的にキャッシュを更新しますが、有効期限や更新の時期およびアルゴリズムはキャッシュごとに異なります。

キャッシュに古くなった情報が含まれる理由としてもう 1 つ考えられるのは、 ONTAP がキャッシュされた情報の更新を試みたにもかかわらずネームサーバと通信しようとしてエラーが発生した場合です。この場合、 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、成功することが想定されるクライアントアクセス要求が失敗し、エラーとなることが想定されるクライアントアクセス要求が成功する可能性があります。クライアントアクセスに関するこのような問題のトラブルシューティング時には、エクスポートポリシーキャッシュの一部を表示したり、手動でフラッシュしたりできます。

アクセスキャッシュの仕組み

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評価の結果を格納します。これにより、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ポリシールール評価の処理を行う場合よりも、アクセスキャッシュから情報をはるかに短時間で取得できるため、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、 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 1 つ以上のジャンクションポイントと交差している場合は、そのパスに付随する複数のエクスポートポリシーに対してこのチェックの実行が必要になる可能性があります。

なお、この評価は、最初のマウント要求についてだけでなく、読み取り、書き込み、リスト、コピーなどの処理を行う 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。

ONTAP が適用可能な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すると、 ONTAP はその情報を格納するためのエントリをアクセスキャッシュ内に作成します。

NFS クライアントが I/O 要求を送信すると、 ONTAP は、そのクライアントの IP アドレス、 SVM の ID 、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、 ONTAP はそこに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、 ONTAP は先ほど述べたすべての適用可能なポリシールールを評価する通常の処理を行います。

アクティブに使用されていないアクセスキャッシュエントリは更新されません。これにより、外部ネームサーバとの無駄な通信が削減されます。

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を評価する全体的な処理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のエントリの更新期間は、いくつかのパラメータで制御されます。これらのパラメータの仕組みを理解しておくと、パラメータを変更してアクセスキャッシュを調整し、パフォーマンスと格納される情報の最新度のバランスを取ることができます。

アクセスキャッシュには、ボリュームまたはqtreeにアクセスす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るエントリが格納されます。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。更新時間はアクセスキャッシュパラメータによって決まり、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パラメータは、個 々 のSVMに対して指定できます。これにより、SVMのアクセス要件に応じてパラメータを変更できます。アクティブに使用されていないアクセスキャッシュエントリは更新されないため、外部ネームサーバとの不要で無駄な通信が削減されます。

アクセスキャッシュエントリタイプ	説明	更新期間（秒）
正のエントリ	クライアントへのアクセス拒否が発生していないアクセスキャッシュエントリ。	最小：300 最大値：86、400 デフォルト：3、600
負のエントリ	クライアントへのアクセス拒否の原因となったアクセスキャッシュエントリ。	最小：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。ONTAPは、クライアントをエクスポートポリシールールと照合し、エクスポートポリシールールの設定に基づいてアクセスを許可していると判断します。ONTAPはエクスポートポリシールールを正の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、 ONTAP は、この正のエントリを 1 時間（ 3 、 600 秒）アクセスキャッシュ内に保持したあと、情報を最新の状態にするためにこのエントリを自動的に更新します。

アクセスキャッシュが不必要にいっぱいになるのを防ぐために、クライアントアクセスの決定に一定期間使用

されていない既存のアクセスキャッシュエントリを消去するパラメータが追加されています。 `-harvest-timeout`このパラメータの有効範囲は60~2、592、000秒で、デフォルト設定は86、400秒です。

qtreeからエクスポートポリシーを削除する

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、エクスポートポリシーを削除できます。これを行うには `volume qtree modify`、コマンドでパラメータと空の名前文字列（""）を指定し `-export-policy`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. 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ファイル操作のqtree IDを検証する

ONTAP では、オプションで qtree ID の検証を追加で実行できます。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 が使用されるとともに、クライアントによるファイルの移動が同じ qtree 内でのみ行えるようになります。この検証を有効または無効にするには、パラメータを変更し `-validate-qtree-export`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。

タスクの内容

このパラメータは、 Storage Virtual Machine （ SVM ）上の 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有効です。

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。

検証する **qtree ID** の状態	入力するコマンド
有効	`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

ネストされたジャンクションでは制限の少ないポリシーを設定し、上位のジャンクションではより制限の厳しいポリシーを設定するようにエクスポートポリシーを設定した場合、下位のジャンクションへのアクセスが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の少ないエクスポートポリシーを設定する必要があります。

NFSでのKerberos使用によるセキュリティ強化

ONTAPでのKerberosのサポート

Kerberosは、クライアント/サーバアプリケーションに強力で安全な認証を提供します。認証は、サーバに対するユーザIDとプロセスIDの検証を提供します。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。

ONTAP 9では、次の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は、チェックサムを使用して、クライアントとサーバ間で転送される各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確認など）とデータ整合性上の理由（信頼性の低いネットワークでNFSを使用する場合のデータ破損の防止など）の両方で役立ちます。

- プライバシーチェックを使用したKerberos 5認証（krb5p）

  krb5pはチェックサムを使用して、クライアントとサーバ間のすべてのトラフィックを暗号化します。これはより安全であり、より多くの負荷が発生します。

- 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。ONTAPでは、セキュリティを強化するために、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でサポートされます。

- 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の設定に関してクラスタ管理者に頼る必要がなくなり、個 々 のKerberos Realm設定をマルチテナンシー環境で作成できます。

NFSでKerberosを使用するようにシステムで設定する前に、ネットワークおよびストレージの環境内の特定の項目が適切に設定されていることを確認する必要があります。

> 環境を設定する手順は、使用しているクライアントオペレーティングシステム、ドメインコントローラ、Kerberos、DNSなどのバージョンとタイプによって異なります。これらすべての変数を文書化することは、このドキュメントの範囲外です。詳細については、各コンポーネントのそれぞれの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NFSv3およびNFSv4でのONTAPおよびKerberos 5のセットアップ方法の詳細な例については、テクニカルレポート4073を参照してください。

最初に次の項目を設定する必要があります。

ネットワーク環境の要件

- Kerberos

  Windows Active DirectoryベースのKerberosやMIT Kerberosなど、Key Distribution Center（KDC；キー配布センター）を使用してKerberosを設定しておく必要があります。

  NFSサーバは、マシンプリンシパルのプライマリコンポーネントとしてを使用する必要があります `nfs`。

- ディレクトリサービス

  Active DirectoryやOpenLDAPなど、SSL/TLS経由のLDAPを使用するように設定されたセキュアなディレクトリサービスを環境で使用する必要があります。

- NTP

  NTPを実行している稼働中のタイムサーバが必要です。これは、時間のずれによるKerberos認証の失敗を防ぐために必要です。

- ドメイン名解決（DNS）

  各UNIXクライアントおよび各SVM LIFについて、KDCのフォワードルックアップゾーンとリバースルックアップ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。すべての参加者は、DNSを介して適切に解決できる必要があります。

- ユーザアカウント

  各クライアントには、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。

クライアントがRFC1964およびRFC2203をサポートしている必要があります。

- Kerberos

  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。詳細は次のとおりです。

  - TGS 通信の暗号化が有効です。

    最も強力なセキュリティを実現するAES-256。

  - TGT 通信に対する最も安全な暗号化タイプが有効です。
  - Kerberos Realm とドメインを正しく設定します。
  - GSSはイネーブルです。

    マシンのクレデンシャルを使用する場合：

  - パラメータを指定し `-n`てを実行しないで `gssd`ください。
  - をrootユーザとして実行しない `kinit`でください。
- 各クライアントは、最新の更新されたオペレーティングシステムバージョンを使用する必要があります。

  これにより、Kerberosを使用したAES暗号化に最高の互換性と信頼性が提供されます。

- DNS

  正しい名前解決のためにDNS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。

- NTP

  各クライアントがNTPサーバと同期している必要があります。

- ホストおよびドメインの情報

  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

  各クライアントには、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。セキュリティを最大限に高めるには、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用意する必要があります。

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場合にWindowsクレデンシャルを確認するためにのみ必要です。厳密な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

  各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確保するには、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。

- SMB サーバ

  マルチプロトコル環境の場合は、SVMでSMBを設定しておく必要があります。SMB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権限	777

  ルートボリュームとは異なり、データボリュームにはどちらのセキュリティ形式も使用できます。

- 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
デーモン	1
root	0
pcuser	65534（SVMを作成するとONTAPによって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トCIFSノマルチフロトコルノシヨウニヒツヨウ SVMを作成すると、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およびルール

  ルートボリューム、データボリューム、および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、 `-rwrule`、 `-superuser`、を、 `krb5i`または `krb5p`に `krb5`設定でき `-rorule`ます。

- Kerberos-UNIXネームマッピング

  NFSクライアントユーザSPNによって識別されたユーザにroot権限を付与する場合は、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

"NetAppテクニカルレポート4073：『Secure Unified Authentication』"

"NetApp Interoperability Matrix Tool"

"システム管理"

"論理ストレージ管理"

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、オプションを設定し `-v4-id-domain`ます。

タスクの内容

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。 ONTAPNIS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ドメインがある場合などに、ユーザIDドメインの設定が必要になることがあります。ドメイン名は、ドメインコントローラのドメイン設定と一致している必要があります。NFSv3の場合は必要ありません。

ステップ

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でのTLSの使用によるセキュリティ強化

NFSでのTLSを使用したセキュリティ強化の概要

TLSを使用すると、暗号化されたネットワーク通信をKerberosやIPsecと同等のセキュリティで実現でき、複雑さも軽減されます。管理者は、System Manager、ONTAP CLI、またはONTAP REST APIを使用して、NFSv3およびNFSv4.x接続でのセキュリティを強化するためのTLSの有効化、設定、および無効化を行うことができます。

ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

ONTAPでは、TLS経由のNFS接続にTLS 1.3が使用されます。

要件

NFS over TLSにはX.509証明書が必要です。CA署名済みサーバ証明書を作成してONTAPクラスタにインストールするか、NFSサービスが直接使用する証明書をインストールできます。証明書は次のガイドラインに従っている必要があります。

- 各証明書の共通名（CN）には、TLSを有効にするデータLIFのFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を設定する必要があります。
- 各証明書のサブジェクト代替名（SAN）に、TLSを有効にするデータLIFのIPアドレスを設定する必要があります。必要に応じて、データLIFのIPアドレスとFQDNの両方を使用してSANを設定できます。IPアドレスとFQDNの両方が設定されている場合、NFSクライアントはIPアドレスまたはFQDNを使用して接続で

きます。

- 同じLIFに複数のNFSサービス証明書をインストールすることができますが、NFS TLS設定で一度に使用できるのはそのうちの1つだけです。

ONTAPでの**NFS**クライアントに対する**TLS**の有効化または無効化

NFSクライアントとONTAPの間でネットワーク経由で送信されるすべてのデータを暗号化するようにNFS over TLSを設定すると、NFS接続のセキュリティを強化できます。これにより、NFS接続のセキュリティが向上します。これは、NFSに対して有効になっている既存のStorage VMで設定できます。

ONTAP 9では、TLS経由のNFSがパブリックプレビューとして提供されています。15.1プレビュー版として、ONTAP 9の本番ワークロードではNFS over TLSはサポートされていません。15.1

TLSを有効にする

NFSクライアントに対してTLS暗号化を有効にすると、転送中のデータのセキュリティを強化できます。

開始する前に

- 作業を開始する前に、『for NFS over TLS』を参照してください"要件"。
- この手順のコマンドの詳細については、ONTAPのマニュアルページを参照してください。
- リンクhttps://docsの詳細については、ONTAPコマンドリファレンスを参照してください。NetApp .com /us-en/ ONTAP -CLI/ vserver-nfs-tls-interface-enable.html[`vserver nfs tls interface show`^]コマンドを参照してください。

手順

1. TLSを有効にするStorage VMと論理インターフェイス（LIF）を選択してください。
2. そのStorage VMおよびインターフェイスのNFS接続に対してTLSを有効にします。

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. コマンドを使用し `vserver nfs tls interface show`て結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、Storage VMのLIF `vs1`でNFS over TLSを有効にし `data1`ます。

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

TLSの無効化

転送中データのセキュリティ強化が必要なくなった場合は、NFSクライアントのTLSを無効にできます。

開始する前に

リンクhttps://docsの詳細については、ONTAPコマンドリファレンスを参照してください。NetApp .com /us-en/ ONTAP -CLI/ vserver-nfs-tls-interface-disable.html[`vserver nfs tls interface disable`^]コマンドを参照してください。

手順

1. TLSを無効にするStorage VMと論理インターフェイス（LIF）を選択してください。
2. そのStorage VMおよびインターフェイスのNFS接続に対するTLSを無効にします。

   ```
   vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
   ```

3. コマンドを使用し `vserver nfs tls interface show`て結果を表示します。

   ```
   vserver nfs tls interface show
   ```

例

次のコマンドは、Storage VMのLIF `vs1`でNFS over TLSを無効にし `data1`ます。

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

TLS設定の編集

既存のNFS over TLS設定を変更できます。たとえば、この手順を使用してTLS証明書を更新できます。

開始する前に

リンクhttps://docsの詳細については、ONTAPコマンドリファレンスを参照してください。NetApp .com /us-en/ ONTAP -CLI/ vserver-nfs-tls-interface-modify.html[`vserver nfs tls interface modify`^]コマンドを参照してください。

手順

1. NFSクライアントのTLS設定を変更するStorage VMと論理インターフェイス（LIF）を選択してください。
2. 設定を変更します。を指定する場合は `status enable`、パラメータも指定する必要があり `certificate-name`ます。括弧<>の値は、環境の情報で置き換えます。

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. コマンドを使用し `vserver nfs tls interface show`て結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、Storage VMのLIFの `vs2`NFS over TLSの設定を変更します `data2`。

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address          TLS Status TLS Certificate
Name
-------------- ------------- ---------------- ----------
-----------------------
vs1            data1         10.0.1.1         disabled   -
vs2            data2         10.0.1.2         enabled    new_cert
2 entries were displayed.
```

関連情報

"NFSを使用したLinuxサーバ用のNASストレージの有効化"です。

ネームサービスを設定する

ONTAPネームサービススイッチ設定の仕組み

ONTAPでは、UNIXシステムの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 `/etc/nsswitch.conf`。このテーブルを環境に合わせて適切に設定できるように、このテーブルの機能とONTAPでの使用方法を理解しておく必要があります。

ONTAPネームサービススイッチテーブルは、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序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、SVMごとにONTAPで管理されます。

データベースタイプ

このテーブルには、次のデータベースタイプごとに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
ホスト	ホスト名からIPアドレスへの変換	フアイル、DNS
グループ	ユーザグループ情報の検索	フアイル、NIS、LDAP
パスワード	ユーザ情報の検索	フアイル、NIS、LDAP
ネットグループ	ネットグループ情報の検索	フアイル、NIS、LDAP
namemap	ユーザ名のマッピング	フアイル、LDAP

ソースタイプ

ソースによって、適切な情報の取得に使用するネームサービスソースが指定されます。

ソースタイプ	情報の検索先	使用するコマンド

ファイル	ローカルソースファイル	`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を使用する場合でも、NISまたはLDAP認証が失敗した場合に備えて、ローカルユーザをフォールバックとして含めて設定しておく必要があります `files`。

外部ソースへのアクセスに使用するプロトコル

ONTAPでは、外部ソースのサーバにアクセスするために、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

次の例は、SVM svm_1のネームサービススイッチ設定を表示します。

```
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アドレスを検索するために、ONTAPは最初にローカルソースファイルを参照します。クエリから結果が返されない場合は、次にDNSサーバがチェックされます。

ユーザーまたはグループ情報を検索するために、ONTAPはローカルソースファイルのみを参照します。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を検索するために、ONTAPは最初に外部NISサーバを参照します。クエリから結果が返されない場合は、次にローカルネットグループファイルがチェックされます。

SVM svm_1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ありません。したがって、ONTAPはデフォルトでローカルソースファイルのみを参照します。

関連情報

"NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

LDAPを使用

LDAPの概要

LDAP（Lightweight Directory Access Protocol）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LDAPサーバに格納する場合は、既存のLDAPデータベース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。

- ONTAP用にLDAPを設定する前に、サイト環境がLDAPサーバとクライアントの設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAPサーバのドメイン名がLDAPクライアントのエントリと一致している必要があります。
  - LDAPサーバでサポートされるLDAPユーザパスワードのハッシュタイプには、ONTAPでサポートされるハッシュタイプが含まれている必要があります。
    - Crypt（すべてのタイプ）およびSHA-1（SHA、SSHA）。
    - ONTAP 9 .8以降では、SHA-2ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384、およびSSHA-512）もサポートされます。
  - LDAPサーバでセッションセキュリティ対策が必要な場合は、LDAPクライアントで設定する必要があります。

    次のセッションセキュリティオプションを使用できます。

        - LDAP署名（データ整合性チェックを提供）およびLDAP署名と封印（データ整合性チェックと暗号化を提供）
        - START TLS
        - LDAPS （ LDAP over TLS または SSL ）
    - 署名および封印されたLDAPクエリを有効にするには、次のサービスを設定する必要があります。
        - LDAPサーバは、GSSAPI（Kerberos）SASLメカニズムをサポートしている必要があります。
        - LDAPサーバには、DNS A/AAAAレコードと、DNSサーバで設定されたPTRレコードが必要です。
        - Kerberosサーバには、DNSサーバ上にSRVレコードが存在する必要があります。
    - START TLSまたはLDAPSを有効にするには、次の点を考慮する必要があります。
        - NetAppでは、LDAPSではなくStart TLSを使用することを推奨します。
        - LDAPSを使用する場合は、ONTAP 9 .5以降で、TLSまたはSSLに対してLDAPサーバが有効になっている必要があります。ONTAP 9ではSSLはサポートされていません。0-9.4
        - 証明書サーバがドメインで設定済みである必要があります。
    - LDAPリファーラル追跡を有効にするには（ONTAP 9 .5以降で）、次の条件を満たす必要があります。
        - 両方のドメインに次のいずれかの信頼関係を設定する必要があります。
            - 双方向
            - 一方向（プライマリがリファーラルドメインを信頼する場合）
            - 親子
        - 参照されるすべてのサーバ名を解決するようにDNSを設定する必要があります。
        - trueに設定した場合、認証するドメインパスワードは同じである必要があります `--bind-as-cifs-server`。

> 次の設定はLDAPリファーラル追跡ではサポートされていません。
>
> - すべてのONTAPバージョン：
> - 管理 SVM 上の LDAP クライアント
> - ONTAP 9.8 以前では（ 9.9.1 以降でサポートされています）：
> - LDAPの署名と封印（ `-session-security`オプション）
> - 暗号化されたTLS接続（ `-use-start-tls`オプション）
> - LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap`オプション）

- ONTAP 9 .11.1以降では、"nsswitch認証のためのLDAP高速バインド。"
- SVMでLDAPクライアントを設定するときは、LDAPスキーマを入力する必要があります。

  ほとんどの場合、デフォルトのONTAPスキーマのいずれかが適切です。ただし、環境で使用するLDAPスキーマがこれらと異なる場合は、LDAPクライアントを作成する前に、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。環境の要件については、LDAP管理者にお問い合わせください。

- ホスト名解決にLDAPを使用することはサポートされていません。

詳細については、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

LDAPの署名と封印の概念

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへのクエリに対してLDAPセッションセキュリティを有効にすることができます。Storage Virtual Machine（SVM）のNFSサーバセキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、シークレットキーテクノロジを使用してLDAPペイロードデータの整合性を確認します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。LDAPトラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトは.testです `none`。

SMBトラフィックでのLDAPの署名と封印は、コマンドのオプションを `vserver cifs security modify`使用して`SVM`で有効にします `-session-security-for-ad-ldap`。

LDAPSの概念

ONTAPでの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。ONTAPでは、Active Directory統合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するために、START TLSまたはLDAPSを使用できます。

用語

ONTAPでのLDAPSを使用したLDAP通信の保護方法について理解しておくべき用語があります。

- * LDAP *

  （Lightweight Directory Access Protocol）情報ディレクトリにアクセスして管理するためのプロトコル。LDAPは、ユーザ、グループ、ネットグループなどの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。LDAPは、これらのオブジェクトを管理し、LDAPクライアントからのLDAP要求を満たすディレクトリサービスも提供します。

- **SSL**

  (Secure Sockets Layer)インターネットを介して情報を安全に送信するために開発されたプロトコルです。SSLはONTAP 9以降でサポートされていますが、TLSの導入に伴い廃止されています。

- * tls *

  （Transport Layer Security）IETF標準の追跡プロトコルで、以前のSSL仕様に基づいています。SSLの後継です。TLSはONTAP 9 .5以降でサポートされています。

- * LDAPS （ LDAP over SSL または TLS ） *

  TLSまたはSSLを使用してLDAPクライアントとLDAPサーバの間の通信を保護するプロトコル。「*ldap*

over SSL」と「*ldap over TLS*」は同じ意味で使用されることがあります。LDAPSはONTAP 9 .5以降でサポートされています。

- LDAP.5-9.8ではONTAP 9、LDAPSはポート636でのみ有効にできます。そのためには、コマンドでパラメータを `vserver cifs security modify`使用し `-use-ldaps-for-ad-ldap`ます。
- ONTAP 9.9.1以降では、任意のポートでLDAPSを有効にできますが、デフォルトはポート636です。そのためには、パラメータをに `true`設定し `-ldaps-enabled`、必要なパラメータを指定します `-port`。詳細については、のマニュアルページを参照してください。 `vserver services name-service ldap client create`

NetAppでは、LDAPSではなくStart TLSを使用することを推奨します。

- * TLS を開始 *

（ *START_TLS*,*STARTTLS* 、 *_StartTLS* とも呼ばれます）。 TLS 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。

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。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 TLS接続が失敗します。

ONTAPでの**LDAPS**の使用方法

ONTAPはTLSサーバ認証をサポートしています。これにより、SVM LDAPクライアントは、バインド処理時にLDAPサーバのIDを確認できます。TLS対応LDAPクライアントでは、公開鍵暗号化の標準的な技術を使用して、サーバの証明書と公開IDが有効であり、クライアントの信頼できるCAのリストに記載されている認証局（CA）によって発行されたものであることを確認できます。

LDAPでは、TLSを使用した通信の暗号化でSTARTTLSがサポートされます。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TLS接続にアップグレードされます。

ONTAPは次の機能をサポートします。

- Active Directory統合LDAPサーバとSVMの間のSMB関連トラフィックに対するLDAPSの使用
- ネームマッピングやその他のUNIX情報のLDAPトラフィックに対するLDAPSの使用

  Active Directory統合LDAPサーバまたはUNIXベースのLDAPサーバのいずれかを使用して、LDAPネームマッピングおよびその他のUNIX情報（ユーザ、グループ、ネットグループなど）の情報を格納できます。

- シコシヨメイルウトCAシヨウメイシヨ

  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ているときに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、そのLDAPアプリケーションに適した方法で自己署名ルート証明書が生成されて保存されます。

デフォルトでは、LDAPSは無効になっています。

LDAPのRFC2307bisサポートを有効にする

LDAPを使用する必要があり、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追加機能が必要な場合は、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。

必要なもの

デフォルトのLDAPクライアントスキーマのいずれかのコピーを作成しておく必要があります。

タスクの内容

LDAPクライアントスキーマでは、グループオブジェクトはmemberUid属性を使用します。この属性には複数の値を含めることができ、そのグループに属するユーザの名前がリストされます。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でuniqueMember属性が使用されます。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識別名（DN）を含めることができます。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。ONTAPでは、この256グループ制限を超えるグループは無視されます。

デフォルトでは、RFC2307bisサポートは無効になっています。

> MS-AD-BISスキーマを使用してLDAPクライアントを作成すると、ONTAPでRFC2307bisサポートが自動的に有効になります。

詳細については、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

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の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
   ```

環境に最も適した方法でLDAPサーバに接続するようにONTAP LDAPクライアントを設定することで、ユーザ、グループ、ネットグループ情報を含むLDAPディレクトリ検索を最適化できます。デフォルトのLDAPベースと範囲の検索値で十分な状況と、カスタム値の方が適切な場合に指定する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に対する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、クライアントのパフォーマンスの問題を回避するために、検索を可能な限り効率的に行うこともできます。

デフォルトのベースおよび範囲検索値

LDAPベースは、LDAPクライアントがLDAPクエリの実行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を使用して実行されます。このオプションは、LDAPディレクトリが比較的小さく、関連するすべてのエントリが同じDN内にある場合に適しています。

カスタムベースDNを指定しない場合、デフォルトはです `root`。つまり、各クエリでディレクトリ全体が検索されます。これにより、LDAPクエリが成功する可能性は最大になりますが、非効率的になり、大規模なLDAPディレクトリではパフォーマンスが大幅に低下す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クエリの実行に使用するデフォルトの検索スコープです。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実行されます。LDAPクエリーで、名前付きエントリのみを検索するか、DNの1レベル下のエントリを検索するか、DNの下のサブツリー全体を検索するかを決定します。

カスタムベーススコープを指定しない場合、デフォルトはです `subtree`。つまり、各クエリはDNの下のサブツリー全体を検索します。これにより、LDAPクエリが成功する可能性は最大になりますが、非効率的になり、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

カスタム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。この方法で検索ベースとクエリの範囲を制限すると、検索がLDAPディレクトリのより小さなサブセクションに制限されるため、パフォーマンスが大幅に向上します。

カスタムベースと範囲の値を指定すると、ユーザ、グループ、およびネットグループ検索の一般的なデフォルトの検索ベースと範囲が上書きされます。カスタムのベース値と範囲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	カスタム指定要素
`-base-dn`	すべてのLDAP検索のベースDN必要に応じて複数の値を入力できます（ONTAP 9 .5以降のリリースでLDAPリファーラル追跡が有効になっている場合など）。
`-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、ユーザネーム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ディレクトリ構造がより複雑な場合は、特定の情報についてLDAPディレクトリの複数の部分を検索するために、複数のベースDNを指定する必要がある場合があります。ユーザ、グループ、およびネットグループDNの各パラメータに複数のDN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ている場合は、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指定されたDNSの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3つの異なるユーザDNとサブツリーのリストを指定すると、LDAPユーザ検索では、指定された3つのDNのそれぞれについてサブツリー全体が検索されます。

また、 ONTAP 9.5 以降では、 LDAP_referral_c追いかけ _ を指定することもできます。これにより、プライマリ LDAP サーバから LDAP リファーラル応答が返されなかった場合に、 ONTAP LDAP クライアントがその他の LDAP サーバへのルックアップ要求を参照することができます。クライアントは、そのリファーラルデータを使用して、リファーラルデータに記載されたターゲットオブジェクトをサーバから読み出します。参照されたLDAPサーバにあるオブジェクトを検索するには、参照されたオブジェクトのベースDNをLDAPクライアント設定の一部としてベースDNに追加します。ただし、参照されたオブジェクトが検索されるのは、LDAPクライアントの作成時または変更時にリファーラル追跡が有効（オプションを使用）になっている場合のみです `-referral-enabled true`。

LDAPディレクトリのホスト単位のネットグループ検索のパフォーマンスの向上

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、この機能を利用するようにONTAPを設定し、ホスト単位のネットグループ検索を実行できます。これにより、ネットグループ検索にかかる時間が大幅に短縮され、ネットグループ検索時のレイテンシによるNFSクライアントアクセスの問題が軽減されます。

必要なもの

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

DNSサーバには、NFSクライアントのフォワード（A）ルックアップレコードとリバース（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。

ネットグループでIPv6アドレスを指定する場合は、常にRFC 5952で指定されているとおりに各アドレスを短縮および圧縮する必要があります。

タスクの内容

NISサーバは、 netgroup.byuser、および netgroup.byhost`という3つの独立したマップにネットグループ情報を格納します `netgroup。マップと netgroup.byhost`マップの目的は `netgroup.byuser、ネットグループの検索速度を上げることです。ONTAPでは、マウントの応答時間を短縮するために、NISサーバ上でホスト単位のネットグループ検索を実行できます。

デフォルトでは、LDAPディレクトリにはNISサーバのようなマップがありません netgroup.byhost。ただし、サードパーティのツールを使用すれば、NISマップをLDAPディレクトリにインポートして、ホスト単位の高速ネットグループ検索を有効にすることができます netgroup.byhost。ホスト単位のネットグループ検索を許可するようにLDAP環境を設定している場合は、ONTAP LDAPクライアントにマップ名、DN、および検索範囲を設定して、ホスト単位のネットグループ検索を高速化できます netgroup.byhost。

ホスト単位のネットグループ検索の結果をより速く受け取ることで、ONTAPクライアントがエクスポートへのアクセスを要求したときに、エクスポートルールをより迅速に処理できるようになります。これにより、ネットグループ検索のレイテンシの問題が原因でアクセスが遅延する可能性が低くなります。

手順

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

   マップ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には、正確なマップDNを指定する必要があります。

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｝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。デフォルトはです false。

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

   -netgroup-byhost-scope{base|onelevel subtree｝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のデフォルトのはです subtree。

   LDAPクライアント設定がまだ存在しない場合は、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ときにこれらのパラメータを指定することで、ホスト単位のネットグループ検索を有効にできます vserver services name-service ldap client create。

   > ONTAP 9 .2以降では、 -ldap-servers`フィールドがフィールドに置き換わります `-servers。この新しいフィールドには、LDAPサーバのホスト名またはIPアドレスを指定できます。

4. admin権限レベルに戻ります。 set -privilege admin

例

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

`netgroup.byhost`ディレクトリ内のマップと`netgroup`マップは、クライアントアクセスに関する問題を回避するために、常に同期されている必要があります。

関連情報

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

nsswitch認証に**LDAP**高速バインドを使用する

ONTAP 9.11.1以降では、ldap_fast bind_fルキノ ウ（_コンカレントbind_とも呼ばれます）を利用して、クライアント認証要求を迅速かつ簡単に行うことができます。この機能を使用するには、LDAPサーバが高速バインド機能をサポートしている必要があります。

タスクの内容

高速バインドを使用しない場合、ONTAPはLDAP簡易バインドを使用してLDAPサーバで管理者ユーザを認証します。この認証方式では、ONTAPはユーザ名またはグループ名をLDAPサーバに送信し、保存されているハッシュパスワードを受信して、サーバハッシュコードとユーザパスワードからローカルに生成されたハッシュパスコードを比較します。これらが同一の場合、ONTAPはログイン権限を付与します。

高速バインド機能を使用すると、ONTAPはユーザクレデンシャル（ユーザ名とパスワード）のみをセキュアな接続経由でLDAPサーバに送信します。LDAPサーバはこれらのクレデンシャルを検証し、ONTAPにログイン権限を付与するように指示します。

高速バインドの利点の1つは、パスワードのハッシュはLDAPサーバによって実行されるため、LDAPサーバがサポートする新しいハッシュアルゴリズムをONTAPでサポートする必要がないことです。

"高速バインドの使用方法について説明します。"

LDAP高速バインドには、既存のLDAPクライアント設定を使用できます。ただし、LDAPクライアントをTLSまたはLDAPS用に設定することを強く推奨します。設定しないと、パスワードはプレーンテキストでネットワーク経由で送信されます。

ONTAP環境でLDAP高速バインドを有効にするには、次の要件を満たす必要があります。

- ONTAP管理者ユーザは、高速バインドをサポートするLDAPサーバで設定する必要があります。
- ネームサービススイッチ（nsswitch）データベースでLDAP用にONTAP SVMが設定されている必要があります。

- 高速バインドを使用したnsswitch認証用に、ONTAP管理者のユーザおよびグループのアカウントを設定する必要があります。

手順

1. LDAPサーバでLDAP高速バインドがサポートされていることをLDAP管理者に確認します。
2. ONTAP管理者ユーザクレデンシャルがLDAPサーバに設定されていることを確認します。
3. 管理SVMまたはデータSVMにLDAP高速バインドが正しく設定されていることを確認します。

   a. LDAP高速バインドサーバがLDAPクライアント設定に表示されていることを確認するには、次のように入力します。

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

      "LDAPクライアント設定について説明します。"

   b. がnsswitchデータベースに設定されているソースの1つである `passwd`ことを確認するには `ldap`、次のように入力します。

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

   "nsswitchの設定について説明します。"

4. 管理者ユーザがnsswitchで認証されていること、およびLDAP高速バインド認証がアカウントで有効になっていることを確認します。

   ◦ 既存のユーザの場合は、次のパラメータ設定を入力し `security login modify`て確認します。

      ```
      -authentication-method nsswitch
      ```

   ```
   -is-ldap-fastbind true
   ```

   ◦ 新しい管理者ユーザについては、を参照してください。"LDAPまたはNISアカウントアクセスを有効にします。"

LDAP統計の表示

必要なもの

- SVM で LDAP クライアントを設定しておく必要があります。
- データを表示できる LDAP オブジェクトを特定しておく必要があります。

ステップ

1. カウンタオブジェクトのパフォーマンスデータを表示します。

   ```
   statistics show
   ```

例

次の例は、* smpl_1 *という名前のサンプルについて、avg_processor_busyカウンタとcpu_busyカウンタの統計を表示します。

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

ネームマッピングの設定

ネームマッピングの設定の概要

ONTAPでは、ネームマッピングを使用して、SMB IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをSMB IDにマッピングします。この情報は、NFSクライアントとSMBクライアントのどちらから接続しているかに関係なく、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です。

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、ボリューム上でSMB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。
- 代わりにデフォルトユーザを使用するように設定します。

  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個別に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ないことに注意してください。

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という語で開始または終了するすべての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。

ネームマッピングの仕組み

ONTAPで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は、まずローカルの

ネームマッピングデータベースとLDAPサーバで既存のマッピングの有無を確認します。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、SVMのネームサービスの設定で決まります。

- 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、ONTAPは小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。見つからない場合は、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、ONTAPはSMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合は、デフォルトのSMBユーザを使用します（設定済みの場合）。デフォルトのSMBユーザが設定されておらず、この方法でも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。

マシンアカウントは、デフォルトで指定されたデフォルトのUNIXユーザにマッピングされます。デフォルトのUNIXユーザが指定されていない場合、マシンアカウントのマッピングは失敗します。

- ONTAP 9 .5以降では、マシンアカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9 .4以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントのネームマッピングが定義されていても、それらのマッピングは無視されます。

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

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。また、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ONTAPとどのように連携するかを理解しておく必要があります。SMBサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、SVMのSMB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されます。SMB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するユーザを認証および許可できます。その逆も同様です。

  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間で双方向の信頼関係が確立された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、ホームドメインはもう一方のドメインを信頼します。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す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実行時に _not_searched になります。

- 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SMBサーバのホームドメインを信頼します。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するユーザを認証または許可できません。

  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実行時に _not_searched になります。

ワイルドカード（*）を使用したネームマッピング用のマルチドメイン検索の設定方法

マルチドメインネームマッピングの検索は、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することで簡単に実行できます。次の表に、ネームマッピングエントリのドメイン部分でワイルドカードを使用してマルチドメイン検索を有効にする方法を示します。

パターン	交換	結果
root	｛Asterisk｝ ｛backslash｝ ｛backslash｝ 管理者	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。
*	｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝	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。 パターン ｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝ は、UNIX から Windows へのネームマッピングでのみ有効で、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

マルチドメイン名の検索に使用する信頼できるドメインのリストを決定するには、次の2つの方法のいずれかを選択します。

- ONTAPによってコンパイルされた自動検出双方向信頼リストを使用する
- コンパイルした信頼できるドメインの優先リストを使用する

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、マッピングされたWindowsユーザはこの検索リストでのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係が確立されたすべてのドメインでWindowsユーザの検索が行われます。
- ホームドメインに双方向の信頼関係が確立されたドメインがない場合は、ホームドメインでユーザの検索が行われます。

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、ホームドメインでWindowsユーザの検索が行われます。

ネームマッピングの変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 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プログラムのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed`。

ネームマッピングを作成する

コマンドを使用すると、ネームマッピングを作成できます `vserver name-mapping create`。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。

タスクの内容

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> および `-replacement`ステートメントは、 `-pattern`正規表現として記述できます。また、ステートメントを使用して、`null`の置換文字列（スペース文字）を使用してユーザへのマッピングを明示的に拒否する `" "`こともできます `-replacement`。詳細については、のマニュアルページを参照して `vserver name-mapping create` ください。

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 ONTAP システムに接続していたすべての SMB 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、優先順位リストの1番目にあります。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 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。パターンとリプレースメントには正規表現が使用されています。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 LDAP 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"
```

次のコマンドは、 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。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

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。または、マッピングされていないユーザの認証を失敗させる場合は、デフォルトユーザを設定しないでください。

タスクの内容

CIFS認証で、各Windowsユーザを個 々 のUNIXユーザにマッピングしない場合は、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 々 のWindowsユーザにマッピングしない場合は、代わりにデフォルトのWindowsユーザを指定できます。

ステップ

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`

ネームマッピングの管理用コマンド

ONTAPには、ネームマッピングを管理するため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注：ネームマッピングがIP修飾子エントリで設定されている場合はスワップは許可されません。	`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`
ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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。

Windows NFSクライアントのアクセスを有効にする

ONTAP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。つまり、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は、クラスタのNFSv3エクスポートのファイルにアクセスできます。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、一定の要件と制限事項に注意する必要があります。

タスクの内容

デフォルトでは、Windows NFSv3クライアントのサポートは無効になっています。

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。

手順

1. Windows NFSv3クライアントのサポートを有効にします。

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly
   disabled
   ```

2. Windows NFSv3クライアントをサポートするすべてのSVMで、パラメータと `-v3-connection-drop`パラメータを無効にし `-enable-ejukebox`ます。

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

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

3. オプションを指定して、各Windows NFSv3クライアントがハードマウントを使用するようにします `-o mtype=hard`。

   これは、マウントの信頼性を確保するために必要です。

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

NFSクライアントで**NFS**エクスポートの表示を有効にする

NFSクライアントでは、コマンドを使用して、ONTAP NFSサーバから使用可能なエクスポートのリストを表示できます `showmount -e`。これは、ユーザがマウントするファイルシステムを確認するのに役立ちます。

ONTAP 9.2 以降 ONTAP では、 NFS クライアントでのエクスポートリストの表示がデフォルトで許可されます。以前のリリースでは、 `showmount`コマンドのオプションを `vserver nfs modify`明示的に有効にする必要がありました。エクスポートリストを表示するには、 SVM で NFSv3 が有効になっている必要があります。

例

次のコマンドは、 vs1 という SVM に対して showmount を実行します。

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1     enabled
```

次のコマンドは、 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を表示します。

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

NFSを使用したファイルアクセスの管理

NFSv3の有効化または無効化

NFSv3を有効または無効にするには、オプションを変更し `-v3`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ようになります。デフォルトでは、NFSv3が有効になっています。

ステップ

1. 次のいずれかを実行します。

状況	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を有効または無効にする

NFSv4.0を有効または無効にするには、オプションを変更し `-v4.0`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ようになります。ONTAP 9.9.1では、NFSv4.0はデフォルトで有効になっています。以前のリリースでは、デフォルトで無効になっていました。

ステップ

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を有効または無効にする

NFSv4.1を有効または無効にするには、オプションを変更し`-v4.1`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ようになります。ONTAP 9.9.1では、NFSv4.1がデフォルトで有効になります。以前のリリースでは、デフォルトで無効になっていました。

ステップ

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`

NFSv4ストレージプールの制限を管理します。

ONTAP 9 .13以降では、管理者がクライアントあたりのストレージプールのリソース制限に達したときに、NFSv4サーバがNFSv4クライアントに対するリソースを拒否するように設定できます。クライアントがNFSv4ストレージプールリソースを大量に消費すると、NFSv4ストレージプールリソースが使用できないために他のNFSv4クライアントがブロックされる可能性があります。

この機能を有効にすると、各クライアントによるアクティブなストレージプールリソース消費量を表示することもできます。これにより、システムリソースを使い果たしているクライアントを識別しやすくなり、クライアントごとのリソース制限を課すことができます。

消費されたストレージプールリソースの表示

`vserver nfs storepool show`コマンドは、消費された`storepool`リソースの数を表示します。ストレージプールは、`NFSv4`クライアントが使用するリソースのプールです。

ステップ

1. 管理者は、コマンドを実行して `vserver nfs storepool show`NFSv4クライアントのストレージプール情報を表示します。

例

次の例は、NFSv4クライアントのストレージプール情報を表示します。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

ストレージプールの制限制御を有効または無効にする

管理者は、次のコマンドを使用して、ストレージプールの制限制御を有効または無効にできます。

ステップ

1. 管理者は、次のいずれかの操作を実行します。

状況	入力するコマンド
ストレージプール制限の制御を有効にする	`vserver nfs storepool config modify -limit-enforce enabled`
ストレージプール制限制御を無効にする	`vserver nfs storepool config modify -limit-enforce disabled`

ブロックされたクライアントのリストを表示する

ストレージプール制限が有効になっている場合、管理者は、クライアントごとのリソースしきい値に達したときにブロックされたクライアントを確認できます。管理者は次のコマンドを使用して、ブロックされたクライアントとしてマークされているクライアントを確認できます。

手順

1. コマンドを使用して `vserver nfs storepool blocked-client show`、NFSv4のブロックされたクライアントリストを表示します。

クライアントあたりのしきい値に達したクライアントは切断され、ブロッククライアントキャッシュに追加されます。管理者は次のコマンドを使用して、ブロッククライアントキャッシュからクライアントを削除できます。これにより、クライアントはONTAP NFSv4サーバに接続できるようになります。

手順

1. コマンドを使用して `vserver nfs storepool blocked-client flush -client-ip <ip address>`、storepool blockedクライアントキャッシュをフラッシュします。
2. コマンドを使用し `vserver nfs storepool blocked-client show`て、クライアントがブロッククライアントキャッシュから削除されたことを確認します。

例

この例では、IPアドレスが「10.2.1.1」のブロックされたクライアントがすべてのノードからフラッシュされています。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

pNFSの有効化または無効化

pNFSを使用すると、NFSクライアントが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できるようになり、潜在的なボトルネックとしてNFSサーバがバイパスされるため、パフォーマンスが向上します。pNFS（Parallel NFS）を有効または無効にするには、オプションを変更します `-v4.1-pnfs`。

ONTAPのリリース	**pNFS**のデフォルト
9.8以降	無効
9.7以前	有効

必要なもの

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。

ステップ

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`

関連情報

- NFSトランキングの概要

TCPおよび**UDP**経由の**NFS**アクセスの制御

TCPおよびUDP経由のStorage Virtual Machine（SVM）へのNFSアクセスを有効または無効にするには、パラメータと `-udp`パラメータをそれぞれ変更し `-tcp`ます。これにより、環境内で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。

タスクの内容

これらのパラメータはNFSにのみ適用されます。補助プロトコルには影響しません。たとえば、NFS over TCPを無効にしても、TCP経由のマウント処理は引き続き成功します。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。

> コマンドが失敗しないように、NFSに対してTCPを無効にする前にSnapDiff RPCサーバをオフにする必要があります。TCPを無効にするには、コマンドを使用し `vserver snapdiff-rpc-server off -vserver vserver name`ます。

ステップ

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 経由で無効にしました	`vserver nfs modify -vserver vserver_name -udp disabled`

非予約ポートからの**NFS**要求を制御する

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できます `-mount-rootonly`。非予約ポートからのすべてのNFS要求を拒否するには、オプションを有効にし `-nfs-rootonly`ます。

タスクの内容

デフォルトでは、オプション `-mount-rootonly`はです `enabled`。

デフォルトでは、オプション `-nfs-rootonly`はです `disabled`。

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。

ステップ

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`
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**ユーザの**NTFS**ボリュームまたは**qtree**への**NFS**アクセスを処理する

ONTAPは、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、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。セキュリティを強化するためにこのようなユーザに対してアクセスを拒否するようにを設定することも、デフォルトのWindowsユーザにマッピングしてすべてのユーザに最小限のアクセスレベルを保証するようにONTAPを設定することもできます。

必要なもの

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

タスクの内容

UNIXユーザがNTFSセキュリティ形式のボリュームまたはqtreeにアクセスしようとする場合、そのUNIXユーザは、ONTAPがNTFSアクセス権を適切に評価できるように、まずWindowsユーザにマッピングされている必要があります。ただし、ONTAPは、設定されているユーザ情報ネームサービスソースでUNIXユーザの名前を検索できない場合、特定のWindowsユーザにUNIXユーザを明示的にマッピングすることはできません。このような不明なUNIXユーザの処理方法は、次の方法で決定できます。

- 不明なUNIXユーザへのアクセスを拒否します。

  これにより、NTFSボリュームまたはqtreeにアクセスするすべてのUNIXユーザに明示的なマッピングを要求することで、より厳格なセキュリティが適用されます。

- 不明なUNIXユーザをデフォルトのWindowsユーザにマッピングします。

  これにより、セキュリティは低下しますが、すべてのユーザがデフォルトのWindowsユーザを介してNTFSボリュームまたはqtreeへの最小限のレベルのアクセス権を取得できるようになるため、利便性が向上します。

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	`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
   ```

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考慮事項

この `-mount-rootonly`オプションは、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必要があるストレージシステムでは、ユーザがrootとしてログインしている場合でも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。

この `-mount-rootonly`オプションを有効にすると、ONTAPでは、非予約ポート（1、023より大きいポート）を使用するNFSクライアントにNFSエクスポートのマウントを許可しません。

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

デフォルトでは、 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実行します。この追加チェックにより、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ことが確認されます。一致しない場合、 ONTAP はクライアントアクセスを拒否します。

タスクの内容

ONTAP は、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およびネットグループが含まれているエクスポートポリシールールを評価する際に、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 ONTAP が確認する必要があります。そのために、 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、 Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を取得します。

ネットグループファイルにホストの短い名前のみがリストされていて、そのホストの短い名前が複数のドメインに存在している場合は、異なるドメインのクライアントがこのチェックなしでアクセス権を取得することが可能です。

この問題を回避するために、 ONTAP は、ホストについて DNS から返されたドメインを SVM 用に設定されている DNS ドメイン名のリストと比較します。一致した場合は、アクセスが許可されます。一致しない場合、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。これを管理するには、advanced権限レベルで使用できるパラメータを変更し `-netgroup-dns-domain-search`ます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 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	入力するコマンド
有効	`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
   ```

NFSv3サービスに使用するポートを変更します。

ストレージシステム上のNFSサーバは、マウントデーモンやNetwork Lock Managerなどの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。ほとんどのNFS環境ではデフォルトポートは正しく機能し、変更は必要ありませんが、NFSv3環境で別のNFSネットワークポートを使用する場合は変更できます。

必要なもの

ストレージシステムでNFSポートを変更するには、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、変更を行う前にこの情報をユーザに伝えておく必要があります。

タスクの内容

NFSマウントデーモン、Network Lock Manager（NLM；ネットワークロックマネージャ）、Network Status Monitor（ネットワークステータスモニタ）、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、TCPとUDPの両方でデータにアクセスするNFSクライアントに影響します。

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_namenfs_port_parameterport_number
   ```

NFS ポートのパラメータ	説明	デフォルトポート
`-mountd-port`	NFSマウントデーモン	635
`-nlm-port`	ネットワークロックマネージャ	4045
`-nsm-port`	ネットワークステータスモニタ	4046
`-rquotad-port`	NFSクォータデーモン	4049

   デフォルトのポート以外に、使用できるポート番号の範囲は1024~65535です。各NFSサービスは一意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. コマンドを使用し `network connections listening show`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

ONTAPには、NFSサーバを管理するため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`

NFSv3マウントポイントのディレクトリの一覧を非表示にする `.snapshot` このオプションを有効にしても、ディレクトリへの明示的なアクセス `.snapshot`は許可されます。	`vserver nfs`enabledオプションを指定したコマンド `-v3-hide-snapshot`

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。

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、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、検索の詳細や結果を調べてトラブルシューティングに役立てることができます `vserver services name-service getxxbyyy`。

タスクの内容

- 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。

    これにより、特定のノードまたはSVMでネームサービス検索をテストして、ネームサービス設定の問題の可能性を絞り込むことができます。
  - 検索に使用されるソースを表示するかどうか。

    これにより、正しいソースが使用されているかどうかを確認できます。
- 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アドレスのみ）
グループのメンバー（グループID別）	`vserver services name-service getxxbyyy getgrbygid`

グループのメンバー（グループ名別）	`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アドレスのみ）
ユーザ情報（ユーザ名別）	`vserver services name-service getxxbyyy getpwbyname`パラメータをに `true`指定すると、RBACユーザの名前解決をテストできます `-use-rbac`。
ユーザ情報（ユーザID別）	`vserver services name-service getxxbyyy getpwbyuid`パラメータをに `true`指定すると、RBACユーザの名前解決をテストできます `-use-rbac`。
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`
ホスト単位のネットグループ検索を使用した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 netgrpbyhost`

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、501768というUIDを持つ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という名前の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
```

1. 実行したテストの結果を分析し、必要な措置を取ります。

状況	を確認します
ホスト名またはIPアドレスの検索に失敗したか、正しくない結果が返されました	DNS構成
ルックアップで不正なソースが照会されました	ネームサービススイッチの設定

状況	を確認します
ユーザまたはグループの検索に失敗したか、正しくない結果が得られた	• ネームサービススイッチの設定 • ソースの設定（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やルートなど）
ホスト名の検索に失敗するかタイムアウトし、DNSの短縮名（host1など）がDNSサーバで解決されない	Top-Level Domain（TLD；最上位レベルドメイン）クエリのDNS設定。TLDクエリを無効にするには、コマンドのオプションを `vserver services name-service dns modify`使用し `-is-tld-query-enabled false`ます。

関連情報

"NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

ネームサービス接続を確認する

ONTAP 9 .2以降では、DNSおよびLDAPネームサーバがONTAPに接続されていることを確認できます。これらのコマンドは、admin権限レベルで使用できます。

タスクの内容

ネームサービス設定チェックを使用して、必要に応じてDNSまたはLDAPのネームサービス設定が有効かどうかを確認できます。この検証チェックは、コマンドラインまたはSystem Managerで開始できます。

DNS構成では、すべてのサーバがテストされ、構成が有効であるとみなされるためにはすべてのサーバが動作している必要があります。LDAP設定の場合、いずれかのサーバが稼働していれば設定は有効です。ネームサービスコマンドは、フィールドがtrue（デフォルトはfalse）でないかぎり設定チェックを適用します `skip-config-validation`。

ステップ

1. 該当するコマンドを使用して、ネームサービスの設定を確認します。設定されているサーバのステータスがUIに表示されます。

確認する項目	使用するコマンド
DNSの設定ステータス	`vserver services name-service dns check`
LDAPの設定ステータス	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                |
```

設定済みのサーバ（name-servers/ldap-servers）の少なくとも1つが到達可能でサービスを提供している場合、設定の検証に成功します。一部のサーバに到達できない場合は警告が表示されます。

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の管理では、エントリを作成、表示、変更、削除できます。

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します。	`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。

関連情報

"NetAppテクニカルレポート4668：『ネームサービスベストプラクティスガイド』"

ネームサービスキャッシュの管理用コマンド

ネームサービスキャッシュは、Time-To-Live（TTL）値を変更することで管理できます。TTL値は、ネームサービス情報をキャッシュに保持する期間を決定します。

TTL 値を変更する対象	使用するコマンド
UNIXユーザ	`vserver services name-service cache unix-user settings`
UNIXグループ	`vserver services name-service cache unix-group settings`
UNIXネットグループ	`vserver services name-service cache netgroups settings`
ホスト	`vserver services name-service cache hosts settings`
グループメンバーシップ	`vserver services name-service cache group-membership settings`

関連情報

"ONTAPコマンド リファレンス"

ネームマッピングの管理用コマンド

ONTAPには、ネームマッピングを管理するため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注：ネームマッピングがIP修飾子エントリで設定されている場合はスワップは許可されません。	`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`

ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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。

ロオカル**UNIX**ユウサノカンリヨウコマント

ONTAPには、ローカルUNIXユーザを管理するため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ユーザをロードします。	`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。

ローカル**UNIX**グループの管理用コマンド

ONTAPには、ローカルUNIXグループを管理するため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。

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

ONTAP では、クラスタ内の UNIX ユーザおよびグループの最大数の制限と、この制限を管理するためのコマンドが導入されました。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過剰に作成し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 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。ローカル UNIX ユーザについては別途制限があります。これらの制限はクラスタ全体に適用されます。これらの新しい制限はそれぞれデフォルト値に設定されており、あらかじめ割り当てられたハードリミットまで引き上げることができます。

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	六五、五三六
ローカルUNIXグループおよびグループメンバー	３２、７６８	六五、五三六

ローカル**UNIX**ユーザおよびグループの制限を管理します。

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、過剰な数のローカル UNIX ユーザおよびグループに関連していると考えられる、クラスタ内のパフォーマンスの問題のトラブルシューティングを行うことができます。

タスクの内容

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。

ステップ

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します	`vserver services unix-group max-limit show`

状況	使用するコマンド
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の管理では、URIからのロード、ノード間でのステータスの確認、表示、削除を行います。

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以上の権限レベルで使用できます。
ローカルネットグループを表示します。	`vserver services name-service netgroup file show`
ローカルネットグループを削除します。	`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。

NISドメイン設定の管理用コマンド

ONTAPには、NISドメイン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ドメイン設定を作成する	`vserver services name-service nis-domain create`
NISドメイン設定を表示する	`vserver services name-service nis-domain show`
NISドメイン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統計を表示する	`vserver services name-service nis-domain show-statistics`advanced以上の権限レベルで使用できます。
NIS統計のクリア	`vserver services name-service nis-domain clear-statistics`advanced以上の権限レベルで使用できます。
NISドメイン設定を変更する	`vserver services name-service nis-domain modify`
NISドメイン設定を削除する	`vserver services name-service nis-domain delete`
ホスト単位のネットグループ検索のキャッシュを有効にする	`vserver services name-service nis-domain netgroup-database config modify`advanced以上の権限レベルで使用できます。

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。

LDAPクライアント設定の管理用コマンド

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

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または削除することはできません。

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。

LDAP設定の管理用コマンド

ONTAPには、LDAP設定を管理するため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。

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

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。

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または削除することはできません。

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以上の権限レベルで使用できます。
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以上の権限レベルで使用できます。
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以上の権限レベルで使用できます。

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。

NFS Kerberosインターフェイス設定の管理用コマンド

ONTAPには、NFS Kerberosインターフェイスの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LIFでNFS Kerberosを有効にする	`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`
LIFでNFS Kerberosを無効にする	`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。

NFS Kerberos Realm設定の管理用コマンド

ONTAPには、NFS Kerberos Realmの設定を管理するため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の設定を作成します。	`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。

エクスポートポリシーの管理用コマンド

ONTAPには、エクスポートポリシーを管理するため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。

エクスポートルールの管理用コマンド

ONTAPには、エクスポートルールを管理するため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`

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管理時にそれらのルールの同期を維持してください。

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。

NFSクレデンシャルキャッシュの設定

NFSクレデンシャルキャッシュノTime-To-Liveヲヘンコウスルリユ

ONTAP は、アクセス高速化とパフォーマンス向上のために、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でのユーザ認証に必要な情報を格納します。情報を環境に合わせてカスタマイズするために、クレデンシャルキャッシュに保存する期間を設定できます。

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か、またそうした変更がどのような影響を及ぼす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 の変更を検討してください。

問題	修正アクション
環境内のネームサーバで ONTAP からの要求の負荷が高いためにパフォーマンスが低下している。	キャッシュされている受理および拒否のクレデンシャルに対するTTLを大きくして、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、以前に拒否されたNFSユーザへのアクセスを許可するように変更を加えました。	キャッシュされている拒否のクレデンシャルに対するTTLを短くして、NFSユーザがアクセスできるようにONTAPが新しいクレデンシャルを外部ネームサーバに要求するまでの待機時間を短縮します。

問題	修正アクション
ネームサーバ管理者が、以前に許可されていたNFSユーザへのアクセスを拒否する変更を行いました。	キャッシュされている受理されたクレデンシャルに対するTTLを短くして、ONTAPが新しいクレデンシャルを外部ネームサーバに要求してNFSユーザがアクセスを拒否されるようになるまでの時間を短縮します。

結果

受理されたクレデンシャルと拒否されたクレデンシャルをキャッシュする期間を個別に変更できます。ただし、その利点と欠点の両方に注意する必要があります。

状況	利点は ...	欠点は ...
受理のクレデンシャルのキャッシュ時間を長くする	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下し、ネームサーバの負荷が軽減されます。	以前はアクセスが許可されていたが今後は許可されなくなったNFSユーザに対して、アクセスを拒否するのにかかる時間が長くなります。
受理された認証情報のキャッシュ時間を短くする	以前はアクセスが許可されていたが今後は許可されなくなったNFSユーザに対して、アクセスを拒否するのにかかる時間が短縮されます。	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。
拒否されたクレデンシャルのキャッシュ時間を長くします	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下し、ネームサーバの負荷が軽減されます。	以前はアクセスが許可されていなかったが今後は許可されるようになるNFSユーザにアクセスを許可するのにかかる時間が長くなります。
拒否されたクレデンシャルのキャッシュ時間を短くします	以前はアクセスが許可されていなかったが今後は許可されるようになったNFSユーザにアクセスを許可するのにかかる時間が短縮されます。	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**Time-To-Live**を設定する

Storage Virtual Machine（SVM）のNFSサーバを変更することで、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（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やNFSユーザアクセスに影響するクレデンシャルの変更に関連する特定の問題を軽減できます。

タスクの内容

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. 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
受理のクレデンシャル	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTLはミリ秒単位で測定されます。ONTAP 9.10.1以降では、デフォルトは1時間（3,600,000ミリ秒）です。ONTAP 9.9.1以前では、デフォルトは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。
拒否の認証情報	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTLはミリ秒単位で測定されます。デフォルトは 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を管理します。

エクスポートポリシーキャッシュをフラッシュする

ONTAP は、アクセスを高速化するために、エクスポートポリシーに関連する情報の格納に複数のエクスポートポリシーキャッシュを使用します。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(`vserver export-policy cache flush`）と古い可能性がある情報が削除され、ONTAPが適切な外部リソースから最新の情報を取得するように強制的に実行されます。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。

タスクの内容

エクスポートポリシーキャッシュの情報は、次の理由で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が最近変更された
- ネームサーバのホスト名レコードに対する最近の変更
- ネームサーバのネットグループエントリに対する最近の変更
- ネットグループのフル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. ネームサービスキャッシュを有効にしていない場合は、 advanced 権限モードで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 `-node`。
ホスト名キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache host`
ネットグループキャッシュ	`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`

2. ネームサービスキャッシュが有効になっている場合は、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
エクスポートポリシールール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 `-node`。
ホスト名キャッシュ	`vserver services name-service cache hosts forward-lookup delete-all`

フラッシュ対象	入力するコマンド
ネットグループキャッシュ	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all`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のネットグループキューとキャッシュを表示する

ONTAP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、結果の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関連の問題をトラブルシューティングするときは、コマンドと `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とネットグループキャッシュの内容を表示できます `vserver export-policy netgroup queue show`。

ステップ

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であるかどうかを確認する

ネットグループに関連するNFSクライアントアクセスの問題をトラブルシューティングするときは、コマンドを使用して、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 `vserver export-policy netgroup check-membership`。

タスクの内容

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ことまた

はメンバーでないことを 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 ONTAP 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、クライアントに対して予期せずアクセスが許可または拒否される理由を理解するのに役立ちます。

ステップ

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確認します。 `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   このコマンドによって次のような結果が返されることがあります。

   - クライアントはネットグループのメンバーです。

     これは、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。

     クライアントが 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。
   - ONTAP が現在ネットグループキャッシュを更新中なので、まだクライアントのメンバーシップを決定できません。

     これが完了するまで、メンバーシップの判断を明示的に下すことはできません。コマンドを使用し `vserver export-policy netgroup queue show`てネットグループのロードを監視し、ロード完了後にチェックを再試行します。

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
```

アクセスキャッシュのパフォーマンスを最適化

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に格納される情報の鮮度とのバランスをとったりすることができます。

タスクの内容

アクセスキャッシュの更新期間を設定するときは、次の点に注意してください。

- 値を大きくすると、アクセスキャッシュ内のエントリの保持期間が長くなります。

  長所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの減少によるパフォーマンスの向上が挙げられます。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、エントリの更新にかかる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権を取得する可能性があります。

- 値を小さくすると、 ONTAP によるアクセスキャッシュエントリの更新頻度が高くなります。

  長所は、エントリの鮮度が向上し、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、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの増加によるパフォーマンスの低下が挙げられます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

変更の対象	入力するコマンド
正のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
負のエントリの更新期間	`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
   ```

ファイルロックを管理します。

プロトコル間のファイルロックについて

ファイルロックは、別のユーザが以前に開いていたファイルにユーザがアクセスできないようにするためにクライアントアプリケーションで使用される方法です。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クライアントの場合はロックを推奨します。クライアントがSMBクライアントの場合はロックは必須です。

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以前に開いたファイルにNFSクライアントからアクセスすると失敗することがあります。

NFSクライアントがSMBアプリケーションでロックされているファイルにアクセスしようとすると、次の状況が発生します。

- mixed形式またはNTFS形式のボリュームでは、、 `rmdir`などのファイル操作を `rm`mv`行うと、NFSアプリケーションが失敗することがあります。
- NFSの読み取り処理と書き込み処理は、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。
- ファイルの書き込み範囲が排他的なSMBバイトロックでロックされている場合、NFSの書き込み処理が失敗します。

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上の他のすべてのNFS処理では、SMBロック状態が維持されます。

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ます。

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。

ONTAP 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、 ONTAP は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。 ONTAP

- 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、 ONTAP はそのファイルの読み取り専用ビットを有効にします。
- 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、 ONTAP はそのファイルの読み取り専用ビットを無効にします。
- 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 ONTAP 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クライアントがその読み取り専用ビットを無効にすると、ONTAPはそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 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。

ファイル権限の変更は、 SMB クライアントではすぐに反映されますが、 NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理に関するONTAPとWindowsの違い

Windowsとは異なり、ONTAPはファイルが開いている間、開いているファイルへのパスの各コンポーネントをロックしません。この動作はSMB共有パスにも影響します。

ONTAPではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。その結果、共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、Windows Access Control List（ACL；アクセス制御リスト）のセキュリティ設定を適用して、ユーザやアプリケーションが重要なディレクトリの名前を変更できないようにします。

詳細については、をご覧ください "クライアントがアクセスしている間にディレクトリの名前を変更しないようにする方法"。

ロックに関する情報を表示する

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。

タスクの内容

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。

`vserver locks show`このコマンドは、次の4種類のロックに関する情報を表示します。

- 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、各ロックタイプ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。

ステップ

1. コマンドを使用して、ロックに関する情報を表示します `vserver locks show`。

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。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
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します `/data2/data2_2/intro.pptx`。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

ファイルロックによってクライアントがファイルにアクセスできない場合は、現在有効なロックに関する情報を表示して、特定のロックを解除できます。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。

タスクの内容

コマンドは `vserver locks break`、advanced権限レベル以上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、コマンドを使用し `vserver locks show`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`

4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSでの**FPolicy**の**first-read**および**first-write**フィルタの動作

外部FPolicyサーバを使用してFPolicyが有効になっていて、読み取り/書き込み操作が監視対象イベントとして設定されている場合、読み取り/書き込み要求のトラフィックが多いときにNFSクライアントの応答時間が長くなります。NFSクライアントの場合、FPolicyでfirst-readフィルタとfirst-writeフィルタを使用すると、FPolicy通知の数が減り、パフォーマンスが向上します。

NFSでは、クライアントはファイルのハンドルを取得してI/Oを実行します。このハンドルは、サーバおよびクライアントのリブート後も有効なままになることがあります。したがって、クライアントはハンドルを自由にキャッシュし、ハンドルを再度取得することなく、ハンドルに対する要求を送信できます。通常のセッションでは、大量の読み取り / 書き込み要求がファイルサーバに送信されます。これらすべての要求に対して通知が生成されると、次の問題が発生する可能性があります。

- 追加の通知処理が原因で負荷が大きくなり、応答時間が長くなります。
- サーバがすべての通知の影響を受けていないにもかかわらず、多数の通知がFPolicyサーバに送信される。

特定のファイルに対するクライアントからの最初の読み取り/書き込み要求を受信すると、キャッシュエントリが作成され、読み取り/書き込み数が増分されます。この要求は初回読み取り/書き込み処理とマークされ、FPolicyイベントが生成されます。NFSクライアント用のFPolicyフィルタを計画して作成する前に、FPolicyフィルタの基本的な仕組みを理解しておく必要があります。

- first-read：初回読み取りのクライアント読み取り要求をフィルタリングします。

  このフィルタをNFSイベントに使用すると、および `-file-session-io-grouping-duration`の設定によって、`-file-session-io-grouping-count`FPolicyが処理される初回読み取り要求が決定されます。

- first-write：first-writeのクライアント書き込み要求をフィルタリングします。

  このフィルタをNFSイベントに使用すると、 `-file-session-io-grouping-count`および `-file-session-io-grouping-duration`の設定によって、FPolicyが処理された初回書き込み要求が決定されます。

次のオプションがNFSサーバデータベースに追加されます。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

NFSv4.1サーバ実装**ID**を変更する

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。サーバ実装 ID のデフォルト値は変更できます。デフォルト値を変更すると、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トラブルシューティングしたりするときに役立ちます。詳細については、 RFC 5661 を参照してください。

タスクの内容

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 -ドメイン	`-v4.1-implementation -domain`	NetApp .com
NFSv4.1実装ID -名前	`-v4.1-implementation-name`	クラスタバージョンの名前
NFSv4.1実装ID -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を管理します。

NFSv4 ACLを有効にする利点

NFSv4 ACLを有効にすると、多くのメリットがあります。

NFSv4 ACLを有効にする利点は次のとおりです。

- 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セキュリティの強化
- CIFSとの相互運用性の向上
- NFS のユーザあたりの最大グループ数は 16 ではなくなりました

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が設定されたディレクトリに新しいファイルまたはサブディレクトリを作成すると、新しいファイルまたはサブディレクトリには、該当する継承フラグが設定されたACL内のすべてのAccess Control Entry（ACE；アクセス制御エントリ）が継承されます。

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が含まれている場合は、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に適切な継承フラグが設定されていれば、それらのACEが新しいファイルまたはディレクトリに継承されます。

  親ACLは、がに設定されている `off`場合でも継承され `-v4.0-acl`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。

または `vserver export-policy rule`ファミリーのコマンドで `vserver nfs`パラメータをに設定した `restricted`場合 `-chown-mode`は、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザにファイル所有権の変更が許可されていても、スーパーユーザのみがファイル所有権を変更できます。詳細については、関連するマニュアルページを参照してください。

NFSv4 ACLの変更を有効または無効にする

ONTAPがACLを含むファイルまたはディレクトリに対するコマンドを受信した場合、`chmod`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するように変更されます。代わりにACLをドロップする場合は、パラメータをディセーブルにして動作を変更できます `-v4-acl-preserve`。

タスクの内容

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ときに、NTFSファイル権限を保持するか破棄するかを指定します。

このパラメータのデフォルトは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
   ```

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、 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を有効または無効にする

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

タスクの内容

`-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。

ステップ

1. 次のいずれかを実行します。

状況	そしたら…。
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ACEの最大数を変更する

パラメータを変更すると、各NFSv4 ACLに許可されるACEの最大数を変更できます `-v4-acl-max-aces`。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。この制限値を増やすと、400個を超えるACEを含むACLのデータをONTAPを実行するストレージシステムに移行する際に役立ちます。

タスクの内容

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の最大数を変更します。

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

有効な範囲

`max_ace_limit`で `192`ある `1024.`

3. admin権限レベルに戻ります。

```
set -privilege admin
```

NFSv4ファイル委譲を管理します。

NFSv4読み取りファイル委譲を有効または無効にする

NFSv4読み取りファイル委譲を有効または無効にするには、オプション-v4.0-read-delegationまたは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。

タスクの内容

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。

ステップ

1. 次のいずれかを実行します。

状況	そしたら…。
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します	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`

結果

ファイル委譲オプションは、変更されるとすぐに有効になります。NFSをリブートしたり再起動したりする必要はありません。

NFSv4書き込みファイル委譲を有効または無効にする

書き込みファイル委譲を有効または無効にするには、オプション`-v4.0-write -delegation`または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。

タスクの内容

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。

ステップ

1. 次のいずれかを実行します。

状況	そしたら...。
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`
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します	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します	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

結果

ファイル委譲オプションは、変更されるとすぐに有効になります。NFSをリブートしたり再起動したりする必

要はありません。

NFSv4ファイルおよびレコードロックの設定

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、 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。

"NetAppテクニカルレポート3580：『NFSv4の拡張機能とベストプラクティスガイド：Data ONTAPでの実装』"

NFSv4ロックリース期間を指定する

NFSv4ロックリース期間（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、オプションを変更します `-v4-lease-seconds`。リース期間を短くするとサーバのリカバリにかかる時間が短縮され、リース期間を長くすると、大量のクライアントを処理するサーバに効果的です。

タスクの内容

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

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をONTAPに再要求する期間）を指定するには、オプションを変更します `-v4-grace-seconds`。

タスクの内容

デフォルトでは、このオプションはに設定されて `45`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、 ONTAP は NFSv4 クライアントに対して「 SVM 内」のリファーラルを提供します。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）の別の論理インターフェイス（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返すのは、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リファーラルを有効または無効にする

Storage Virtual Machine（SVM）でNFSv4リファーラルを有効にするには、オプションと`-v4.0-referrals`またはを有効にし`-v4-fsid-change`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アクセス速度が向上します。

必要なもの

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
   ```

NFS統計の表示

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のNFS統計を表示することができます。

手順

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

   ```
   statistics catalog object show -object nfs*
   ```

2. コマンドとオプションの `statistics stop`コマンドを使用し `statistics start`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. サンプルデータを表示するには、コマンドを使用し `statistics show`ます。

例：**NFSv3**のパフォーマンスの監視

次の例は、NFSv3プロトコルのパフォーマンスデータを表示します。

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、成功した読み取り要求と書き込み要求の数と読み取り要求と書き込み要求の総数を比較するカウンタを指定して、サンプルから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
```

関連情報

"パフォーマンス監視のセットアップ"

DNS統計を表示します。

パフォーマンスを監視して問題を診断するために、ストレージ システム上のStorage Virtual Machine（SVM）のDNS統計を表示することができます。

手順

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

   ```
   statistics catalog object show -object external_service_op*
   ```

2. コマンドと `statistics stop`コマンドを使用して `statistics start`、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. サンプルデータを表示するには、コマンドを使用し `statistics show`ます。

DNS統計の監視

次の例は、DNSクエリのパフォーマンスデータを表示します。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 external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

次のコマンドは、送信したDNSクエリの数と、受信した、失敗した、またはタイムアウトしたDNSクエリの

数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバのDNSクエリについて特定のエラーを受信した回数を表示するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

関連情報

"パフォーマンス監視のセットアップ"

NIS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のNIS統計を表示することができます。

手順

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

   ```
   statistics catalog object show -object external_service_op*
   ```

2. コマンドと `statistics stop`コマンドを使用して `statistics start`、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. サンプルデータを表示するには、コマンドを使用し `statistics show`ます。

NIS統計の監視

次の例は、NISクエリのパフォーマンスデータを表示します。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 external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

次のコマンドは、送信したNISクエリの数と、受信した、失敗した、またはタイムアウトしたNISクエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバのNISクエリについて特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                            YP_NOTFOUND
    server_ip_address                                     10.227.13.221
3 entries were displayed.
```

関連情報

"パフォーマンス監視のセットアップ"

VMware vStorage over NFSのサポート

ONTAPは、NFS環境で特定のVMware vStorage APIs for Array Integration（VAAI）機能をサポートします。

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ホストは、仮想マシンまたは仮想マシンディスク（VMDK）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コピーできます。これにより、ESXiホストのCPUサイクルとネットワーク帯域幅が節約されます。ソースボリュームがスパースの場合、コピーオフロードでスペース効率が維持されます。

- 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

VMware vStorage over NFSには、次の制限事項があります。

- 次の場合、コピーオフロード処理が失敗することがあります。
  - ソースボリュームまたはデスティネーションボリュームで wafliron を実行中に、ボリュームが一時的にオフラインになっている
  - 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
  - スイッチオーバーまたはスイッチ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が原因でサーバ側のコピーが失敗することがあります。

  qtreeを現在エクスポートしている、または以前にエクスポートしていたSVMから、これまでにqtreeをエクスポートしたことがないSVMにデータをコピーしようとします。この制限を回避するには、デスティネーション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

"Data ONTAPでは、どのようなVAAIオフロード処理がサポートされていますか。"

VMware vStorage over NFSの有効化または無効化

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、コマンドを使用し `vserver nfs modify`ます。

タスクの内容

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. SVMの現在のvStorage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

この機能を使用する前に、NFS Plug-in for VMware VAAIをインストールする必要があります。詳細については、「 NetApp NFS Plug-in for VMware VAAI のインストール」を参照してください。

関連情報

"NetAppのマニュアル：NetApp NFS Plug-in for VMware VAAI"

rquotaのサポートを有効または無効にする

ONTAP 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のクォータ情報を取得できます。Storage Virtual Machine（SVM）でrquotaを有効にするには、コマンドを使用し `vserver nfs modify`ます。

タスクの内容

デフォルトでは、 rquota は無効です。

ステップ

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します	`vserver nfs modify -vserver vserver_name -rquota enable`
SVM で rquota のサポートを無効にします	`vserver nfs modify -vserver vserver_name -rquota disable`

クォータの詳細については、を参照してください"論理ストレージ管理"。

TCP 最大転送サイズを変更することで、高レイテンシ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 / NFSv4 クライアントのパフォーマンスを向上させることができます。

レイテンシが 10 ミリ秒を超えるワイドエリアネットワーク（ WAN ）またはメトロエリアネットワーク（ MAN ）などの高レイテンシネットワークを介してクライアントがストレージシステムにアクセスしている場合は、 TCP 最大転送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を向上させることができます。ローカルエリアネットワーク（ LAN ）などの低レイテンシ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レイテンシの影響を上回らない場合は、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レイテンシ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。このような状況では、クライアントとサーバは、接続を介して送信される小さな要求と応答を待機するデューティサイクルの大部分を消費するため、使用可能な帯域幅を完全に使用することはできません。

NFSv3 と NFSv4 の要求サイズを大きくすることで、クライアントとサーバは使用可能な帯域幅をより効果的に使用できるようになり、単位時間あたりの移動データ量が多くなります。そのため、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注意してください。ストレージシステムとクライアントでサポートされる転送処理の最大サイズは 1MB です。ただし、ストレージシステムで最大転送サイズを 1MB に設定しても、クライアントがサポートするサイズが 64KB であると、マウントの転送サイズは 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、変更すると、大量の応答をアセンブルして送信するのに時間がかかり、ストレージシステムで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レイテンシ接続が増えるほど、メモリ消費量も増加します。メモリ容量が多いストレージシステムでは、この変更による影響はほとんどありません。メモリ容量が少な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効果的に使用するには、クラスタの複数のノードからデータを取得する必要があります。クラスタネットワーク固有のレイテンシによって、応答の全体的なレイテンシが増加す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、全体的なレイテンシが増大する傾向があります。そのため、レイテンシの影響を受けやすいワークロードは悪影響を受ける可能性があります。

NFSv3および**NFSv4**の**TCP**最大転送サイズを変更する

NFSv3およびNFSv4.xプロトコルを使用するすべてのTCP接続に対して最大転送サイズを設定するオプションを変更できます `-tcp-max-xfer-size`。

タスクの内容

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。

ONTAP 9以降では、 `v3-tcp-max-read-size`オプションと `v3-tcp-max-write-size`オプションは廃止されています。代わりにオプションを使用する必要があり `-tcp-max-xfer-size`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またはNFSv4のTCP最大転送サイズを変更する	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

オプション	範囲	デフォルト
`-tcp-max-xfer-size`	8192~1048576バイト	65536バイト

> 最大転送サイズは4KB（4096バイト）の倍数にする必要があります。要求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. コマンドを使用し `vserver nfs show -fields tcp-max-xfer-size`て変更を確認します。
4. 静的マウントを使用するクライアントがある場合は、アンマウントおよび再マウントして新しいパラメータサイズを有効にします。

例

次のコマンドは、vs1というSVMでNFSv3とNFSv4.xのTCP最大転送サイズを1、048576バイトに設定します。

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

NFSユーザに許可するグループ**ID**の数を設定する

ONTAPでは、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がサポートされます。AUTH_SYS認証を使用する場合、RFC 5531で定義されているように、グループIDのデフォルトの最大数は16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。

タスクの内容

デフォルト数を超えるグループIDがクレデンシャルに設定されている場合、残りのグループIDは切り捨てられ、ストレージシステムのファイルにアクセスしようとするとエラーが表示されることがあります。SVMあたりのグループの最大数は、環境内の最大グループ数に相当する数に設定する必要があります。

> 拡張グループを有効にするためのAUTH_SYS認証の前提条件を理解するには(`-auth-sys-extended-groups`、次のナレッジベースの記事を参照してください。 "AUTH_SYS拡張グループによるONTAP 9のNFS認証の変更"

次の表に、グループIDの最大数を決定するコマンドの2つのパラメータを3つの設定例で示し `vserver nfs modify`ます。

パラメータ	設定	結果として得られるグループ ID の上限数

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	これらはデフォルト設定です。
		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

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

許可される補助グループの最大数の設定対象	入力するコマンド
RPCSEC_GSSの場合のみ、AUTH_SYSはデフォルト値の16のままにします。	`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. 値を確認し `-extended-groups-limit`、拡張グループがAUTH_SYSで使用されているかどうかを確認します。 `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

次に、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に設定する例を示します。これらの変更は、vs1というSVM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**ユーザアクセスを制御する

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セキュリティ形式のデータへのアクセスを許可したりするようにONTAPを設定できます。NFSデータストアでNTFSセキュリティ形式を使用する場合は、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。

タスクの内容

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場合は、次の2つのオプションがあります。

- 他の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します。
- NTFS ACLを無視し、rootにフルアクセスを提供します。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 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`

NT ACLチェックのバイパス	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

デフォルトでは、このパラメータは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ない場合、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
```

サポートされる**NFS**のバージョンとクライアント

サポートされる**NFS**のバージョンとクライアントの概要

ネットワークでNFSを使用する前に、ONTAPがサポートする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。

次の表は、ONTAPでNFSプロトコルのメジャーバージョンとマイナーバージョンがデフォルトでサポートされる状況を示しています。デフォルトでサポートされるONTAPは、そのNFSプロトコルをサポートする最も古いバージョンであるとは限りません。

バージョン	サポート対象	導入済み
NFSv3	○	すべてのONTAPリリース
NFSv4.0	○	ONTAP 8
NFSv4.1	○	ONTAP 8.1
NFSv4.2	○	ONTAP 9.8
pNFS	○	ONTAP 8.1

ONTAPでサポートされるNFSクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ONTAPでサポートされる**NFSv4.0**の機能

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

次の NFSv4 機能がサポートされます。

- * コンパウンド *

  クライアントは、 1 つのリモート手順呼び出し（ RPC ）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、一部のタイプのクライアントにファイル制御を委譲して読み取りおよび書き込みアクセスを許可します。

- * 擬似 fs *

  NFSv4 サーバでストレージシステム上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。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。

NFSv4の**ONTAP**サポートの制限事項

ONTAPでのNFSv4の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でサポートされているわけではありません。
- ONTAP 9 .4以前のリリースでは、UTF8以外のボリュームでASCII以外の文字を含む名前はストレージシステムで拒否されます。

  ONTAP 9 .5以降のリリースでは、utf8mb4言語設定で作成され、NFS v4を使用してマウントされたボリュームにはこの制限は適用されなくなりました。

- すべてのファイルハンドルは永続的です。サーバは揮発性ファイルハンドルを提供しません。
- 移行とレプリケーションはサポートされていません。
- NFSv4クライアントは、読み取り専用負荷共有ミラーではサポートされていません。

  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用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ていません。
- 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

> 属性はサポートされませ `quota*`んが、ONTAPはRQUOTA側のバンドプロトコルを通じてユーザクォータとグループクォータをサポートします。

ONTAPでの**NFSv4.1**のサポート

NFSv4.1が有効になっている場合、NFSv.8以降でONTAP 9はデフォルトでnconnect機能を使用できます。

以前のNFSクライアント実装では、マウントでTCP接続を1つしか使用しません。ONTAPでは、1つのTCP接続がIOPSの増加に伴うボトルネックになる可能性があります。ただし、nconnect対応クライアントは、1つのNFSマウントに複数のTCP接続（最大16）を関連付けることができます。このようなNFSクライアントでは、ファイル操作が複数のTCP接続にラウンドロビン方式で多重化されるため、使用可能なネットワーク帯域幅からより高いスループットが得られます。nconnectは、NFSv3とNFSv4.1のマウントでのみ推奨されます。

NFS クライアントのマニュアルを参照して、 nConnect がクライアントバージョンでサポートされているかどうかを確認してください。

ONTAP 9.9.1以降では、NFSv4.1がデフォルトで有効になっています。以前のリリースでは、Storage Virtual Machine（SVM）にNFSサーバを作成するときにオプションを指定し、に設定する `enabled`ことで有効にすることができ `-v4.1`ました。

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

NFSv4 4.2 の **ONTAP** サポート

ONTAP 9 .8以降では、ONTAPでNFSv4.2プロトコルがサポートされ、NFSv4.2対応クライアントのアクセスが許可されます。

NFSv4.2は、ONTAP 9 .9.1以降ではデフォルトで有効になっています。ONTAP 9 .8では、Storage Virtual Machine（SVM）にNFSサーバを作成するときにオプションを指定してに設定し `enabled`、v4.2を手動で有効にする必要があります。 `-v4.1`NFSv4.1を有効にすると、クライアントはv4.2としてマウントした状態でNFSv4.1の機能を使用できるようになります。

ONTAPの以降のリリースでは、NFSv4.2のオプション機能のサポートが拡張されています。

最初の文字	**NFSv4.2**のオプションの機能
ONTAP 9 12.1	• NFS拡張属性 • スパースファイル • スペースリザベーション

最初の文字	**NFSv4.2**のオプションの機能
ONTAP 9 .9.1	NFSラベルのMandatory Access Control（MAC；必須アクセス制御）

NFS v4.2セキュリティラベル

ONTAP 9 .9.1以降では、NFSセキュリティラベルを有効にできます。デフォルトでは無効になっています。

NFS v4.2セキュリティラベルでは、ONTAP NFSサーバは必須アクセス制御（MAC）に対応し、クライアントから送信されたsec_label属性を格納および取得します。

詳細については、を参照してください "RFC 7240"。

手順

1. 権限の設定をadvancedに変更します。

```
set -privilege advanced
```

2. セキュリティラベルを有効にします。

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS拡張属性

ONTAP 9.12.1以降では、NFS拡張属性（xattrs）がデフォルトで有効になっています。

拡張属性は、最新のNFSクライアントで定義され、有効になっている標準のNFS属性です "RFC 8276"。ユーザ定義のメタデータをファイルシステムオブジェクトに添付するために使用でき、高度なセキュリティの導入に役立ちます。

NFS拡張属性は、現在のところNDMPダンプ処理ではサポートされていません。ファイルまたはディレクトリで拡張属性が検出されると、ダンプは続行されますが、それらのファイルまたはディレクトリの拡張属性はバックアップされません。

拡張属性を無効にする必要がある場合は、コマンドを使用し `vserver nfs modify -v4.2-xattrs disabled`ます。

Parallel NFSのONTAPサポート

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。これにより、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。

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ときは、正しい種類のマウントを使用し

ていることを確認する必要があります。NFS は、ソフトマウントとハードマウントの 2 つのマウントタイプをサポートしています。信頼性を確保するために、ハードマウントのみを使用してください。

特に NFS タイムアウトが頻繁に発生する可能性がある場合は、ソフトマウントは使用しないでください。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。

NFSトSMBノファアイルオヨヒテイレクトリノメイメイキソク

NFSトSMBノファアイルオヨヒテイレクトリノメイメイキソクノカイヨウ

ファイルとディレクトリの命名規則は、 ONTAP クラスタおよびクライアントの言語設定に加え、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ファイル共有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ファイル共有プロトコルによって、次の項目が決まります。

- 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

ONTAPでは、ONTAPのリリースに応じて、ファイル、ディレクトリ、およびqtreeの名前でマルチバイト文字がサポートされます。

ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、 UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン（ : ）を使用しないでください。コロンは、 MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限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。

マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。マルチプロトコル環境におけるこれらの影響と、SMB共有の作成時にパスを指定する場合や、共有内のデータにアクセスする場合に実行する必要がある対処方法を理解しておく必要があります。

SMBクライアントでという名前のディレクトリを作成すると、 `testdir`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `testdir`。ただし、SMBユーザがあとでディレクトリ名を作成しようとすると、SMBクライアントではその名前がすでに存在しているとみなされるため作成 `TESTDIR` できません。NFSユーザがあとでという名前のディレクトリを作成すると、 `TESTDIR`このディレクトリ名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ディレクトリ名の大文字と小文字が区別されるため、両方のディレクトリ名が作成したとおりにと `TESTDIR`表示されます（例：） `testdir`。

- SMBクライアントでは、2つのディレクトリを区別するために8.3形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TESTDI~1`表示され `testdir`ます。
  - ONTAPは、2つのディレクトリを区別するためにディレクトリ名を作成します `TESTDI~1`。

    この場合、Storage Virtual Machine（SVM）で共有を作成または変更するときに共有パスを指定するときは、8.3形式の名前を使用する必要があります。

ファイルについても同様に、SMBクライアントでを作成すると、 `test.txt`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `text.txt`。ただし、SMBユーザがあとでを作成しようとすると、 `Test.txt`SMBクライアントではその名前がすでに存在しているとみなされるため作成できません。NFSユーザがという名前のファイルをあとで作成すると、 `Test.txt`このファイル名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ファイル名の大文字と小文字が区別されるため、両方のファイル名が作成したとおりに、およびと `Test.txt`表示されます `test.txt`。
- SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。1つのファイルにはベースファイル名が付いています。追加のファイルには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TEST~1.TXT`表示され `test.txt`ます。
  - ONTAPは、2つのファイルを区別するためにファイル名を作成します `TEST~1.TXT`。

> Vserver cifs character-mappingコマンドを使用して文字マッピングを作成した場合、通常は大文字と小文字が区別されないWindows検索では大文字と小文字が区別される可能性があります。これは、文字マッピングが作成されていて、ファイル名がその文字マッピングを使っている場合にのみ、ファイル名のルックアップで大文字小文字が区別されることを意味します。

ONTAPでのファイル名とディレクトリ名の作成方法

ONTAP は、 SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2 つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、 ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（ ~ ）と 1~5 の数字が追加されます。

  同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成する `specifications.html`と、ONTAPではという`8.3`形式のファイル名が作成されます `specif~1.htm`。この名前がすでに存在する場合、 ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという別のファイルを作成する

と `specifications_new.html`、の8.3形式は `specifications_new.html`になり `specif~2.htm`ます。

マルチバイトのファイル名、ディレクトリ名、**qtree**名の**ONTAP**での処理

ONTAP 9 .5以降では、4バイトのUTF-8エンコード名がサポートされているため、基本多言語面（BMP）以外のUnicode補助文字を含むファイル名、ディレクトリ名、ツリー名を作成および表示できます。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8エンコード名のサポートを有効にするために、コマンドファミリーと `volume`コマンドファミリーで新しい_utf8mb4_言語コードを使用でき `vserver`ます。

- 次のいずれかの方法で新しいボリュームを作成する必要があります。
- ボリューム・オプションを明示的に設定し `-language`ます。

  ```
  volume create -language utf8mb4 {…}
  ```

- ボリュームオプションを指定して作成または変更されたSVMからボリュームオプションを継承し `-language`ます。

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- ONTAP 9 .6以前を使用している場合、utf8mb4をサポートするために既存のボリュームを変更することはできません。utf8mb4対応の新しいボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

  ONTAP 9 .7P1以降を使用している場合は、utf8mb4の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください "ONTAPでの作成後にボリュームの言語を変更できますか。"。

+ SVMはutf8mb4をサポートするように更新できますが、既存のボリュームの言語コードは元のままです。

+

> 4バイトのUTF-8文字を使用するLUN名は現在サポートされていません。

- 通常、Unicode文字データは、Windowsファイルシステムアプリケーションでは16-bit Unicode Transformation Format（UTF-16）を使用し、NFSファイルシステムでは8-bit Unicode Transformation Format（UTF-8）を使用して表されます。

  ONTAP 9 .5より前のリリースでは、Windowsクライアントで作成されたUTF-16の補助文字を含む名前は他のWindowsクライアントには正しく表示されましたが、NFSクライアントではUTF-8に正しく変換されませんでした。同様に、NFSクライアントで作成されたUTF-8の補助文字を含む名前は、Windowsクライアントでは正しく変換されませんでした。

- ONTAP 9 .4以前を実行しているシステムで、有効または無効な補助文字を含むファイル名を作成すると、ONTAPはファイル名を拒否し、無効なファイル名エラーを返します。

  この問題を回避するには、ファイル名にBMP文字のみを使用して補助文字を使用しないようにするか、ONTAP 9 .5以降にアップグレードしてください。

qtree名にはUnicode文字を使用できます。

- qtree名を設定または変更するには、コマンドファミリーまたはSystem Managerを使用し `volume qtree` ます。
- qtree名には、日本語や中国語などのUnicode形式のマルチバイト文字を含めることができます。
- ONTAP 9 .5より前のリリースでは、BMP文字（つまり、3バイトで表現できる文字）のみがサポートされていました。

> ONTAP 9 .5より前のリリースでは、qtreeの親ボリュームのジャンクションパスに、Unicode文字を使用したqtree名とディレクトリ名を含めることができます。 `volume show`親ボリュームの言語設定がUTF-8の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定がUTF-8のいずれかでない場合は、ジャンクションパスの一部が数値のNFS名に置き換えられて表示されます。

- 9.5以降のリリースでは、utf8mb4が有効なボリュームにqtreeが含まれていれば、qtree名で4バイト文字がサポートされます。

ボリュームでの**SMB**ファイル名の変換のための文字マッピングの設定

NFSクライアントは、SMBクライアントおよび特定のWindowsアプリケーションで無効な文字を含むファイル名を作成できます。ボリュームでのファイル名の変換のための文字マッピングを設定すると、本来は無効なNFS名を持つファイルにSMBクライアントからアクセスできるようになります。

タスクの内容

SMBクライアントがNFSクライアントによって作成されたファイルにアクセスすると、ONTAPはファイル名を確認します。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、 ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、重要な情報を長いファイル名にエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステム上のクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMBクライアントで有効でない文字を含むファイル名をNFSクライアントが作成する場合は、無効なNFS文字をSMBと特定のWindowsアプリケーションの両方で使用できるUnicode文字に変換するマップを定義できます。たとえば、この機能は、CATIA MCADおよびMathematicaアプリケーションだけでなく、この要件を持つ他のアプリケーションもサポートしています。

文字マッピングはボリューム単位で設定できます。

ボリュームに文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイント全体には適用されません。

  文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字または不正な文字を表すUnicode文字は、通常はファイル名に使用されない文字であることを確認する必要があります。使用されていないと、不要なマッピングが発生します。

  たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用さ

れていれば 'Windows クライアントが "a-b`" という名前のファイルにアクセスしようとすると ' その要求は NFS 名 "a:b`" にマップされます (望ましい結果ではありません)

- 文字マッピングを適用したあともマッピングに無効なWindows文字が含まれている場合、ONTAPはWindows 8.3ファイル名にフォールバックします。
- FPolicy通知、NAS監査ログ、およびセキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- DPタイプのSnapMirror関係が作成された場合、ソースボリュームの文字マッピングはデスティネーションDPボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされたWindows名はNFS名に変わるため、名前の検索はNFSのセマンティクスに従って行われます。これには、NFS検索では大文字と小文字が区別されることも含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windowsの大文字と小文字を区別しない動作に依存してはなりません。ただし8.3形式の名前は使用可能で、大文字と小文字は区別されません。
- 部分マッピングまたは無効なマッピング：名前をマッピングしてディレクトリ列挙（「dir」）を実行するクライアントに戻ったあと、生成されたUnicode名がWindowsで有効かどうかがチェックされます。その名前に無効な文字が含まれている場合、またはWindowsで無効な文字が含まれている場合（例：「.」または空白で終わる場合）は、無効な名前の代わりに8.3形式の名前が返されます。

ステップ

1. 文字マッピングを設定します。

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   マッピングは、「 : 」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16進数を使用して入力されたUnicode文字です。例： 3C ： E03C

   コロンで区切られた各ペアの最初の値 `mapping_text`は、変換するNFS文字の16進値です。2番目の値は、SMBで使用されるUnicode値です。マッピングペアは一意である必要があります（1対1のマッピングが存在する必要があります）。

   - ソースマッピング

     次の表に、ソースマッピングで許可されるUnicode文字セットを示します。

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C	\	バックスラッシュ
0x3A	：	コロン
0x2A	*	アスタリスク
0x3F	?	疑問符

0x22	"	引用符
0x3C	<	より小さい
0x3E	>	次の値より大きい
0x7C		
縦線	0xB1	±

◦ ターゲットマッピング

ターゲット文字には、 U+E0000…U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、 Storage Virtual Machine （ SVM ） vs1 上の「 data 」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

SMBファイル名の変換のための文字マッピングの管理用コマンド

文字マッピングを管理するには、FlexVolでSMBファイル名の変換に使用する情報を作成、変更、表示、または削除します。

状況	使用するコマンド
新しいファイル文字マッピングを作成する	`vserver cifs character-mapping create`
ファイル文字マッピングに関する情報を表示する	`vserver cifs character-mapping show`
既存のファイル文字マッピングを変更する	`vserver cifs character-mapping modify`
ファイル文字マッピングを削除します。	`vserver cifs character-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。

NFSトランキングを管理します。

ONTAP NFSトランキングの詳細

NFSv4.1クライアントでは、セッショントランキングを利用してNFSサーバ上の異なるLIFへの複数の接続を開くことができます。これにより、データ転送速度が向上し、マルチパスによる耐障害性が実現しますONTAP 9。

トランキングは、FlexVolボリュームをトランキング対応のクライアント（特にVMwareおよびLinuxクライアント）にエクスポートする場合や、NFS over RDMA、TCP、pNFSにエクスポートする場合に便利です。

lif.14.1では、トランキングは1つのノードのONTAP 9に制限されています。トランキングは複数のノードにまたがるLIFにはできません。

FlexGroupボリュームはトランキングでサポートされています。これによりパフォーマンスは向上しますが、FlexGroupボリュームへのマルチパスアクセスはシングルノードでしか設定できません。

このリリースのマルチパスでは、セッショントランキングのみがサポートされます。

トランキングの使用方法

トランキングによるマルチパスのメリットを活用するには、トランキング対応NFSサーバがあるSVMに関連付けられた一連のLIF（_trunking group_と呼ばれます）が必要です。トランキンググループ内のLIFは、クラスタの同じノードにホームポートがあり、それらのホームポートに配置されている必要があります。トランキンググループ内のすべてのLIFが同じフェイルオーバーグループのメンバーであることを推奨します。

ONTAPでは、1つのクライアントからノードあたり最大16のトランク接続がサポートされます。

クライアントがトランキング対応サーバからエクスポートをマウントする場合、クライアントはトランキンググループ内のLIFのIPアドレスの数を指定します。クライアントが最初のLIFに接続したあとに追加されたLIFは、NFSv4.1セッションに追加され、トランキンググループの要件を満たしている場合にのみトランキングに使用されます。クライアントは、独自のアルゴリズム（ラウンドロビンなど）に基づいて、複数の接続にNFS処理を分散します。

最大のパフォーマンスを得るには、シングルパスエクスポートではなく、マルチパスエクスポート専用のSVMでトランキングを設定します。つまり、トランキングが有効なクライアントのみにエクスポートが提供されているSVM内のNFSサーバでのみトランキングを有効にします。

サポートされるクライアント

ONTAP NFSv4.1サーバは、NFSv4.1セッショントランキングに対応したすべてのクライアントとのトランキングをサポートしています。

次のクライアントは、ONTAP 9.14.1でテスト済みです。

- VMware-ESXi 7.0U3F以降
- Linux - Red Hat Enterprise Linux（RHEL）8.8および9.3

NFSサーバでトランキングが有効になっている場合、トランキングをサポートしていないNFSクライアントでエクスポートされた共有にアクセスすると、パフォーマンスが低下することがあります。これは、SVMデータLIFへの複数のマウントに使用されるTCP接続が1つだけであるためです。

NFSトランキングと**nconnect**の違い

NFSv4.1が有効になっている場合、NFSv.8以降でONTAP 9はデフォルトでnconnect機能を使用できます。nconnect対応クライアントでは、1つのNFSマウントで、1つのLIFを介して複数のTCP接続（最大16）を確立できます。

一方、トランキングは_multipathing_functionalityで、複数のLIFを介して複数のTCP接続を提供します。環境に追加のNICを使用できる場合は、トランキングによってnconnectの機能を超えた並列処理とパフォーマンスが向上します。

詳細はこちら"nconnect："

トランキング用に新しい**NFS**サーバとエクスポートを設定する

ONTAP SVMにトランキング対応**NFS**サーバを作成する

ONTAP 9.14.1以降では、NFSサーバでトランキングを有効にできます。NFSv4.1は、NFSサーバの作成時にデフォルトで有効になります。

開始する前に

トランキング対応のNFSサーバを作成するにはSVMが必要です。SVMの条件：

- クライアントのデータ要件に対応する十分なストレージを基盤としています。
- NFSに対して有効にします。

既存のSVMを使用できますが、トランキングを有効にするにはすべてのNFSv4.xクライアントを再マウントする必要があるため、システムが停止する可能性があります。再マウントできない場合は、NFSサーバ用に新しいSVMを作成します。

手順

1. 適切なSVMが存在しない場合は作成します。

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. 新しく作成したSVMの設定とステータスを確認します。

   ```
   vserver show -vserver svm_name
   ```

   詳細については、をご覧ください "SVMの作成"。

3. NFSサーバを作成します。

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. NFSが実行されていることを確認します。

   ```
   vserver nfs status -vserver svm_name
   ```

5. NFSが必要に応じて設定されていることを確認します。

   ```
   vserver nfs show -vserver svm_name
   ```

   詳細はこちら"NFSサーバの設定"

終了後

必要に応じて次のサービスを設定します。

- "DNS"
- "LDAP"
- "Kerberos"

ONTAP NFSトランキング用のネットワークの準備

NFSv4.1トランキングを利用するには、トランキンググループ内のLIFが同じノードに配置され、同じノードにホームポートがある必要があります。LIFは、同じノードのフェイルオーバーグループに設定する必要があります。

タスクの内容

LIFとNICを1対1でマッピングするとパフォーマンスが最大限に向上しますが、トランキングを有効にする必要はありません。少なくとも2つのNICをインストールするとパフォーマンスが向上しますが、必須ではありません。

複数のフェイルオーバーグループを設定できますが、トランキングのフェイルオーバーグループにはトランキンググループに含めるLIFだけを指定する必要があります。

フェイルオーバーグループの接続（および基盤となるNIC）を追加または削除するときは、常にトランキングフェイルオーバーグループを調整する必要があります。

開始する前に

- フェイルオーバーグループを作成する場合は、NICに関連付けられているポート名を確認しておく必要があります。
- すべてのポートが同じノード上にある必要があります。

手順

1. 使用するネットワークポートの名前とステータスを確認します。

   ```
   network port status
   ```

2. フェイルオーバーグループを作成します。

   ```
   network interface failover-groups create -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

フェイルオーバーグループは必須ではありませんが、使用することを強く推奨します。

- `*svm_name*`は、NFSサーバが含まれているSVMの名前です。
- `*ports_list*`は、フェイルオーバーグループに追加するポートのリストです。

  ポートは_node_name：port_number_の形式で追加します（例：node1：e0c）。

  次のコマンドは、SVM vs1にフェイルオーバーグループfg3を作成し、ポートを3つ追加します。

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

詳細はこちら"フェイルオーバーグループ："

3. 必要に応じて、トランキンググループのメンバー用のLIFを作成します。

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- `-home-node`- network interface revertコマンドをLIFで実行したときにLIFが戻るノード。

  オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

- `-home-port`は、network interface revertコマンドをLIFに対して実行したときにLIFが戻る物理ポートまたは論理ポートです。
- IPアドレスは、オプションではなく、オプションと `-netmask`オプション `-subnet`で指定できます `-address`。
- 別のIPサブネットにクライアントまたはドメインコントローラがある場合は、IPアドレスを割り当てるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。 `network route create`のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- `-service-policy`- LIFのサービスポリシー。ポリシーを指定しない場合は、デフォルトポリシーが自動的に割り当てられます。コマンドを使用し `network interface service-policy show`て、使用可能なサービスポリシーを確認します。
- `-auto-revert`-起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はfalseですが、環境内のネットワーク管理ポリシーに応じてtrueに設定できます。

  トランキンググループ内のすべてのLIFに対してこの手順を繰り返します。

  次のコマンドは、ノードの `cluster1_01`ポートに `e0c`SVM用 `vs1`にを作成し `lif-A`ます。

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

詳細はこちら"LIFの作成"

4. LIFが作成されたことを確認します。

```
network interface show
```

5. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

ONTAPボリュームエクスポートポリシーを作成する

データ共有へのクライアントアクセスを許可するには、ボリュームを1つ以上作成し、ボリュームに少なくとも1つのルールが設定されたエクスポートポリシーを設定する必要があります。

クライアントのエクスポート要件：

- Linuxクライアントでは、トランキング接続ごと（つまりLIFごと）に、個別のマウントと個別のマウントポイントが必要です。
- VMwareクライアントでは、複数のLIFを指定したエクスポートされたボリュームに対してマウントポイントが1つだけ必要です。

  VMwareクライアントには、エクスポートポリシーでルートアクセスが必要です。

手順

1. エクスポートポリシーを作成します。

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   ポリシー名の最大文字数は256文字です。

2. エクスポートポリシーが作成されたことを確認します。

   ```
   vserver export-policy show -policyname policy_name
   ```

   例

   次のコマンドは、 vs1 という SVM で、 exp1 という名前のエクスポートポリシーを作成し、作成を確認します。

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   パラメータには、 `-clientmatch`エクスポートをマウントするトランキング対応のLinuxまたはVMwareク

ライアントを指定する必要があります。

詳細はこちら"エクスポートルールを作成しています。"

4. ジャンクションポイントを設定してボリュームを作成します。

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

詳細はこちら"ボリュームを作成します。"

5. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

```
volume show -vserver svm_name -volume volume_name -junction-path
```

NFSトランキング用に**ONTAP**ボリュームまたはデータ共有をマウント

トランキングをサポートするLinuxおよびVMwareクライアントは、トランキングが有効になっているONTAP NFSv4.1サーバからボリュームまたはデータ共有をマウントできます。

クライアントでmountコマンドを入力する場合は、トランキンググループ内の各LIFのIPアドレスを入力する必要があります。

詳細はこちらをご覧ください "サポートされるクライアント"。

Linuxクライアントの要件

トランキンググループ内の接続ごとに、個別のマウントポイントが必要です。

次のようなコマンドを使用して、エクスポートしたボリュームをマウントします。

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

version(`vers`）の値は以降である必要があります `4.1`。

この `max_connect`値は、トランキンググループ内の接続数に対応します。

VMwareクライアントの要件

トランキンググループ内の各接続のIPアドレスを含むMOUNTステートメントが必要です。

次のようなコマンドを使用して、エクスポートしたデータストアをマウントします。

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

`-H`値はトランキンググループ内の接続に対応しています。

既存の**NFS**エクスポートをトランキングに適合させる

シングルパスエクスポートの**ONTAP NFS**トランキングへの適合

既存のシングルパス（非トランキング）のNFSv4.1エクスポートでトランキングを使用するように設定できます。トランキング対応のクライアントは、サーバとクライアントの前提条件を満たしていれば、サーバでトランキングが有効になるとすぐにパフォーマンスの向上を利用できます。

シングルパスエクスポートをトランキング用に適応させると、エクスポートされたデータセットを既存のボリュームおよびSVMに保持できます。これを行うには、NFSサーバでトランキングを有効にし、ネットワーク設定とエクスポート設定を更新し、エクスポートされた共有をクライアントに再マウントする必要があります。

トランキングをイネーブルにすると、サーバが再起動されます。VMwareクライアントでは、エクスポートしたデータストアを再マウントする必要があります。Linuxクライアントでは、オプションを使用してエクスポートしたボリュームを再マウントする必要があります `max_connect`。

ONTAP NFSサーバでトランキングを有効にする

トランキングはNFSサーバで明示的に有効にする必要があります。NFSv4.1は、NFSサーバの作成時にデフォルトで有効になります。

トランキングを有効にしたら、次のサービスが必要に応じて設定されていることを確認します。

- "DNS"
- "LDAP"
- "Kerberos"

手順

1. トランキングを有効にし、NFSv4.1が有効になっていることを確認します。

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. NFSが実行されていることを確認します。
   ```
   vserver nfs status -vserver svm_name
   ```
3. NFSが必要に応じて設定されていることを確認します。

   ```
   vserver nfs show -vserver svm_name
   ```

   詳細については、"NFSサーバの設定"このSVMからWindowsクライアントにデータを提供する場合は、共有を移動してからサーバを削除します。
   ```
   vserver cifs show -vserver svm_name
   ```

   +
   ```
   vserver cifs delete -vserver svm_name
   ```

ONTAP NFSトランキング用のネットワークの更新

NFSv4.1トランキングを使用するには、トランキンググループ内のLIFが同じノードに配置され、同じノードにホームポートがある必要があります。すべてのLIFは、同じノードのフェイルオーバーグループに設定する必要があります。

タスクの内容

LIFとNICを1対1でマッピングするとパフォーマンスが最大限に向上しますが、トランキングを有効にするためには必要ありません。

複数のフェイルオーバーグループを設定できますが、トランキングのフェイルオーバーグループにはトランキンググループに含まれるLIFだけを指定する必要があります。

フェイルオーバーグループの接続（および基盤となるNIC）を追加または削除するときは、常にトランキングフェイルオーバーグループを調整する必要があります。

開始する前に

- フェイルオーバーグループを作成するには、NICに関連付けられているポート名を確認しておく必要があります。
- すべてのポートが同じノード上にある必要があります。

手順

1. 使用するネットワークポートの名前とステータスを確認します。

   ```
   network port show
   ```

2. トランキングフェイルオーバーグループを作成するか、既存のフェイルオーバーグループを変更します。

```
network interface failover-groups create -vserver svm_name -failover-group
failover_group_name -targets ports_list

network interface failover-groups modify -vserver svm_name -failover-group
failover_group_name -targets ports_list
```

フェイルオーバーグループは必須ではありませんが、使用することを強く推奨します。

- `svm_name`は、NFSサーバが含まれているSVMの名前です。
- `ports_list`は、フェイルオーバーグループに追加するポートのリストです。

  ポートはの形式で追加され `node_name:port_number`ます（例：） `node1:e0c`。

  次のコマンドは、SVM vs1のフェイルオーバーグループを作成し `fg3`てポートを3つ追加します。

  ```
  network interface failover-groups create -vserver vs1 -failover-group fg3
  -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
  ```

詳細はこちら"フェイルオーバーグループ："

3. 必要に応じて、トランキンググループのメンバー用に追加のLIFを作成します。

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- `-home-node`- network interface revertコマンドをLIFで実行したときにLIFが戻るノード。

  オプションを使用すると、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定できます `-auto-revert`。

- `-home-port`は、network interface revertコマンドをLIFに対して実行したときにLIFが戻る物理ポートまたは論理ポートです。
- オプションと `-netmask`オプションでIPアドレスを指定できます `-address`。
- IPアドレスを手動で（サブネットを使用せずに）割り当てるときに、クライアントまたはドメインコントローラが別のIPサブネットにある場合は、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内で静的ルートを作成する方法については、network route createのマニュアルページを参照してください。
- `-service-policy`- LIFのサービスポリシー。ポリシーを指定しない場合は、デフォルトポリシーが自動的に割り当てられます。コマンドを使用し `network interface service-policy show`て、使用可能なサービスポリシーを確認します。
- `-auto-revert`-起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定します。*デフォルト設定はfalse *ですが、環境内のネットワーク管理ポリシーに応じてtrueに設定できます。

  トランキンググループに追加するLIFごとに、この手順を繰り返します。

次のコマンドは、ノードcluster1_01のポートe0cにSVM vs1用のlif-aを作成します。

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

詳細はこちら"LIFの作成"

4. LIFが作成されたことを確認します。

```
network interface show
```

5. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

ONTAPボリュームのエクスポートポリシーを変更します。

クライアントが既存のデータ共有のトランキングを利用できるようにするには、エクスポートポリシーとルール、およびそれらが接続されているボリュームの変更が必要になる場合があります。LinuxクライアントとVMwareデータストアには、エクスポートに関するさまざまな要件があります。

クライアントのエクスポート要件：

- Linuxクライアントでは、トランキング接続ごと（つまりLIFごと）に、個別のマウントと個別のマウントポイントが必要です。

  ONTAP 9 14.1にアップグレードしていて、すでにボリュームをエクスポートしている場合は、そのボリュームをトランキンググループで引き続き使用できます。

- VMwareクライアントでは、複数のLIFを指定したエクスポートされたボリュームに対してマウントポイントが1つだけ必要です。

  VMwareクライアントには、エクスポートポリシーでルートアクセスが必要です。

手順

1. 既存のエクスポートポリシーが設定されていることを確認します。

```
vserver export-policy show
```

2. 既存のエクスポートポリシールールがトランキング構成に適していることを確認します。

```
vserver export-policy rule show -policyname policy_name
```

特に、エクスポートをマウントするトランキング対応のLinuxクライアントまたはVMwareクライアントがパラメータで正しく識別されていることを確認します `-clientmatch`。

調整が必要な場合は、コマンドを使用してルールを変更する `vserver export-policy rule modify`か、新しいルールを作成します。

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

詳細はこちら"エクスポートルールを作成しています。"

3. エクスポートした既存のボリュームがオンラインであることを確認します。

```
volume show -vserver svm_name
```

NFSトランキング用の**ONTAP**またはデータ共有の再マウント

トランキングされていないクライアント接続をトランキングされた接続に変換するには、LinuxクライアントおよびVMwareクライアントの既存のマウントを、LIFに関する情報を使用してアンマウントし、再マウントする必要があります。

クライアントでmountコマンドを入力する場合は、トランキンググループ内の各LIFのIPアドレスを入力する必要があります。

詳細はこちらをご覧ください "サポートされるクライアント"。

VMwareクライアントをアンマウントすると、データストア上のVMが停止します。別の方法として、トランキングを有効にした新しいデータストアを作成し、* Storage VMotion *を使用してVMを古いデータストアから新しいデータストアに移動します。詳細については、VMwareのドキュメントを参照してください。

Linuxクライアントの要件

トランキンググループ内の接続ごとに、個別のマウントポイントが必要です。

次のようなコマンドを使用して、エクスポートしたボリュームをマウントします。

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

`vers`値は以降である必要があり `4.1`ます。

この `max_connect`値は、トランキンググループ内の接続数に対応している必要があります。

VMwareクライアントの要件

トランキンググループ内の各接続のIPアドレスを含むMOUNTステートメントが必要です。

次のようなコマンドを使用して、エクスポートしたデータストアをマウントします。

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

`-H`値は、トランキンググループ内の接続に対応している必要があります。

RDMA経由のNFSを管理します。

NFS over RDMAの概要

NFS over RDMAはRDMAアダプタを使用するため、ストレージシステムメモリとホストシステムメモリの間でデータを直接コピーできるため、CPUの中断やオーバーヘッドを回避できます。

NFS over RDMA構成は、機械学習や分析など、レイテンシの影響を受けやすいワークロードや広帯域ワークロードを抱えているお客様向けに設計されています。NVIDIAでは、RDMA経由でNFSを拡張してGPUダイレクトストレージ（GDS）を実現しました。GDSは、CPUとメインメモリをすべてバイパスし、RDMAを使用してストレージシステムとGPUメモリの間でデータを直接転送することで、GPU対応のワークロードをさらに高速化します。

RDMA .10.1以降では、over RDMA構成がMellanox CX-5またはCX-6アダプタで使用されている場合にNFSv4.0プロトコルでサポートされます。このアダプタを使用すると、バージョン2のONTAP 9プロトコルを使用するRDMAがサポートされます。GDSは、Mellanox NICカードとMOFEDソフトウェアを搭載したNVIDIA TeslaおよびAmpereファミリのGPUでのみサポートされます。以降のONTAPリリースでサポートされるNFSバージョンについては、要件の表を参照してください。

NFSマウントサイズが64kを超えると、NFS over RDMA構成のパフォーマンスが不安定になります。

要件

- ストレージシステムでONTAP 9 10.1以降が実行されている必要があります。
- 使用するNFSのバージョンに対応した正しいバージョンのONTAPを実行していることを確認します。

NFSバージョン	**ONTAP**のサポート
NFSv4.0	ONTAP 9.10.1以降
NFSv4.1	ONTAP 9.14.1以降
NFSv3	ONTAP 9.15.1以降

  - ONTAP 9.12.1以降では、System Managerを使用してNFS over RDMAを設定できます。ONTAP 9.10.1および9.11.1では、CLIを使用してNFS over RDMAを設定する必要があります。

- HAペアの両方のノードでバージョンが同じである必要があります。
- ストレージ システム コントローラでRDMAがサポートされている必要があります。

ONTAPのバージョン	**RDMA**をサポートするコントローラ
9.10.1以降	• AFF A400 • AFF A700用 • AFF A800用
ONTAP 9.14.1以降	• AFF Cシリーズ • AFF A900用
ONTAP 9.15.1以降	• AFF A1K用 • AFF A90用 • AFF A70用
ONTAP 9.16.1以降	• AFF A50用 • AFF A30用 • AFF A20用

- データLIFは、RDMAをサポートするように設定する必要があります。
- クライアントでMellanox RDMA対応NICカードとMellanox OFED（MOFED）ネットワークソフトウェアを使用している必要があります。アダプタのサポートについては、を参照して"NetApp Hardware Universe"ください。NFS over RDMAでサポートされるアダプタの説明フィールドに「RoCE」と表示されます。

インターフェイスグループは、RDMA経由のNFSではサポートされません。

次のステップ

- NFS over RDMA用のNICの設定

- RDMA経由のNFS用のLIFの設定
- NFS over RDMAのNFS設定

関連情報

- "RDMA"
- NFSトランキングの概要
- "RFC 7530 ： NFS バージョン 4 プロトコル"
- "RFC 8166 ：リモート手順コールバージョン 1 用のリモートダイレクトメモリアクセストランスポート"
- "RFC 8167 ： RPC-over-RDMA トランスポート上の双方向リモート手順コール"
- "RFC 8267 ： RPC-over-RDMA バージョン 1 への NFS 上位レイヤバインディング"

NFS over RDMA用のNICの設定

RDMA経由のNFSでは、クライアントシステムとストレージプラットフォームの両方でNIC設定を行う必要があります。

ストレージプラットフォームの構成

X1148 RDMAアダプタがサーバにインストールされている必要があります。HA構成を使用している場合は、フェイルオーバー中もRDMAサービスを継続できるように、フェイルオーバーパートナーに対応するX1148アダプタが必要です。NICはROCEに対応している必要があります。

RDMA .10.1以降では、次のコマンドを使用してONTAP 9オフロードプロトコルのリストを表示できます。

```
network port show -rdma-protocols roce
```

クライアントシステム構成

クライアントでMellanox RDMA対応NICカード（X1148など）とMellanox OFEDネットワークソフトウェアを使用している必要があります。サポートされているモデルとバージョンについては、Mellanoxのドキュメントを参照してください。クライアントとサーバは直接接続できますが、スイッチのフェイルオーバーパフォーマンスが向上するため、スイッチの使用を推奨します。

クライアント、サーバ、スイッチ、およびスイッチ上のすべてのポートは、ジャンボフレームを使用して設定する必要があります。また、優先度フロー制御がすべてのスイッチで有効になっていることを確認します。

この構成を確認したら、NFSをマウントできます。

System Manager

Managerを使用してoverのネットワークインターフェイスを設定するには、ONTAP 9 12.1以降を使用している必要があります。

手順

1. RDMAがサポートされているかどうかを確認します。[Network]>[Ethernet Ports]に移動し、グループビューで適切なノードを選択します。ノードを展開するときに、特定のポートの* rdma protocols フィールドを確認します。 RoCE は**RDMA**がサポートされていることを示し、ダッシュ（-*）はサポートされていないことを示します。
2. VLANを追加するには、**+VLAN***を選択します。適切なノードを選択します。**[ポート]***ドロップダウンメニューで、使用可能なポートに「 RoCE Enabled *」というテキストが表示されます（RDMAがサポートされている場合）。RDMAがサポートされていない場合は、テキストは表示されません。
3. 新しいNFSサーバを設定するには、のワークフローに従いNFSを使用したLinuxサーバ用のNASストレージの有効化ます。

   ネットワークインターフェイスを追加する際には、「* RoCEポートを使用*」を選択できます。RDMA経由のNFSを使用するすべてのネットワークインターフェイスに対して、このオプションを選択します。

CLI

1. コマンドを使用して、NFSサーバでRDMAアクセスが有効になっているかどうかを確認します。

   ```
   vserver nfs show-vserver SVM_name
   ```

   デフォルトでは、 `-rdma`が有効になっている必要があります。有効になっていない場合は、NFSサーバでRDMAアクセスを有効にします。

   ```
   vserver nfs modify -vserver SVM_name -rdma enabled
   ```

2. RDMA経由でNFSv4.0を使用してクライアントをマウントします。
   a. protoパラメータの入力は、サーバのIPプロトコルのバージョンによって異なります。IPv4の場合は、を使用し `proto=rdma`ます。IPv6の場合は、を使用し `proto=rdma6`ます。
   b. 標準ポート2049ではなく、NFSターゲットポートをとして指定し `port=20049`ます。

      ```
      mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address
      :/volume_path mount_point
      ```

3. オプション：クライアントをアンマウントする必要がある場合は、次のコマンドを実行します。
   `unmount mount_path`

詳細情報

- NFSサーバを作成する
- NFSを使用したLinuxサーバ用のNASストレージの有効化

RDMA経由のNFS用のLIFの設定

RDMA経由のNFSを利用するには、LIF（ネットワークインターフェイス）をRDMAと互換性があるように設定する必要があります。LIFとそのフェイルオーバーペアの両方でRDMAがサポートされている必要があります。

新しいLIFを作成する

System Manager

Managerで経由の用のネットワークインターフェイスを作成するには、ONTAP 9 .12.1以降を実行している必要があります。

手順

1. Network > Overview > Network Interfaces *を選択します。
2. を選択します ＋ Add 。
3. NFS、SMB / CIFS、S3 を選択すると、[RoCEポートを使用]*オプションが表示されます。「RoCEポートを使用する」のチェックボックスをオンにします。
4. Storage VMとホームノードを選択します。名前、 IPアドレス、およびサブネットマスクを割り当てます。
5. IPアドレスとサブネットマスクを入力すると、System Managerはブロードキャストドメインのリストをを対応ポートを備えたドメインにフィルタリングします。ブロードキャストドメインを選択してください。必要に応じてゲートウェイを追加できます。
6. [保存（ Save ）] を選択します。

CLI

手順

1. LIFを作成します。

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - サービスポリシーは、default-data-files、またはdata-NFSネットワークインターフェイスサービスを含むカスタムポリシーのいずれかである必要があります。
   - `-rdma-protocols`パラメータにはリストを指定できます。このリストはデフォルトでは空です。`roce`を値として追加すると、LIFはRoCEオフロードをサポートしているポートにのみ設定でき、Bot LIFの移行とフェイルオーバーに影響します。

LIFを変更する

System Manager

Managerで経由の用のネットワークインターフェイスを作成するには、ONTAP 9 .12.1以降を実行している必要があります。

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*>[編集]*を選択します ⋮ 。
3. RoCEポートを使用する*をオンにしてNFS over RDMAを有効にするか、オフにして無効にしてください。ネットワークインターフェイスがRoCE対応ポート上にある場合は、「RoCEポートを使用する」の横にチェックボックスが表示されます。
4. 必要に応じて他の設定を変更します。
5. 「* Save *（保存）」を選択して、変更を確定します。

CLI

1. LIFのステータスは、コマンドを使用して確認できます `network interface show`。サービスポリシーにはdata-NFSネットワークインターフェイスサービスを含める必要があります。 `-rdma -protocols`リストにはを含める必要があります `roce`。上記のいずれかの条件が満たされていない場合は、LIFを変更します。
2. LIFを変更するには、次のコマンドを実行します。

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

特定のオフロードプロトコルを必要とするようにLIFを変更するときに、そのプロトコルをサポートするポートにLIFが現在割り当てられていないとエラーが発生します。

LIFを移行する

ONTAPでは、RDMA経由のNFSを利用するためにネットワークインターフェイス（LIF）を移行することもできます。この移行を実行する場合は、デスティネーションポートがRoCEに対応していることを確認する必要があります。ONTAP 9 12.1以降では、この手順をSystem Managerで実行できます。System Managerは、ネットワークインターフェイスのデスティネーションポートを選択する際に、RoCEに対応しているかどうかを指定します。

LIFをRDMA経由のNFS構成に移行できるのは、次の場合のみです。

- RoCE対応ポートでホストされるNFS RDMAネットワークインターフェイス（LIF）です。
- RoCE対応ポートでホストされるNFS TCPネットワークインターフェイス（LIF）です。
- RoCE非対応のポートでホストされるNFS TCPネットワークインターフェイス（LIF）です。

ネットワークインターフェイスの移行の詳細については、を参照してくださいLIFを移行する。

詳細情報

- LIFの作成
- LIFの作成
- LIFを変更する
- LIFを移行する

NFS設定を変更する

ほとんどの場合、RDMA経由のNFS用のNFS対応Storage VMの設定を変更する必要はありません。

ただし、MellanoxチップとLIFの移行に関連する問題に対処している場合は、NFSv4ロック猶予期間を延長する必要があります。デフォルトでは、猶予期間は45秒に設定されています。ONTAP 9 .10.1以降では、猶予期間の最大値は180（秒）です。

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 SVM_name -v4-grace-seconds number_of_seconds
   ```

このタスクの詳細については、を参照してくださいNFSv4ロック猶予期間の指定。

CLIを使用したSMBの設定

CLIヲシヨウシタSMBセツテイノカイヨウ

ONTAP 9 CLIコマンドを使用して、新規または既存のSVMの新しいボリュームまたはqtreeに格納されているファイルへのSMBクライアントアクセスを設定できます。

SMB(Server Message Block) は、 Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（ CLI ）および OnCommand 管理ツールでは、 _cifs_という メッセージが引き続き表示されます。

次の手順は、ボリュームまたはqtreeへのSMBアクセスを設定する場合に使用します。想定している状況は次のとおりです。

- SMBバージョン2以降を使用する。
- NFSクライアントではなく、SMBクライアントのみを処理する（マルチプロトコル構成ではない）。
- 新しいボリュームはNTFSファイル権限を使用して保護されます。
- SVM管理者Privilegesではなく、クラスタ管理者Privilegesが必要です。

  SVM と LIF を作成するにはクラスタ管理者権限が必要です。他の SMB 設定タスクには、 SVM 管理者権限で十分です。

- System Managerや自動スクリプトツールではなく、CLIを使用する必要がある。

  System Managerを使用してNASマルチプロトコルアクセスを設定する方法については、を参照してください"NFSとSMBの両方を使用したWindowsとLinux用のNASストレージのプロビジョニング"。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

  コマンド構文の詳細については、CLIヘルプおよびONTAPのマニュアルページを参照してください。

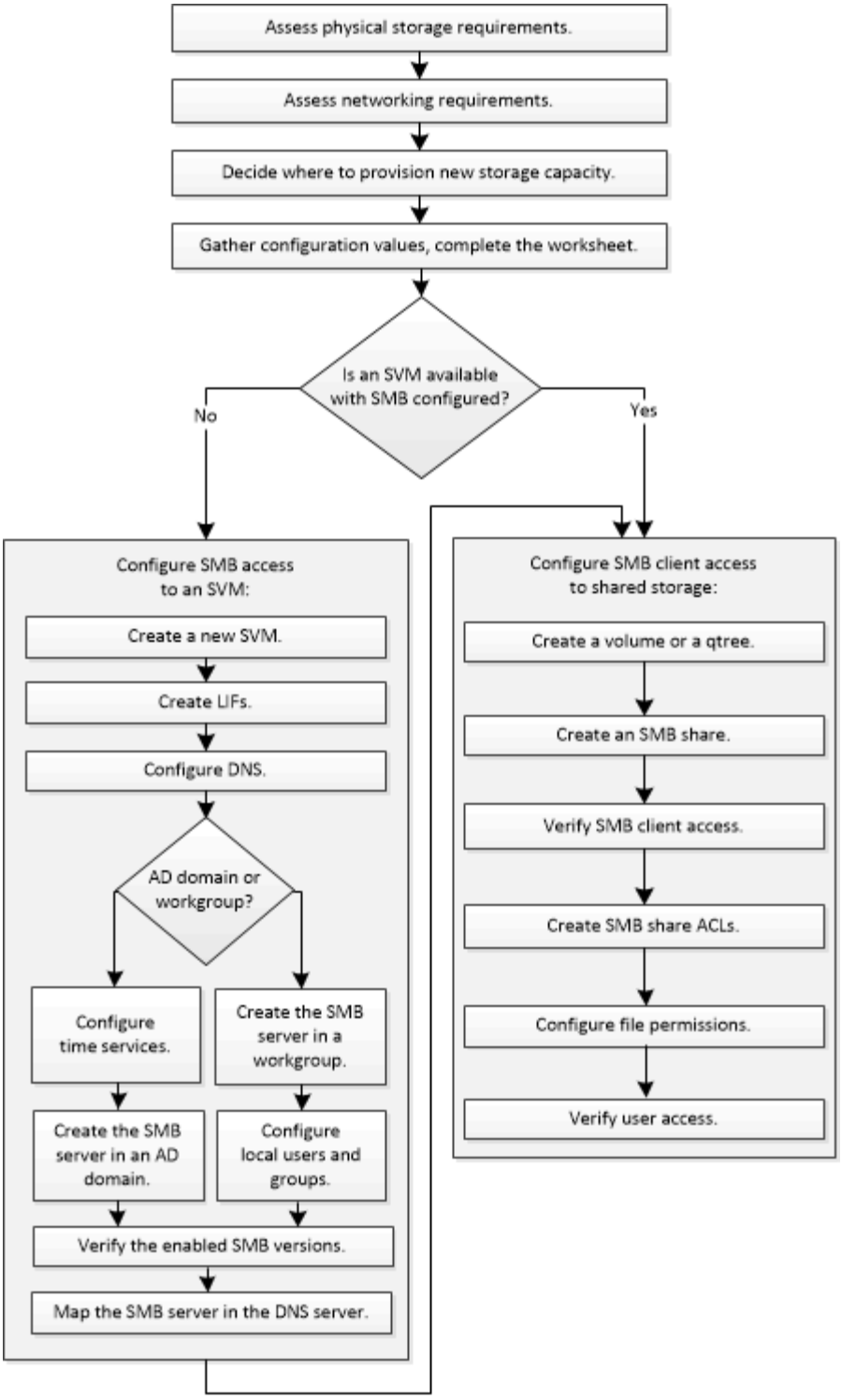
ONTAP SMBプロトコル機能の範囲の詳細については、を参照して"SMBリファレンスノガイヨウ"ください。

ONTAPで実行するその他の方法

実行するタスク	参照先
再設計されたSystem Manager（ONTAP 9 .7以降で使用可能）	"SMBを使用したWindowsサーバ用のNASストレージのプロビジョニング"
System Manager Classic（ONTAP 9 .7以前で使用可能）	"SMBセツテイノカイヨウ"

SMBの設定ワークフロー

SMBを設定するには、物理ストレージとネットワークの要件を評価し、目的に応じたワークフローを選択します。新規または既存のSVMへのSMBアクセスを設定するか、すでにSMBアクセスの設定が完了している既存のSVMにボリュームまたはqtreeを追加します。



準備

物理ストレージ要件の評価

クライアント用のSMBストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリューム用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。 `storage aggregate show`

   十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 十分なスペースを備えたアグリゲートがない場合は、コマンドを使用して既存のアグリゲートにディスクを追加する `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成し `storage aggregate create`ます。

ネットワーク要件の評価

クライアントにSMBストレージを提供する前に、SMBプロビジョニングの要件を満たすようにネットワークが正しく設定されていることを確認する必要があります。

開始する前に

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）
- 外部ファイアウォール

手順

1. 使用可能な物理ポートと仮想ポートを表示します。 `network port show`

- 可能な場合は、データネットワークの速度が最も速いポートを使用してください。
- 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。

2. サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、サブネットが存在し、十分な数のアドレスが使用可能であることを確認します。 `network subnet show`

   サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。

3. 使用可能なIPspaceを表示します。 `network ipspace show`

   デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

4. IPv6アドレスを使用する場合は、IPv6がクラスタで有効になっていることを確認します。 `network options ipv6 show`

   必要に応じて、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

新しい**SMB**ストレージ容量のプロビジョニング先を決定する

新しい SMB ボリュームまたは qtree を作成する前に、その配置先を新規、既存のどちらの SVM にするかを決め、 SVM にどのような設定が必要になるかを確認しておく必要があります。この決定によって、ワークフローが決まります。

選択肢

- 新しい SVM 、または SMB が有効になっているものの設定されていない既存の SVM 上でボリュームまたは qtree をプロビジョニングする場合は、「 SVM への SMB アクセスの設定」と「 SMB 対応 SVM へのストレージ容量の追加」の両方の手順を実行します。

  SVMへのSMBアクセスの設定

  共有ストレージへの SMB クライアントアクセスの設定

  次のいずれかに該当する場合は、新しいSVMを作成します。

  - クラスタでSMBを初めて有効にする場合。
  - クラスタ内の既存のSVMでSMBサポートを有効にするのが望ましくない場合。
  - クラスタ内に SMB 対応 SVM が 1 つ以上あり、次のいずれかの接続が必要な場合。
    - ワークグループ内の別の Active Directory フォレストへの接続。
    - 分離されたネームスペース内の SMB サーバへの接続（マルチテナンシーシナリオ）。SMBが有効になっているが設定はまだ完了していない既存のSVMでストレージをプロビジョニングする場合も、このオプションを選択する必要があります。これは、SANアクセス用のSVMを作成した場合や、SVM作成時にプロトコルが有効になっていなかった場合に該当します。

  SVMでSMBを有効にしたあとに、ボリュームまたはqtreeのプロビジョニングに進みます。

- SMB アクセスの設定が完了している既存の SVM でボリュームまたは qtree をプロビジョニングする場合は、「 SMB 対応 SVM へのストレージ容量の追加」の手順を実行します。

共有ストレージへの SMB クライアントアクセスの設定

SMB設定情報を収集するためのワークシート

SMB設定ワークシートを使用すると、クライアントのSMBアクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所に関する決定に応じて、ワークシートのいずれかまたは両方のセクションを完了する必要があります。

- SVMへのSMBアクセスを設定する場合は、両方のセクションを完了する必要があります。

  SVMへのSMBアクセスの設定

  共有ストレージへの SMB クライアントアクセスの設定

- SMB対応SVMにストレージ容量を追加する場合は、2番目のセクションのみを完了する必要があります。

  共有ストレージへの SMB クライアントアクセスの設定

パラメータの詳細については、コマンドのマニュアルページを参照してください。

SVMへの**SMB**アクセスの設定

- SVM を作成するためのパラメータ *

新しいSVMを作成する場合は、コマンドで次の値を指定します `vserver create`。

フィールド	説明	あなたの価値
`-vserver`	新しいSVMの名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意のSVM名を適用する別の命名規則に従います。	
`-aggregate`	新しいSMBストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-rootvolume`	SVMルート ボリュームの一意の名前を指定します。	
`-rootvolume-security-style`	SVMのNTFSセキュリティ形式を使用します。	`ntfs`
`-language`	このワークフローではデフォルトの言語設定を使用します。	`C.UTF-8`

フィールド	説明	あなたの価値
ipspace	オプション： IPspace は、 SVM が配置される個別の IP アドレススペースです。	

* LIF 作成用のパラメータ *

LIFを作成する場合は、コマンドで次の値を指定します `network interface create`。

フィールド	説明	あなたの価値
-lif	新しいLIFの名前を指定します。	
-role	このワークフローではデータLIFのロールを使用します。	data
-data-protocol	このワークフローではSMBプロトコルのみを使用します。	cifs
-home-node	LIFに対してコマンドを実行したときにLIFが戻るノード `network interface revert`。	
-home-port	LIFに対してコマンドを実行したときにLIFが戻るポートまたはインターフェイスグループ `network interface revert`。	
-address	新しいLIFによるデータアクセスに使用する、クラスタ上のIPv4アドレスまたはIPv6アドレスを指定します。	
-netmask	LIFのネットワークマスクとゲートウェイ。	
-subnet	IPアドレスのプール。および `-netmask`の代わりに使用して `-address`、アドレスとネットマスクを自動的に割り当てます。	
-firewall-policy	このワークフローではデフォルトのデータファイアウォールポリシーを使用します。	data

フィールド	説明	あなたの価値
-auto-revert	オプション：起動時またはその他の状況下でデータ LIF がホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はです false。	

- DNS ホスト名解決のパラメータ *

DNSを設定する場合は、コマンドで次の値を指定します vserver services name-service dns create。

フィールド	説明	あなたの価値
-domains	最大5つのDNSドメイン名。	
-name-servers	DNSネームサーバごとに最大3つのIPアドレス。	

Active Directoryドメインでの**SMB**サーバのセットアップ

- タイムサービス設定のパラメータ *

タイムサービスを設定する場合は、コマンドで次の値を指定します cluster time-service ntp server create。

フィールド	説明	あなたの価値
-server	Active Directory ドメイン用の NTP サーバのホスト名または IP アドレスを指定します。	

- Active Directory ドメイン内に SMB サーバを作成するためのパラメータ *

新しいSMBサーバを作成し、ドメイン情報を指定する場合は、コマンドで次の値を指定します vserver cifs create。

フィールド	説明	あなたの価値
-vserver	SMB サーバを作成する SVM の名前を指定します。	
-cifs-server	SMB サーバの名前（最大 15 文字）を指定します。	

フィールド	説明	あなたの価値
`-domain`	SMB サーバに関連付ける Active Directory ドメインの完全修飾ドメイン名（ FQDN ）を指定します。	
`-ou`	オプション： SMB サーバに関連付ける Active Directory ドメイン内の組織単位を指定します。デフォルトでは、このパラメータはCN=Computersに設定されています。	
`-netbios-aliases`	オプション： NetBIOS エイリアスのリストを指定します。 NetBIOS エイリアスは、 SMB サーバ名の別名です。	
`-comment`	オプション：サーバのテキストコメントを指定します。Windowsクライアントは、ネットワーク上のサーバを参照するときに、SMBサーバの説明を確認できます。	

ワークグループでの**SMB**サーバのセットアップ

- ワークグループで SMB サーバーを作成するためのパラメータ *

新しいSMBサーバを作成し、サポートされるSMBバージョンを指定する場合は、コマンドで次の値を指定します `vserver cifs create`。

フィールド	説明	あなたの価値
`-vserver`	SMB サーバを作成する SVM の名前を指定します。	
`-cifs-server`	SMB サーバの名前（最大 15 文字）を指定します。	
`-workgroup`	ワークグループの名前（最大 15 文字）を指定します。	
`-comment`	オプション：サーバのテキストコメントを指定します。Windowsクライアントは、ネットワーク上のサーバを参照するときに、SMBサーバの説明を確認できます。	

- ローカルユーザー作成用のパラメータ *

コマンドを使用してローカルユーザを作成する場合は、次の値を指定し `vserver cifs users-and-groups local-user create`ます。これらの値は、ワークグループ内、およびオプションで AD ドメイン内の SMB サーバに必要です。

フィールド	説明	あなたの価値
`-vserver`	ローカルユーザを作成する SVM の名前を指定します。	
`-user-name`	ローカルユーザの名前（最大 20 文字）を指定します。	
`-full-name`	オプション：ユーザのフルネームを指定します。フルネームにスペースが含まれている場合は、フルネームを二重引用符で囲みます。	
`-description`	オプション：ローカルユーザの概要。説明にスペースが含まれている場合は、パラメータを引用符で囲みます。	
`-is-account-disabled`	オプション：ユーザアカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。	

- ローカルグループを作成するためのパラメータ *

コマンドを使用してローカルグループを作成する場合は、次の値を指定し `vserver cifs users-and-groups local-group create`ます。AD ドメインおよびワークグループ内の SMB サーバの場合はオプションです。

フィールド	説明	あなたの価値
`-vserver`	ローカルグループを作成する SVM の名前を指定します。	
`-group-name`	ローカルグループの名前（最大 256 文字）を指定します。	
`-description`	オプション：ローカルグループの概要。説明にスペースが含まれている場合は、パラメータを引用符で囲みます。	

SMB対応**SVM**へのストレージ容量の追加

- ボリュームを作成するためのパラメータ *

qtreeではなくボリュームを作成する場合は、コマンドで次の値を指定します `volume create`。

フィールド	説明	あなたの価値
`-vserver`	新しいボリュームをホストする新規または既存のSVMの名前を指定します。	
`-volume`	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
`-aggregate`	新しいSMBボリューム用の十分なスペースがあるクラスタ内のアグリゲートの名前を指定します。	
`-size`	新しいボリュームのサイズとして任意の整数を指定します。	
`-security-style`	このワークフローにはNTFSセキュリティ形式を使用します。	`ntfs`
`-junction-path`	新しいボリュームのマウント先とする、ルート（/）の下の場所を指定します。	

- qtree を作成するためのパラメータ *

ボリュームではなくqtreeを作成する場合は、コマンドで次の値を指定します `volume qtree create`。

フィールド	説明	あなたの価値
`-vserver`	qtreeを含むボリュームが配置されているSVMの名前。	
`-volume`	新しいqtreeを格納するボリュームの名前。	
`-qtree`	新しいqtreeには、64文字以下の一意のわかりやすい名前を指定します。	
`-qtree-path`	ボリュームとqtreeを別 々 の引数として指定する代わりに、qtreeパスをの形式で `/vol/volume_name/qtree_name\>` 指定できます。	

- SMB 共有作成のパラメータ *

コマンドでは、次の値を指定します `vserver cifs share create`。

フィールド	説明	あなたの価値
`-vserver`	SMB 共有を作成する SVM の名前を指定します。	
`-share-name`	作成する SMB 共有の名前（最大 256 文字）を指定します。	
`-path`	SMB 共有へのパスの名前（最大 256 文字）を指定します。このパスは、共有を作成する前にボリューム内に存在している必要があります。	
`-share-properties`	オプション：共有プロパティのリストを指定します。デフォルト設定は `oplocks`、、 `browsable changenotify`、および `show-previous-versions`です。	
`-comment`	オプション：サーバのテキストコメント（最大 256 文字）を指定します。Windows クライアントは、ネットワーク上で参照するとき、この SMB 共有概要を確認できます。	

- SMB 共有アクセス制御リスト（ ACL ）を作成するためのパラメータ *

コマンドでは、次の値を指定します `vserver cifs share access-control create`。

フィールド	説明	あなたの価値
`-vserver`	SMB ACL を作成する SVM の名前を指定します。	
`-share`	作成先の SMB 共有の名前を指定します。	
`-user-group-type`	共有の ACL に追加するユーザまたはグループのタイプを指定します。デフォルトのタイプはです。 `windows`	`windows`

フィールド	説明	あなたの価値
`-user-or-group`	共有の ACL に追加するユーザまたはグループを指定します。ユーザ名を指定する場合は、「ドメイン名」の形式でユーザのドメインを含める必要があります。	
`-permission`	ユーザまたはグループの権限を指定します。	`[No_access
Read	Change	Full_Control]`

SVMへのSMBアクセスの設定

SVMへのSMBアクセスの設定

SMB クライアントアクセス用に SVM を設定していない場合は、新しい SVM を作成して設定するか、既存の SVM を設定する必要があります。SMB を設定する場合は、 SVM ルートボリュームへのアクセスを許可し、 SMB サーバを作成し、 LIF を作成し、ホスト名解決を有効にし、ネームサービスを設定し、必要に応じて Kerberos セキュリティの有効化。

SVMの作成

SMBクライアントにデータアクセスを提供するSVMがクラスタ内に1つもない場合は、SVMを作成する必要があります。

開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

手順

1. SVMを作成します。 `vserver create -vserver *svm_name* -rootvolume *root_volume_name* -aggregate *aggregate_name* -rootvolume-security-style ntfs -language C.UTF-8 -ipspace *ipspace_name*`
   - オプションにはNTFS設定を使用し `-rootvolume-security-style`ます。
   - デフォルトのC.UTF-8オプションを使用し `-language`ます。
   - この `ipspace`設定はオプションです。
2. 新しく作成したSVMの設定とステータスを確認します。 `vserver show -vserver *vserver_name*`

   `Allowed Protocols`フィールドに CIFSを含める必要があります。このリストは後で編集できます。

`Vserver Operational State`フィールドには状態が表示されている必要があり`running`ます。状態が表示された場合は`initializing`、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

例

次のコマンドは、データアクセス用のSVMをIPspace内に作成し`ipspaceA`ます。

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて状態になっていることを示しています running。ルートボリュームには、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あるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                       Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                         Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                      Disallowed Protocols: -
                          QoS Policy Group: -
                               Config Lock: false
                              IPspace Name: ipspaceA
```

ONTAP 9 .13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

SVMで**SMB**プロトコルが有効になっていることを確認する

SVMでSMBを設定して使用する前に、プロトコルが有効になっていることを確認する必要があります。

タスクの内容

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、セットアップ時にプロトコルを有効にしなかった場合でも、コマンドを使用してあとから有効にすることができます `vserver add-protocols`。

作成したプロトコルは、 LIF から追加または削除することはできません。

コマンドを使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols`。

手順

1. SVMに対して現在有効または無効になっているプロトコルを確認します。 `vserver show -vserver vserver_name -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 `vserver show-protocols`。

2. 必要に応じて、プロトコルを有効または無効にします。
   - SMBプロトコルを有効にする手順は次のとおりです。 `vserver add-protocols -vserver vserver_name -protocols cifs`
   - プロトコルを無効にするには： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. 有効なプロトコルと無効な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 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, 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を追加することで、SMB経由のアクセスを許可し `cifs`ます。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

SVMルートボリュームのエクスポートポリシーを開く

SVM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には、すべてのクライアントにSMB経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVMとそのボリュームに対するSMBクライアントのアクセスがすべて拒否されます。

タスクの内容

新しいSVMが作成されると、デフォルトのエクスポートポリシー（default）がSVMのルートボリュームに対し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。

デフォルトのエクスポートポリシーですべてのSMBアクセスが開いていることを確認してから、個 々 のボリュームまたはqtreeにカスタムのエクスポートポリシーを作成して個 々 のボリュームへのアクセスを制限します。

手順

1. 既存のSVMを使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。
`vserver export-policy rule show`

   次のようなコマンド出力が表示されます。

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 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: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

   オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVMルートボリュームのエクスポートルールを作成します。 `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. コマンドを使用してルールの作成を確認します `vserver export-policy rule show`。

結果

これで、SVMで作成されたすべてのボリュームまたはqtreeに、すべてのSMBクライアントからアクセスできるようになります。

LIFの作成

LIFは、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

開始する前に

- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

- LIFで処理されるトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9 .5以前では、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。
- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、同じサブネットにすでに設定されている他のLIFと同じブロードキャストドメイン内の指定したホームノード上の任意のポートを自動的に選択します。

手順

1. LIFを作成します。

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

* ONTAP 9.5 以前 *
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

* ONTAP 9.6 以降 *
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - `-role`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。
   - `-data-protocol`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。ONTAP 9 .5以前を使用している場合は `-data-protocol`、LIFの作成時にパラメータを指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。
   - `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

     オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

- `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
- オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
- サブネットを使用してIPアドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときに、ゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
- IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。 `network route create`のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- オプションには `-firewall-policy`、LIFのロールと同じデフォルトを使用し `data`ます。

  必要に応じて、あとからカスタムファイアウォールポリシーを作成して追加できます。

  > ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false`。

2. LIFが正常に作成されたことを確認します。

   ```
   network interface show
   ```

3. 設定したIPアドレスに到達できることを確認します。

対象	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドは、LIFを作成し、パラメータと `-netmask`パラメータを使用してIPアドレスとネットワークマスク値を指定し `-address`ます。

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワークマスク値を指定したサブネット（client1_sub）から割り当てます。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

次のコマンドは、サービスポリシーが割り当てられたNASデータLIFを作成する方法を示してい `default-data-files`ます。

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

ホスト名解決のための**DNS**の有効化

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。

開始する前に

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。 `vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。

タスクの内容

SVM での動的 DNS の設定については、『ネットワーク管理ガイド』を参照してください。

手順

1. SVMでDNSを有効にします。 `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   ONTAP 9 .2以降では `vserver services name-service dns create`、コマンドによって設定の自動検証が実行され、ONTAPがネームサーバに接続できない場合はエラーメッセージが報告されます。

2. コマンドを使用して、DNSドメイン設定を表示します `vserver services name-service dns show`。 ``

   次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

```
vserver services name-service dns show
                                                 Name
Vserver           State     Domains              Servers
----------------- --------- -------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. コマンドを使用して、ネームサーバのステータスを検証し `vserver services name-service dns check`ます。

   この `vserver services name-service dns check`コマンドは、ONTAP 9 .2以降で使用できます。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Active Directoryドメインでの**SMB**サーバのセットアップ

タイムサービスの設定

アクティブドメインコントローラでSMBサーバを作成する前に、クラスタ時間とSMBサーバが属するドメインのドメインコントローラの時間のずれが5分以内であることを確認する必要があります。

タスクの内容

Active Directoryドメインと同じNTPサーバを時刻の同期に使用するようにクラスタNTPサービスを設定する必要があります。

手順

1. コマンドを使用してタイムサービスを設定します `cluster time-service ntp server create`。
   - 対称認証を使用せずにタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address`
   - 対称認証を使用してタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. コマンドを使用して、タイムサービスが正しく設定されていることを確認します `cluster time-service ntp server show`。

   `cluster time-service ntp server show`

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

NTPサーバの対称認証の管理用コマンド

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

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

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

Active Directoryドメインに**SMB**サーバを作成する

コマンドを使用すると、SVM上にSMBサーバを作成し、所属先のActive Directory（AD）ドメインを指定できます `vserver cifs create`。

開始する前に

データ処理に使用するSVMおよびLIFが、SMBプロトコルを許可するように設定されている必要があります。LIFは、SVM上で設定されているDNSサーバ、およびSMBサーバの追加先ドメインのADドメインコントローラに接続できる必要があります。

SMBサーバの追加先のADドメイン内のマシンアカウントの作成を許可されているすべてのユーザが、SVM上にSMBサーバを作成できます。これには、他のドメインのユーザを含めることができます。

ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

タスクの内容

Activity DirectoryドメインにSMBサーバを作成する場合は、次の点に注意してください。

- ドメインを指定するときは、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用する必要があります。
- デフォルト設定では、SMBサーバマシンアカウントはActive Directory CN=Computerオブジェクトに追加されます。
- オプションを使用すると、SMBサーバを別の組織単位（OU）に追加できます `-ou`。
- 必要に応じて、SMBサーバの1つ以上のNetBIOSエイリアス（最大200）をカンマで区切って追加できます。

  SMBサーバのNetBIOSエイリアスを設定すると、他のファイルサーバのデータをSMBサーバに統合し、SMBサーバが元のサーバの名前に応答するようにする場合に役立ちます。

その他のオプションのパラメータと命名要件については、のマニュアルページを参照して `vserver cifs`ください。

> SMB.1以降では、ONTAP 9バージョン2.0からドメインコントローラ（DC）への接続を有効にすることができます。この処理は、ドメインコントローラでSMB 1.0を無効にしている場合に必要です。SMB.2以降では、ONTAP 9 2.0がデフォルトで有効になります。

ONTAP 9 .8以降では、ドメインコントローラへの接続を暗号化するように指定できます。ONTAPオプションがに設定され `true`ている場合、ドメインコントローラの通信に暗号化が必要です `-encryption-required-for-dc-connection`。デフォルトはです。`false`暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されます。です。

"SMBの管理"SMBサーバ設定オプションの詳細については、を参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMBサーバを認証のみに使用する場合は、CIFSライセンスは必要ありません。

2. ADドメインにSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

   次のコマンドは、ドメイン「 example.com`": 」に SMB サーバ「 'smb_server01' 」を作成します

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   次のコマンドは、ドメイン「 m ydomain.com`" 」に SMB サーバ「 'smb_server02' 」を作成し、 keytab ファイルを使用して ONTAP 管理者を認証します。

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

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

   この例では、「 `s MB_SERVER01' 」という名前の SMB サーバが SVM vs1.example.com 上に作成され、「 example.com`" ドメイン」に追加されたことがコマンド出力に示されています。

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

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. 必要に応じて、ドメインコントローラ（ONTAP 9 .8以降）との暗号化通信を有効にします。 `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

例

次のコマンドは、 SVM vs2.example.com の「 example.com`" 」ドメインに「 'MB_Server02' 」という名前の SMB サーバを作成します。マシン・アカウントは '`OU=eng 、 OU=corp 、 DC=example 、 DC=com コンテナに作成されますSMBサーバにはNetBIOSエイリアスが割り当てられます。

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                      CIFS Server NetBIOS Name: SMB_SERVER02
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
              CIFS Server Administrative Status: up
                        CIFS Server Description: -
                        List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

次のコマンドは、別のドメインのユーザ（ここでは信頼できるドメインの管理者）が、 SVM vs3.example.com 上に「 smb_server03 」という名前の SMB サーバを作成できるようにします。オプションは `-domain`、SMBサーバを作成するホームドメイン（DNSの設定で指定）の名前を指定します。オプションは `username`、信頼できるドメインの管理者を指定します。

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

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

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

SMB認証用のkeytabファイルの作成

ONTAP 9.7 以降 ONTAP では、 keytab ファイルを使用した Active Directory （ AD ）サーバとの SVM 認証がサポートされます。AD管理者はkeytabファイルを生成し、Uniform Resource Identifier（URI）としてONTAP管理者が使用できるようにします。このURIは、コマンドでADドメインとのKerberos認証が必要な場合に指定します `vserver cifs`。

AD管理者は、Windows Serverの標準コマンドを使用してkeytabファイルを作成できます `ktpass`。このコマンドは、認証が必要なプライマリドメインで実行する必要があります。 `ktpass`コマンドを使用してkeytabファイルを生成できるのはプライマリドメインユーザのみです。信頼できるドメインユーザを使用して生成されたキーはサポートされません。

keytab ファイルは、特定の ONTAP 管理者ユーザ用に生成されます。管理者ユーザのパスワードが変更されないかぎり、特定の暗号化タイプとドメインに対して生成されたキーは変更されません。そのため、管理者ユーザのパスワードを変更するたびに、新しいkeytabファイルが必要になります。

次の暗号化タイプがサポートされています。

- AES256-SHA1
- DES-CBC-MD5

  ONTAP では、 DES-CBC-CRC 暗号化タイプはサポートされていません。

- RC4-HMAC

最も高度な暗号化タイプは AES256 です。 ONTAP システムで有効な場合は AES256 を使用してください。

keytab ファイルは、管理パスワードを指定して生成するか、ランダムに生成されたパスワードを使用して生成できます。ただし、 keytab ファイル内のキーを復号化するために AD サーバ側で管理者ユーザに固有な秘密鍵が必要になるため、ある時点で使用できるパスワードオプションはどちらか 1 つだけです。特定の管理者の秘密鍵を変更すると、 keytab ファイルは無効になります。

ワークグループでのSMBサーバのセットアップ

ワークグループでのSMBサーバのセットアップの概要

ワークグループ内のメンバーとして SMB サーバをセットアップするには、 SMB サーバを作成してから、ローカルユーザとローカルグループを作成します。

Microsoft Active Directory ドメインインフラを使用できない場合は、ワークグループに SMB サーバを設定できます。

ワークグループモードの SMB サーバでは NTLM 認証のみがサポートされ、 Kerberos 認証はサポートされません。

ワークグループに**SMB**サーバを作成する

コマンドを使用すると、SVM上にSMBサーバを作成し、所属先のワークグループを指定できます `vserver cifs create`。

開始する前に

データ処理に使用するSVMおよびLIFが、SMBプロトコルを許可するように設定されている必要があります。LIFは、SVMで設定されているDNSサーバに接続できる必要があります。

タスクの内容

ワークグループモードのSMBサーバでは、SMBの次の機能はサポートされません。

- SMB3カンシフロトコル
- SMB3 CA共有
- SQL over SMB
- フォルダ リダイレクト
- 移動プロファイル
- グループ ポリシー オブジェクト（GPO）
- ボリュームSnapshotサービス（VSS）

その他のオプションの設定パラメータと命名要件については、のマニュアルページを参照して `vserver cifs`ください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMBサーバを認証のみに使用する場合は、CIFSライセンスは必要ありません。

2. ワークグループ内にSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   次のコマンドは ' ワークグループ "workgroup01" 内に SMB サーバ "'smb_server01" を作成します

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

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

   次の例では、コマンド出力は、ワークグループ「 workgroup01 」内の SVM vs1.example.com 上に「

'smb_server01' 」という名前の SMB サーバが作成されたことを示しています。

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                  Workgroup Name: workgroup01
                             Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

終了後

ワークグループ内のCIFSサーバの場合は、SVM上にローカルユーザ、および必要に応じてローカルグループを作成する必要があります。

関連情報

"SMBの管理"

ローカルユーザアカウントの作成

SVMに格納されたデータへのSMB接続を介したアクセスの認証に使用できるローカルユーザアカウントを作成できます。SMBセッションの作成時の認証にローカルユーザアカウントを使用することもできます。

タスクの内容

ローカルユーザの機能は、SVMの作成時にデフォルトで有効になります。

ローカルユーザアカウントを作成するときは、ユーザ名を指定する必要があり、アカウントを関連付けるSVMを指定する必要があります。

`vserver cifs users-and-groups local-user`マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

手順

1. ローカルユーザを作成します。 `vserver cifs users-and-groups local-user create -vserver` *vserver_name* `-user-name` *user_name optional_parameters*

   次のオプションのパラメータが役に立つ場合があります。

   - `-full-name`

ユーザのフルネーム。

- `-description`

  ローカルユーザの説明。

- `-is-account-disabled {true|false}`

  ユーザアカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。

ローカルユーザのパスワードの入力を求められます。

2. ローカルユーザのパスワードを入力し、確認のためにもう一度入力します。
3. ユーザが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`

例

次の例では、 SVM vs1.example.com に関連付けられた「 `S MB_SERVER1\Sue` 」という完全な名前のローカルユーザ「 `S ue Chang-」 を作成します。

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

ローカルグループの作成

SVM に関連付けられたデータへの SMB 接続によるアクセスの許可に使用できるローカルグループを作成できます。また、グループのメンバーに付与するユーザ権限と機能を定義した権限を割り当てることもできます。

タスクの内容

ローカルグループの機能は、 SVM の作成時にデフォルトで有効になります。

ローカルグループを作成するときは、グループの名前を指定する必要があり、グループを関連付ける SVM を指定する必要があります。グループ名を指定する際、ローカルドメイン名は指定してもしなくても構いません。また、オプションで、ローカルグループの概要を指定することもできます。別のローカルグループにローカルグループを追加することはできません。

`vserver cifs users-and-groups local-group`マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

手順

1. ローカルグループを作成します。 `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   次のオプションのパラメータが役に立つ場合があります。

   - `-description`

     ローカルグループの説明。

2. グループが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-group show -vserver vserver_name`

例

次の例では、 SVM vs1 に関連付けられるローカルグループ「 `s MB_SERVER01\engineering` 」を作成します。

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ----------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

終了後

新しいグループにメンバーを追加する必要があります。

ローカルグループメンバーシップを管理します。

ローカルグループメンバーシップの管理では、ローカルユーザまたはドメインユーザの追加と削除、またはドメイングループの追加と削除を行うことができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

タスクの内容

特定のグループのメンバーシップに基づいてローカルユーザ、ドメインユーザ、またはドメイングループに付与されたアクセス権や権限を取り消す場合に、メンバーをグループから削除できます。

メンバーをローカルグループに追加する場合は、次の点に注意する必要があります。

- 特殊なグループ _Everyone にユーザーを追加することはできません。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、 ONTAP で名前を SID に解決できる必要があります。

メンバーをローカルグループから削除する場合は、次の点に注意する必要があります。

- 特殊なグループ _Everyone からメンバーを削除することはできません。
- ローカルグループからメンバーを削除するには、 ONTAP で名前を SID に解決できる必要があります。

手順

1. メンバーをグループに追加するか、グループから削除します。
   - メンバーを追加します。 `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループに追加できます。
   - メンバーを削除します。 `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループから削除することができます。

例

次の例では、 SVM vs1.example.com 上のローカルグループ「 `s MB_SERVER01\engineering` 」にローカルユーザ「 ````s MB_SERVER01\engineering 」を追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

次の例では、 SVM vs1.example.com 上のローカルグループ「 `s MB_SERVER1\engineering` 」からローカルユーザ「 `s MB_SERVER01\Sue` 」および「 `S MB_SERVER01\engineering` 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

クライアントおよびドメインコントローラとの接続に対してデフォルトで有効になっているSMBのバージョンは、ONTAP 9のリリースに応じて決まります。ご使用の環境で必要なクライアントと機能がSMBサーバでサポートされていることを確認する必要があります。

タスクの内容

クライアントとドメインコントローラの両方と接続する場合は、可能なかぎりSMB 2.0以降を有効にしてください。セキュリティ上の理由から、SMB 1.0の使用は避け、ご使用の環境で不要であることが確認された場合は無効にしてください。

ONTAP 9では、SMBバージョン2.0以降がクライアント接続用にデフォルトで有効になりますが、デフォルトで有効になるSMB 1.0のバージョンはONTAPのリリースによって異なります。

- ONTAP 9 .1 P8以降では、SVMでSMB 1.0を無効にすることができます。

  コマンドのオプション `vserver cifs options modify`で、`SMB 1.0`を有効または無効にします `-smb1-enabled`。

- ONTAP 9 .3以降では、新しいSVMではデフォルトで無効になっています。

SMBサーバがActive Directory（AD）ドメイン内にある場合、ONTAP 9 .1以降では、SMB 2.0を有効にしてドメインコントローラ（DC）に接続できます。DCでSMB 1.0を無効にしている場合は、この処理が必要です。SMB.2以降では、ONTAP 9 2.0はDC接続に対してデフォルトで有効になっています。

> がwhileに `-smb1-enabled`設定されて `false`いる場合 `-smb1-enabled-for-dc-connections true`、ONTAPはクライアントとしてのSMB 1.0の接続を拒否しますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

"SMBの管理"サポートされるSMBのバージョンと機能の詳細が表示されます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 有効になっているSMBのバージョンを確認します。

   ```
   vserver cifs options show
   ```

   リストを下方向にスクロールすると、クライアント接続用に有効になっているSMBのバージョンを表示できます。また、ADドメイン内のSMBサーバを設定している場合は、ADドメイン接続用に有効になっているバージョンを表示できます。

3. 必要に応じて、クライアント接続用のSMBプロトコルを有効または無効にします。
   - SMBバージョンを有効にする場合：

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

有効な値 `smb_version`は次のとおりです。

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

次のコマンドは、SVM vs1.example.comでSMB 3.1を有効にします。
```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
-enabled true
```

◦ SMBバージョンを無効にするには：

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. SMBサーバがActive Directoryドメイン内にある場合は、必要に応じてDC接続用のSMBプロトコルを有効または無効にします。
   ◦ SMBバージョンを有効にする場合：

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   ◦ SMBバージョンを無効にするには：

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. admin権限レベルに戻ります。

```
set -privilege admin
```

DNSサーバでの**SMB**サーバのマッピング

Windows ユーザがドライブを SMB サーバ名にマッピングできるように、サイトの DNS サーバに、 SMB サーバ名および NetBIOS エイリアスをデータ LIF の IP アドレスにマッピングしたエントリを設定する必要があります。

開始する前に

サイトの DNS サーバに対する管理アクセス権が必要です。管理アクセス権がない場合は、 DNS 管理者にこのタスクの実行を依頼する必要があります。

タスクの内容

SMB サーバ名に NetBIOS エイリアスを使用する場合は、各エイリアスに DNS サーバのエントリポイントを作成することを推奨します。

手順

1. DNSサーバにログインします。
2. フォワードルックアップ（ A - アドレスレコード）とリバースルックアップ（ PTR - ポインタレコード）のエントリを作成して、 SMB サーバ名をデータ LIF の IP アドレスにマッピングします。
3. NetBIOS エイリアスを使用する場合は、エイリアスの正規名（ CNAME リソースレコード）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータ LIF の IP アドレスにマッピングします。

結果

ネットワーク全体にマッピングが反映されると、 Windows ユーザがドライブを SMB サーバ名またはその NetBIOS エイリアスにマッピングできるようになります。

共有ストレージへの**SMB**クライアントアクセスの設定

共有ストレージへの**SMB**クライアントアクセスの設定

SVM 上の共有ストレージに対する SMB クライアントアクセスを許可するには、ストレージコンテナを提供するボリュームまたは qtree を作成し、そのコンテナの共有を作成または変更する必要があります。その後、共有およびファイルの権限を設定し、クライアントシステムからのアクセスをテストできます。

開始する前に

- SVMでSMBの設定が完了している必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Active Directory ドメインまたはワークグループ設定への追加または変更が完了している必要があります。

ボリュームまたは**qtree**のストレージコンテナを作成する

ボリュームの作成

コマンドを使用すると、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create`。

タスクの内容

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームの作成時に指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、コマンドを使用して、SVMネームスペースでボリュームを_mount_theにする必要があります `volume mount`。

開始する前に

- SMBがセットアップされて実行されている必要があります。
- SVMのセキュリティ形式はNTFSである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する `volume create`か、 `-activity-tracking-state`に設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください "ファイルシステム分析を有効にする"。

手順

1. ジャンクションポイントを設定してボリュームを作成します。 `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*]

   の選択肢は `-junction-path`次のとおりです。

   - ルートの直下。例： `/new_vol`

     新しいボリュームを作成し、 SVM のルートボリュームに直接マウントされるように指定することができます。

   - 既存のディレクトリの下（例： `/existing_dir/new_vol`

     新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

   たとえば、新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は `/new_dir/new_vol`、SVMのルートボリュームにジャンクションされている新しい親ボリュームを最初に作成する必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

例

次のコマンドは、 SVM vs1.example.com およびアグリゲート aggr1 上に、 users1 という名前の新しいボリュームを作成します。新しいボリュームは、で使用でき `/users`ます。ボリュームのサイズは750GBで、ボリュームギャランティのタイプはvolume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

次のコマンドでは、「 home4` 」という名前の新しいボリュームを SVM 「 vs1.example.com`" 」およびアグリゲート「 aggr1 」に作成します。ディレクトリは /eng/`vs1 SVMのネームスペース内にすでに存在し、新しいボリュームがで使用可能になります `/eng/home。これがネームスペースのホームディレクトリになります。 /eng/`ボリュームのサイズは750GBで、ボリュームギャランティのタイプは（デフォルト）です `volume。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

qtreeを作成する

コマンドを使用すると、データを含むqtreeを作成し、そのプロパティを指定できます volume qtree create。

開始する前に

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVMのセキュリティ形式はNTFSであり、SMBがセットアップされて実行されている必要があります。

手順

1. qtreeを作成します。 volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs

   ボリュームとqtreeを別 々 の引数として指定するか、の形式でqtreeパスの引数を指定できます /vol/volume_name/_qtree_name。

2. 目的のジャンクションパスでqtreeが作成されたことを確認します。 volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }

例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成し`/vol/data1`ます。

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

SMB共有の作成に関する要件と考慮事項

SMB 共有を作成する前に、特にホームディレクトリに関して、共有パスと共有プロパティの要件を理解しておく必要があります。

SMB共有を作成するには、クライアントがアクセスするディレクトリパス構造を（コマンドのオプションを`vserver cifs share create`使用して）指定する必要があり`-path`ます。ディレクトリパスは、 SVM ネームスペース内に作成したボリュームまたは qtree のジャンクションパスに相当します。ディレクトリパスと対応するジャンクションパスは、共有を作成する前に存在している必要があります。

共有パスには次の要件があります。

- ディレクトリパス名の最大文字数は255文字です。
- パス名にスペースが含まれている場合は、文字列全体を引用符で囲む必要があります（例： `"/new volume/mount here"`）。
- (`\\servername\sharename\filepath`共有のUNCパスの文字数が256文字を超えている場合（UNCパスの先頭のは除く）、Windowsの[プロパティ]ボックスの*[セキュリティ]*タブは使用できません。

  これは、ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないでください。

共有プロパティのデフォルト値は変更できます。

- すべての共有のデフォルトの初期プロパティは `oplocks`、、 `browsable`、 `changenotify`および `show-previous-versions`です。
- 共有の作成時、共有プロパティの指定はオプションです。

  ただし、共有の作成時に共有プロパティを指定した場合、デフォルト値は使用されません。共有の作成時にパラメータを使用する場合 `-share-properties`は、共有に適用するすべての共有プロパティをカンマで区切って指定する必要があります。

- ホームディレクトリ共有を指定するには、プロパティを使用し `homedirectory`ます。

  この機能を使用すると、接続するユーザと一連の変数に基づいてさまざまなディレクトリにマッピングされる共有を設定できます。ユーザごとに別個の共有を作成する必要はありません。 1 つの共有を設定し、いくつかのホームディレクトリパラメータを指定して、エントリポイント（共有）とユーザのホームディレクトリ（ SVM 上のディレクトリ）間のユーザの関係を定義します。

  共有の作成後にこのプロパティを追加または削除することはできません。

ホームディレクトリの共有には次の要件があります。

- SMBホームディレクトリを作成する前に、コマンドを使用して、ホームディレクトリ検索パスを少なくとも1つ追加する必要があります `vserver cifs home-directory search-path add`。
- パラメータの `-share-properties`値をに指定するホームディレクトリ共有で `homedirectory`は、（`Windows`ユーザ名）動的変数を共有名に含める必要があります `%w`。

  共有名には、さらに（ドメイン名）動的変数（など `%d/%w`）を含めることも、静的な部分（など `home1_%w`）を含めることもできます `%d`。

- 管理者またはユーザが他のユーザのホームディレクトリに接続するために共有を使用する場合（コマンドのオプションを使用）は `vserver cifs home-directory modify`、動的な共有名のパターンの先頭にチルダを付ける必要があり(`~`ます。

"SMBの管理"および `vserver cifs share`のマニュアルページに追加情報が記載されています。

SMB共有を作成する

SMB サーバのデータを SMB クライアントと共有するには、 SMB 共有を作成する必要があります。共有を作成するときは、共有をホームディレクトリとして指定するなど、共有プロパティを設定できます。オプションの設定により、共有をカスタマイズすることもできます。

開始する前に

共有を作成する前に、ボリュームまたは qtree のディレクトリパスが SVM ネームスペース内に存在している必要があります。

タスクの内容

共有を作成するときのデフォルトの共有ACL（デフォルトの共有権限）はです `Everyone / Full Control`。共有へのアクセスをテストしたら、デフォルトの共有 ACL を削除し、より安全な方法で置き換える必要があります。

手順

1. 必要に応じて、共有のディレクトリパス構造を作成します。

   コマンドは `vserver cifs share create`、共有の作成時にオプションで指定されたパスをチェックし `-path`ます。指定したパスが存在しない場合、コマンドは失敗します。

2. 指定したSVMに関連付けられているSMB共有を作成します。 `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`

3. 共有が作成されたことを確認します。`vserver cifs share show -share-name share_name`

例

次のコマンドは、「SHARE1」という名前のSMB共有をSVM上に作成し `vs1.example.com`ます。ディレクトリパスはで `/users`、デフォルトのプロパティを使用して作成されます。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

SMBクライアントアクセスの確認

共有にアクセスしてデータを書き込むことで、 SMB が正しく設定されていることを確認する必要があります。SMB サーバ名と NetBIOS エイリアスを使用してアクセスをテストします。

手順

1. Windows クライアントにログインします。
2. SMB サーバ名を使用してアクセスをテストします。

   a. エクスプローラで、次の形式で共有にドライブをマッピングします。 `\\SMB_Server_Name\Share_Name`

      正常にマッピングされない場合は、 DNS マッピングがネットワーク全体にまだ反映されていない可能性があります。しばらく待ってから、再度 SMB サーバ名を使用してアクセスをテストしてください。

      SMBサーバの名前がvs1.example.comで、共有の名前がSHARE1の場合は、次のように入力します。 `\\vs0.example.com\SHARE1`

b. 新しく作成したドライブで、テストファイルを作成して削除します。

SMB サーバ名を使用した共有への書き込みアクセスが可能であることを確認できました。

3. NetBIOS エイリアスについて手順 2 を繰り返します。

SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List（ACL；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

開始する前に

共有へのアクセスを許可するユーザまたはグループを決めておく必要があります。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があり `Everyone / Full Control`ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. 新しいACLを設定します。

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsユーザ	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`
Windowsグループ	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com`"SVM:」上の「sales」共有の「sales Team」Windowsグループに権限を与えます `Change`。

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

次のコマンドは、SVM「vs1」上の「datavol5」共有に対する「Tiger Team」という名前のローカルWindowsグループへの権限と「See Chang」という名前のローカルWindowsユーザへの権限 `Full_Control`を付与します `Change`。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

共有での**NTFS**ファイル権限の設定

共有にアクセスできるユーザまたはグループにファイルアクセスを有効にするには、その共有内のファイルおよびディレクトリに対するNTFSファイル権限をWindowsクライアントから設定する必要があります。

開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

タスクの内容

"SMBの管理"標準および詳細なNTFS権限の設定方法については、Windowsのマニュアルを参照してください。

手順

1. Windows クライアントに管理者としてログインします。
2. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
3. [ネットワークドライブの割り当て *] ボックスに入力します。

   a. ドライブ文字を選択します。

   b. [* フォルダ *] ボックスに、権限を適用するデータと共有名を含む共有を含む SMB サーバー名を入力します。

      SMBサーバ名がSMB_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します。
      `\\SMB_SERVER01\SHARE1`

      SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

   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、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

4. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
5. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
6. [* セキュリティ *] タブを選択します。

   Security タブには、 NTFS 権限が設定されているユーザとグループのリストが表示されます。[< オブジェクト > のアクセス許可] ボックスには、選択したユーザーまたはグループの有効なアクセス許可と拒否のアクセス許可のリストが表示されます。

7. [編集（ Edit ）] をクリックします。

   [< オブジェクト > のアクセス許可] ボックスが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループに対する標準の NTFS 権限を設定します	a. [追加]*をクリックします。 [ユーザー、コンピュータ、サービスアカウント、またはグループの選択] ウィンドウが開きます。 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、 NTFS アクセス権を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に対する標準の NTFS 権限を変更または削除する	[* グループ名またはユーザー名 *] ボックスで、変更または削除するユーザーまたはグループを選択します。

9. 次のうち必要な操作を実行します。

状況	実行する処理
新規または既存のユーザまたはグループに対する標準の NTFS 権限を設定する	[* パーミッション for < オブジェクト >*] ボックスで、選択したユーザーまたはグループに対して許可または許可しないアクセスのタイプの [許可 *] または [拒否 *] ボックスを選択します。
ユーザまたはグループを削除します	[削除（ Remove ）] をクリックします。

標準の権限ボックスの一部またはすべてを選択できない場合、権限は親オブジェクトから継承されます。[* 特別な権限 *] ボックスは選択できません。選択されている場合は、選択したユーザまたはグループに対して詳細な権限が 1 つ以上設定されていることを意味します。

10. そのオブジェクトの NTFS アクセス権の追加、削除、または編集が完了したら、 **OK** をクリックします。

ユーザアクセスを確認

設定したユーザが、 SMB 共有およびその中に含まれるファイルにアクセスできることをテストする必要があります。

手順

1. Windows クライアントで、共有へのアクセスを許可したいずれかのユーザとしてログインします。
2. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
3. [ネットワークドライブの割り当て *] ボックスに入力します。

   a. ドライブ文字を選択します。

   b. [* フォルダー *] ボックスに、ユーザーに提供する共有名を入力します。

SMBサーバ名がSMB_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します。
`\\SMB_SERVER01\share1`

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、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

4. テストファイルを作成し、その存在を確認し、テキストを書き込んで、テストファイルを削除します。

CLIを使用したSMBの管理

SMBの概要

SMBプロトコルでは、ONTAPファイルアクセス機能を使用できます。CIFSサーバの有効化、共有の作成、およびMicrosoftサービスの有効化を行うことができます。

SMB(Server Message Block) は、 Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（ CLI ）および OnCommand 管理ツールでは、 _cifs_という メッセージが引き続き表示されます。

SMBサーバのサポート

SMBサーバのサポートの概要

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

- クラスタ内のデータSVMは、それぞれ1つのActive Directoryドメインにバインドできます。
- データSVMを同じドメインにバインドする必要はありません。
- 複数のSVMを同じドメインにバインドできます。

SMBサーバを作成する前に、データの提供に使用するSVMとLIFを設定する必要があります。データネットワークがフラットでない場合は、IPspace、ブロードキャストドメイン、およびサブネットの設定も必要になることがあります。

関連情報

"ネットワーク管理"

SMBサーバの変更

"システム管理"

サポートされるSMBのバージョンと機能

Server Message Block（SMB；サーバメッセージブロック）は、Microsoft Windowsのクライアントおよびサーバで使用されるリモートファイル共有プロトコルです。ONTAP 9ではすべてのSMBバージョンがサポートされますが、デフォルトでサポートされるSMB

1.0はONTAPのバージョンによって異なります。ONTAP SMBサーバが、ご使用の環境で必要なクライアントと機能をサポートしていることを確認する必要があります。

ONTAP がサポートする SMB クライアントおよびドメインコントローラの最新情報については、Interoperability Matrix Tool を参照してください。

SMB 2.0以降のバージョンは、ONTAP 9 SMBサーバではデフォルトで有効になっており、必要に応じて有効または無効にすることができます。次の表に、SMB 1.0のサポートとデフォルトの設定を示します。

SMB 1.0の機能：	**ONTAP 9** のリリース：			
	9.0	9.1	9.2	9.3以降
デフォルトで有効	○	○	○	いいえ
有効/無効を切り替えることができます。	いいえ	はい * 9.1 P8 以降が必要です。	○	○

ドメインコントローラへのSMB 1.0および2.0接続のデフォルト設定も、ONTAPのバージョンによって異なります。詳細については、のマニュアルページを参照し `vserver cifs security modify`てください。既存のCIFSサーバでSMB 1.0を実行している環境では、できるだけ早く新しいバージョンのSMBに移行して、セキュリティとコンプライアンスを強化する必要があります。詳細については、NetApp担当者にお問い合わせください。

次の表に、SMBの各バージョンでサポートされるSMBの機能を示します。SMBの機能には、デフォルトで有効になるものと、追加の設定が必要なものがあります。

* この機能： *	* 有効化が必要： *	* **ONTAP 9** では、以下のバージョンの **SMB** がサポートされています。 *				
		1.0	2.0	2.1	3.0	3.1.1
従来のSMB 1.0の機能		X	X	X	X	X
永続性ハンドル			X	X	X	X
複合操作			X	X	X	X
非同期操作			X	X	X	X
読み取り/書き込みバッファサイズの増加			X	X	X	X

* この機能： *	* 有効化が必要： *	* **ONTAP 9** では、以下のバージョンの **SMB** がサポートされています。 *				
拡張性の向上			X	X	X	X
SMBシヨメイ	X	X	X	X	X	X
代替データストリーム（ADS）ファイル形式	X	X	X	X	X	X
Large MTU（ONTAP 9 7以降ではデフォルトで有効）	X			X	X	X
oplockリース				X	X	X
継続的可用性を備えた共有	X				X	X
永続的ハンドル					X	X
監視					X	X
SMB 暗号化：AES-128-CCM	X				X	X
スケールアウト（CA共有で必要）					X	X
透過的なフェイルオーバー					X	X
SMBマルチチャネル（ONTAP 9 4以降）	X				X	X
事前認証の整合性						X

* この機能： *	* 有効化が必要： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
クラスタ・クライアント・フェイルオーバーv.2（CCFv2）						X
SMB暗号化：AES-128-GCM（ONTAP 9 .1以降）	X					X

関連情報

SMB署名を使用したネットワークセキュリティの強化

SMBサーバの最小認証セキュリティレベルの設定

SMB経由のデータ転送でのSMBサーバでのSMB暗号化要求の設定

"NetAppの相互運用性"

サポートされない**Windows**の機能

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

ONTAP では、次の Windows 機能はサポートされません。

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

SVM上の**NIS**または**LDAP**ネームサービスの設定

SMBアクセスでは、NTFSセキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIXユーザへのユーザマッピングが常に実行されます。NISまたはLDAPディ

レクトリストアに情報が格納されているUNIXユーザにWindowsユーザをマッピングする場合や、ネームマッピングにLDAPを使用する場合は、SMBのセットアップ時にこれらのネームサービスを設定する必要があります。

開始する前に

ネームサービスインフラに合わせてネームサービスデータベース設定をカスタマイズしておく必要があります。

タスクの内容

SVMは、ネームサービスns-switchデータベースを使用して、指定されたネームサービスデータベースを検索するソースの順序を決定します。ns-switchソースには、、 `nis`、または `ldap`を任意に組み合わせて指定できます `files`。グループデータベースの場合、ONTAPは設定されているすべてのソースからグループメンバーシップを取得しようとし、統合されたグループメンバーシップ情報をアクセスチェックに使用します。UNIXグループ情報の取得時にこれらのソースのいずれかが使用できないと、ONTAPは完全なUNIXクレデンシャルを取得できず、以降のアクセスチェックが失敗することがあります。そのため、ns-switch設定でグループデータベースのすべてのns-switchソースが設定されていることを常に確認する必要があります。

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

手順

1. UNIXユーザ、グループ、およびネットグループ情報がNISネームサービスによって管理されている場合は、NISネームサービスを次のように設定します。

   a. コマンドを使用して、ネームサービスの現在の順番を確認します `vserver services name-service ns-switch show`。

      この例では、ネームサービスソースとして使用できる3つのデータベース(`group`、 `passwd`および`netgroup`） `nis`がソースとしてのみを使用しています `files`。

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

      ```
                                                   Source
      Vserver         Database       Enabled       Order
      --------------- ------------   ---------     ---------
      vs1             hosts          true          dns,
                                                   files
      vs1             group          true          files
      vs1             passwd         true          files
      vs1             netgroup       true          files
      vs1             namemap        true          files
      ```

      ソースを `group`データベースと `passwd`データベースに追加する必要があります。必要に応じてデータベースにも `netgroup`追加できます `nis`。

   b. コマンドを使用して、ネームサービスns-switchデータベースを必要な順番に調整します `vserver`

services name-service ns-switch modify。

パフォーマンスを最大限に高めるには、SVMで設定する予定でないネームサービスデータベースにネームサービスを追加しないでください。

複数のネームサービスデータベースの設定を変更する場合は、変更する各ネームサービスデータベースに対して個別にコマンドを実行する必要があります。

この例では、 `nis`および `files`がデータベースおよび `passwd`のソースとしてこの順序で設定されてい `group`ます。残りのネームサービスデータベースは変更されません。

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

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

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

```
                                                Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. NISネームサービス設定を作成します。+
```
vserver services name-service nis-domain create -vserver <vserver_name>
-domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…
```

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

> ONTAP 9 .2以降では、 `-nis-servers`フィールドがフィールドに置き換わります `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

e. NISネームサービスが適切に設定されていることを確認します。 `vserver services name-service nis-domain show vserver <vserver_name>`

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

```
Vserver         Domain                Server
--------------- --------------------- ---------------
vs1             example.com           10.0.0.60
```

2. UNIXユーザ、グループ、ネットグループ情報またはネームマッピングがLDAPネームサービスによって管理されている場合は、場所にある情報を使用してLDAPネームサービスを設定します"NFSの管理"。

ONTAPネームサービススイッチ設定の仕組み

ONTAPでは、UNIXシステムの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 `/etc/nsswitch.conf`。このテーブルを環境に合わせて適切に設定できるように、このテーブルの機能とONTAPでの使用方法を理解しておく必要があります。

ONTAPネームサービススイッチテーブルは、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序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、SVMごとにONTAPで管理されます。

データベースタイプ

このテーブルには、次のデータベースタイプごとに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
ホスト	ホスト名からIPアドレスへの変換	フアイル、DNS
グループ	ユーザグループ情報の検索	フアイル、NIS、LDAP
パスワード	ユーザ情報の検索	フアイル、NIS、LDAP
ネットグループ	ネットグループ情報の検索	フアイル、NIS、LDAP
namemap	ユーザ名のマッピング	フアイル、LDAP

ソースタイプ

ソースによって、適切な情報の取得に使用するネームサービスソースが指定されます。

ソースタイプ	情報の検索先	使用するコマンド

ファイル	ローカルソースファイル	`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を使用する場合でも、NISまたはLDAP認証が失敗した場合に備えて、ローカルユーザをフォールバックとして含めて設定しておく必要があります `files`。

外部ソースへのアクセスに使用するプロトコル

ONTAPでは、外部ソースのサーバにアクセスするために、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

次の例は、SVMのネームサービススイッチ設定を表示します `svm_1`。

```
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
```

ユーザーまたはグループ情報を検索するために、ONTAPはローカルソースファイルのみを参照します。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を検索するために、ONTAPは最初に外部NISサーバを参照します。クエリから結果が返されない場合は、次にローカルネットグループファイルがチェックされます。

SVM svm_1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ありません。したがって、ONTAPはデフォルトでローカルソースファイルのみを参照します。

SMBサーバを管理します。

SMBサーバの変更

コマンドを使用して、ワークグループからActive Directoryドメイン、ワークグループから別のワークグループ、またはActive DirectoryドメインからワークグループにSMBサーバを移動できます `vserver cifs modify`。

タスクの内容

SMB サーバ名や管理ステータスなど、 SMB サーバのその他の属性を変更することもできます。詳細については、のマニュアルページを参照してください。

選択肢

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。

  a. SMBサーバの管理ステータスをに設定します `down`。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. ワークグループからActive DirectoryドメインにSMBサーバを移動します。 `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

SMBサーバ用のActive Directoryマシンアカウントを作成するには、.comドメイン内のコンテナ *example*`にコンピュータを追加するための十分なPrivilegesを備えたWindowsアカウントの名前とパスワードを指定する必要があります `ou=*example* ou。

ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ`vserver cifs`にそのURIを含め `-keytab-uri`ます。

- ワークグループから別のワークグループに SMB サーバを移動します。
  a. SMBサーバの管理ステータスをに設定します down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. SMBサーバのワークグループを変更します。 `vserver cifs modify -vserver *vserver_name* -workgroup *new_workgroup_name*`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory ドメインからワークグループに SMB サーバを移動するには、次の手順を実行します。
  a. SMBサーバの管理ステータスをに設定します down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Active Directoryドメインからワークグループに SMBサーバを移動します。 `vserver cifs modify -vserver *vserver_name* -workgroup *workgroup_name*`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

ワークグループモードに切り替えるには、継続的可用性を備えた共有、シャドウコピー、 AES など、ドメインベースの機能をすべて無効にし、該当する設定がシステムによって自動的に削除されるようにする必要があります。ただし、「 EXAMPLE.COM\userName" 」などのドメインで設定された共有 ACL は正しく機能しませんが、 ONTAP で削除することはできません。このような共有 ACL は、コマンドの完了後できるだけ早く外部ツールを使用して削除してください。AES が有効になっている場合は、「 example.com 」ドメインで AES を無効にするための十分な権限を持つ Windows アカウントの名前とパスワードの入力を求められることがあります。

  - その他の属性を変更するには、コマンドの該当するパラメータを使用し `vserver cifs modify`ます。

オプションを使用した**SMB**サーバのカスタマイズ

SMBサーバのカスタマイズ方法を検討する場合は、使用可能なオプションを把握しておくと役立ちます。一部のオプションは一般的なものですが、SMBの特定の機能を有効にして設定するためのオプションもいくつかあります。SMBサーバオプションは、オプションで制御し `vserver cifs options modify`ます。

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

- * SMB セッションタイムアウト値の設定 *

  このオプションでは、SMBセッションが切断されるまでのアイドル時間（秒）を指定できます。アイドルセッションとは、ユーザがクライアント上でファイルやディレクトリを開いていないセッションのことです。デフォルト値は900秒です。

- * デフォルトの UNIX ユーザーの構成 *

  このオプションでは、SMBサーバで使用するデフォルトのUNIXユーザを指定できます。ONTAP はデフォルトユーザ「 pcuser 」（ UID は 65534 ）を自動的に作成し、グループ「 pcuser 」（ GID は 65534 ）を作成して、デフォルトユーザを「 pcuser 」グループに追加します。SMB サーバを作成すると、 ONTAP は自動的に「 pcuser 」をデフォルトの UNIX ユーザとして設定します。

- * ゲスト UNIX ユーザの設定 *

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

- * モードビットの読み取り権限付与の実行の有効化または無効化 *

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

- * NFS クライアントからの読み取り専用ファイルの削除機能の有効化または無効化 *

  このオプションを有効または無効にして、読み取り専用属性が設定されたファイルまたはフォルダの削除をNFSクライアントに許可するかどうかを指定します。NTFSの削除セマンティクスでは、読み取り専用属性が設定されている場合、ファイルやフォルダの削除は許可されません。UNIXの削除セマンティクスでは読み取り専用ビットが無視され、代わりに親ディレクトリの権限を使用してファイルまたはフォルダを削除できるかどうかが判断されます。デフォルトの設定はで `disabled`、NTFSの削除セマンティクスが適用されます。

- * Windows Internet Name Service サーバーアドレスの設定 *

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

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

- * CIFS ユーザーへの UNIX グループ権限の付与 *

  このオプションでは、ファイルの所有者ではない受信CIFSユーザにグループ権限を付与するかどうかを指定します。CIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合にこのパラメータをに設定する `true`と、ファイルに対するグループ権限が付与されます。`CIFS`ユーザが`UNIX`セキュリティ形式のファイルの所有者ではない場合に、このパラメータをに設定する `false`と、通常の`UNIX`ルールに従ってファイル権限が付与されます。このパラメータは、権限がに設定された`UNIX`セキュリティ形式のファイルに適用さ `mode bits`れます。セキュリティモードが`NTFS`または`NFSv4`のファイルには適用されません。デフォルト設定はです `false`。

- * SMB 1.0の有効化または無効化*

  ONTAP 9にSMBサーバが作成されているSVMでは、SMB 1.0はデフォルトで無効になっています。3.

  > SMB.3以降ではONTAP 9、SMB.3で作成された新しいONTAP 9サーバについてはSMB 1.0がデフォルトで無効になります。セキュリティとコンプライアンスの強化に備えて、できるだけ早く新しいバージョンのSMBに移行する必要があります。詳細については、NetApp担当者にお問い合わせください。

- * SMB 2.x の有効化または無効化 *

  SMB 2.0は、LIFフェイルオーバーをサポートするSMBの最小バージョンです。SMB 2.xを無効にすると、ONTAPはSMB 3.Xも自動的に無効にします。

  SMB 2.0はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * SMB 3.0の有効化または無効化*

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

  SMB 3.0はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * SMB 3.1の有効化または無効化*

  Windows 10は、SMB 3.1をサポートする唯一のWindowsバージョンです。

  SMB 3.1はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * ODX コピーオフロードの有効化または無効化 *

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

- * ODX コピーオフロードの直接コピーメカニズムの有効化または無効化 *

  直接コピーメカニズムを使用すると、Windowsクライアントがコピーの実行中にファイルが変更されないモードでコピーのソースファイルを開こうとすると、コピーオフロード処理のパフォーマンスが向上します。デフォルトでは、直接コピーメカニズムが有効になっています。

- * 自動ノードリファーラルの有効化または無効化 *

  自動ノードリファーラルでは、SMBサーバはクライアントに対して、要求した共有を介してアクセスするデータのホストノードに対してローカルなデータLIFを自動的に参照することになります。

- * SMB * のエクスポート・ポリシーの有効化または無効化

  このオプションは、デフォルトでは無効になっています。

- * ジャンクションポイントのリパースポイントとしての使用の有効化または無効化 *

  このオプションを有効にすると、SMBサーバはジャンクションポイントをリパースポイントとしてSMBクライアントに公開します。このオプションは、SMB 2.x接続またはSMB 3.0接続でのみ有効です。このオプションはデフォルトで有効になっています。

  このオプションはSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * TCP 接続ごとの最大同時操作数の設定 *

  デフォルト値は255です。

- * ローカルの Windows ユーザーとグループ機能の有効化または無効化 *

  このオプションはデフォルトで有効になっています。

- * ローカル Windows ユーザー認証の有効化または無効化 *

  このオプションはデフォルトで有効になっています。

- * VSS シャドウ・コピー機能の有効化または無効化 *

  ONTAPでは、シャドウコピー機能を使用して、Hyper-V over SMBソリューションを使用して格納されたデータのリモートバックアップを実行します。

  このオプションは、SVM、およびHyper-V over SMB構成でのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * シャドウ・コピーのディレクトリ階層の設定 *

  このオプションを設定すると、シャドウコピー機能を使用する場合に、シャドウコピーを作成するディレクトリの最大階層を定義できます。

  このオプションは、SVM、およびHyper-V over SMB構成でのみサポートされます。このオプションは、SVMではデフォルトで有効になっています。

- * マルチドメインネームマッピングの検索機能の有効化または無効化 *

  有効にすると、 UNIX ユーザが Windows ユーザ名のドメイン部分にワイルドカード（ * ）を使用して Windows ドメインユーザにマッピングされている場合に（ * \joe など）、 ONTAP はホームドメインと双方向の信頼関係が確立されたすべてのドメインで、指定したユーザを検索します。ホームドメインは、SMBサーバのコンピュータアカウントが含まれているドメインです。

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。このオプションを有効にして優先リストを設定すると、その優先リストを使用してマルチドメインネームマッピングの検索が実行されます。

デフォルトでは、マルチドメインネームマッピングの検索は有効になります。

- * ファイルシステムセクターサイズの設定 *

  このオプションでは、ONTAPがSMBクライアントに報告するファイルシステムセクターサイズをバイト単位で設定できます。このオプションには、との `512`2つの有効な値があります `4096`。デフォルト値はです `4096`。Windowsアプリケーションが512バイトのセクターサイズのみをサポートしている場合は、この値をに設定する必要が `512`あります。

- * ダイナミックアクセス制御の有効化または無効化 *

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

  このオプションはSVMでのみサポートされます。

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

  このオプションを設定すると、認証されていないセッションのアクセス制限を指定できます。制限は匿名ユーザに適用されます。デフォルトでは、匿名ユーザに対するアクセス制限はありません。

- * UNIX 対応のセキュリティを使用するボリューム（ UNIX セキュリティ形式のボリューム、または UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）での NTFS ACL の提供を有効または無効にする *

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

- * SMB 擬似オープン機能の有効化または無効化 *

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

- * UNIX 拡張の有効化または無効化 *

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

  Mac OSXクライアントなどのUNIXベースのSMBクライアントが環境内にある場合は、UNIX拡張を有効にする必要があります。UNIX拡張を有効にすると、SMBサーバはPOSIX/UNIXセキュリティ情報をSMB経

由でUNIXベースのクライアントに送信できるようになります。クライアントは、受け取ったセキュリティ情報をPOSIX/UNIXセキュリティに変換します。

- * 略称を使用した検索のサポートの有効化または無効化 *

  このオプションを有効にすると、SMBサーバは短縮名に対して検索を実行できます。このオプションを有効にした検索クエリでは、8.3形式のファイル名と長いファイル名が照合されます。このパラメータのデフォルト値はです `false`。

- * DFS 対応の自動通知のサポートの有効化または無効化 *

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

- * SMB クレジットの最大数の設定 *

  ONTAP 9 .4以降では、クライアントとサーバがSMBバージョン2以降を実行している場合に、オプションを設定して `-max-credits`SMB接続に付与するクレジット数を制限できます。デフォルト値は128です。

- * SMB マルチチャネルのサポートの有効化または無効化 *

  ONTAP 9 .4以降のリリースでこのオプションを有効にする `-is-multichannel-enabled`と、クラスタとそのクライアントに適切なNICが導入されている場合に、SMBサーバは単一のSMBセッションに対して複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。このパラメータのデフォルト値はです `false`。

  SMBマルチチャネルが有効な場合は、次のパラメータも指定できます。

  - マルチチャネルセッションごとに許可される最大接続数。このパラメータのデフォルト値は32です。
  - マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。このパラメータのデフォルト値は256です。

SMBサーバオプションの設定

SMBサーバオプションは、Storage Virtual Machine（SVM）でのSMBサーバの作成後にいつでも設定できます。

ステップ

1. 必要な操作を実行します。

SMBサーバオプションの設定	入力するコマンド
admin権限レベルで設定	`vserver cifs options modify -vserver` *`vserver_name options`*

SMBサーバオプションの設定	入力するコマンド
advanced権限レベルで設定	a. `set -privilege advanced` b. `vserver cifs options modify -vserver vserver_name options` c. `set -privilege admin`

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

SMBユーザへのUNIXグループ権限付与の設定

このオプションを設定すると、受信SMBユーザがファイルの所有者でない場合でも、ファイルまたはディレクトリにアクセスするグループ権限を付与できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. UNIXグループ権限付与を必要に応じて設定します。

状況	入力するコマンド
ユーザがファイルの所有者でない場合にもファイルやディレクトリにアクセスするためのグループ権限を付与する	`vserver cifs options modify –grant-unix-group-perms-to-others true`
ユーザがファイルの所有者でない場合でも、ファイルまたはディレクトリへのアクセスを無効にしてグループ権限を取得する	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. admin権限レベルに戻ります。 `set -privilege admin`

匿名ユーザに対するアクセス制限の設定

デフォルトでは、認証されていない匿名ユーザ（ _null ユーザ）はネットワーク上の特定の情報にアクセスできます。SMBサーバオプションを使用して、匿名ユーザに対するアクセス制限を設定できます。

タスクの内容

`-restrict-anonymous`SMBサーバオプションは、Windowsのレジストリエントリに対応し`RestrictAnonymous`ます。

匿名ユーザは、ユーザ名と詳細、アカウントポリシー、共有名など、ネットワーク上のWindowsホストから特

定のタイプのシステム情報をリストまたは列挙できます。匿名ユーザのアクセスを制御するには、次の3つのアクセス制限設定のいずれかを指定します。

値	説明
`no-restriction` （デフォルト）	匿名ユーザに対するアクセス制限を指定しません。
`no-enumeration`	匿名ユーザに対して列挙だけを制限します。
`no-access`	匿名ユーザに対してアクセスを制限します。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. restrict anonymousを設定します。 `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver` *`vserver_name`*
4. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

使用できるSMBサーバオプション

UNIXセキュリティ形式のデータに対するファイルセキュリティの**SMB**クライアントへの提供方法を管理します。

UNIXセキュリティ形式のデータに関してファイルセキュリティを**SMB**クライアントに提供する方法の概要を管理します。

SMBクライアントへのNTFS ACLの提供を有効または無効にすることで、UNIXセキュリティ形式のデータに関するファイルセキュリティをSMBクライアントに提供する方法を選択できます。それぞれの設定には利点があり、ビジネス要件に最適な設定を選択するために理解しておく必要があります。

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

- Windows の [プロパティ] ボックスの [セキュリティ *] タブを使用して、 UNIX アクセス権を表示および編集する。

  処理がUNIXシステムで許可されていない場合、Windowsクライアントから権限を変更することはできません。たとえば、所有していないファイルの所有権は変更できません。これは、UNIXシステムではこの処理が許可されていないためです。この制限により、SMBクライアントはファイルやフォルダに対して設定されたUNIXアクセス権をバイパスできないようになっています。

- UNIXセキュリティ形式のボリューム上のファイルの編集や保存に特定のWindowsアプリケーション（Microsoft Officeなど）を使用しており、ONTAPでの保存時にUNIXアクセス権を維持する必要がある場合。
- 使用するファイルのNTFS ACLを読み取ることを想定した特定のWindowsアプリケーションが環境内にあ

ります。

状況によっては、NTFS ACLとしてのUNIXアクセス権の提供を無効にすることができます。この機能を無効にすると、ONTAPはUNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供します。UNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供する理由はいくつかあります。

- UNIXアクセス権を変更するには、UNIXクライアントでマウントを使用する必要があります。

  UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合は、[セキュリティ]タブは使用できません。マッピングされたドライブは、ファイル権限がないFATファイルシステムでフォーマットされているように見えます。

- SMBを介したアプリケーションを使用している場合、アクセスするファイルやフォルダにNTFS ACLを設定していますが、データがUNIXセキュリティ形式のボリューム上にあると失敗する可能性があります。

  ONTAPでボリュームがFATと報告された場合、アプリケーションはACLの変更を試行しません。

関連情報

FlexVolでのセキュリティ形式の設定

qtreeでのセキュリティ形式の設定

UNIXセキュリティ形式のデータに対する**NTFS ACL**の提供を有効または無効にする

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

タスクの内容

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

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. UNIX NTFS ACLオプションを設定します。 `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
4. admin権限レベルに戻ります。 `set -privilege admin`

ONTAPによる**UNIX**アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、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、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

Windowsの[セキュリティ]タブを使用したUNIXアクセス権の管理

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれ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できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 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できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限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 アクセス権を NTFS アクセス権に変更しています

  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のセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの 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。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式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。

SMBサーバのセキュリティ設定を管理します。

ONTAPによるSMBクライアント認証の処理

SMB接続を確立してSVMに格納されているデータにアクセスする前に、ユーザはSMBサーバが属しているドメインで認証される必要があります。SMBサーバでは、KerberosとNTLM（NTLMv1またはNTLMv2）の2つの認証方式がサポートされます。Kerberos

は、ドメインユーザの認証に使用されるデフォルトの方法です。

Kerberos認証

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

KerberosはActive Directoryのプライマリ認証サービスです。KerberosサーバまたはKerberos Key Distribution Center（KDC；キー配布センター）サービスは、Active Directoryのセキュリティ原則に関する情報を格納および取得します。NTLMモデルとは異なり、SMBサーバなどの別のコンピュータとのセッションを確立するActive Directoryクライアントは、KDCに直接接続してセッションクレデンシャルを取得します。

NTLM認証

NTLMクライアント認証は、パスワードに基づくユーザ固有のシークレットの共有情報に基づくチャレンジ応答プロトコルを使用して行われます。

ユーザがローカルのWindowsユーザアカウントを使用してSMB接続を作成した場合、認証はSMBサーバによってNTLMv2を使用してローカルに行われます。

SVM ディザスタリカバリ構成での **SMB** サーバセキュリティ設定に関するガイドライン

IDが保持されないディザスタリカバリデスティネーションとして設定されているSVMを作成する前に（ `-identity-preserve`SnapMirror構成でオプションがに設定されている `false`）、デスティネーションSVMでのSMBサーバセキュリティ設定の管理方法を確認しておく必要があります。

- デフォルト以外の SMB サーバセキュリティ設定はデスティネーションにレプリケートされません。

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

- デフォルト以外の SMB サーバセキュリティ設定は手動で設定する必要があります。

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

SMBサーバのセキュリティ設定に関する情報を表示する

Storage Virtual Machine（SVM）上のSMBサーバセキュリティ設定に関する情報を表示できます。この情報を使用して、セキュリティ設定が正しいことを確認できます。

タスクの内容

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

一部のオプションが無効なため、ワークグループモードのSMBサーバに対してはコマンドを使用しない `vserver cifs security show`でください。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定したSVMのすべてのセキュリティ設定	`vserver cifs security show -vserver` *vserver_name*
SVMの特定のセキュリティ設定	`vserver cifs security show -vserver` _vserver_name_ `-fields [fieldname,...]`と入力して、使用できるフィールドを指定できます `-fields ?`。

例

次の例は、SVM vs1のすべてのセキュリティ設定を表示します。

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

Vserver: vs1

                           Kerberos Clock Skew:        5 minutes
                           Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:         7 days
                         Kerberos KDC Timeout:         3 seconds
                           Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:        false
                         LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:        false
                        Client Session Security:        none
               SMB1 Enabled for DC Connections:         false
               SMB2 Enabled for DC Connections:         system-default
LDAP Referral Enabled For AD LDAP connections:         false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:         false
 AES session key enabled for NetLogon channel:         false
  Try Channel Binding For AD LDAP Connections:         false
```

表示される設定は、実行中のONTAPのバージョンによって異なります。

次の例は、SVM vs1のKerberosのクロックスキューを表示します。

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

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

関連情報

GPO設定に関する情報の表示

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

パスワードの複雑さの要件を使用すると、Storage Virtual Machine（SVM）上のローカルSMBユーザに対するセキュリティを強化できます。パスワードの複雑さの要件はデフォルトでは有効になっています。この機能は、いつでも無効にして再度有効にすることができます。

開始する前に

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

タスクの内容

一部のオプションが無効なため、ワークグループモードのCIFSサーバに対してはコマンドを使用しないで `vserver cifs security modify`ください。

手順

1. 次のいずれかを実行します。

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

2. パスワードの複雑さの要件に関するセキュリティ設定を確認します。 `vserver cifs security show -vserver` *`vserver_name`*

例

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

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

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

関連情報

CIFSサーバのセキュリティ設定に関する情報の表示

ローカルユーザおよびローカルグループを使用した認証と許可

ローカルユーザのパスワードの要件

ローカルユーザアカウントのパスワードの変更

CIFSサーバの**Kerberos**セキュリティ設定を変更します。

許可されるKerberosクロックスキューの最大時間、Kerberosチケットの有効期間、チケットを更新する最大日数など、CIFSサーバのKerberosセキュリティ設定を変更できます。

タスクの内容

コマンドによるCIFSサーバのKerberos設定の変更では `vserver cifs security modify`、パラメータで指定した単一のStorage Virtual Machine（SVM）の設定のみを変更 `-vserver`できます。Active Directoryのグループポリシーオブジェクト（GPO）を使用すると、同じActive Directoryドメインに属するクラスタ上のすべてのSVMのKerberosセキュリティ設定を一元管理できます。

手順

1. 次の操作を1つ以上実行します。

状況	入力するコマンド
Kerberosクロックスキューの許容最大時間を分（9.13.1以降）または秒（9.12.1以前）で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* デフォルト設定は5分です。
Kerberosチケットの有効期間を時間単位で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` デフォルト設定は10時間です。

チケットの最大更新日数を指定します。	`vserver cifs security modify -vserver` *vserver_name* `-kerberos-renew-age` *integer_in_days* デフォルトの設定は7日です。
KDC上のソケットのタイムアウトを指定します。このタイムアウトを過ぎると、すべてのKDCが到達不能としてマークされます。	`vserver cifs security modify -vserver` *vserver_name* `-kerberos-kdc-timeout` *integer_in_seconds* デフォルト設定は3秒です。

2. Kerberosセキュリティ設定を確認します。

   `vserver cifs security show -vserver` *vserver_name*

例

次の例では、 SVM vs1 の Kerberos セキュリティ設定を「 Kerberos Clock Skew 」に 3 分、「 Kerberos Ticket Age 」に 8 時間に変更しています。

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

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

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

関連情報

"CIFSサーバのセキュリティ設定に関する情報の表示"

"サポートされるGPO"

"CIFSサーバへのグループ ポリシー オブジェクトの適用"

SMB サーバの *LMCompatibilityLevel* とも呼ばれる SMB サーバの最小セキュリティレベルを設定することで、 SMB クライアントアクセスのビジネスセキュリティ要件を満たすことができます。最小セキュリティレベルは、SMBサーバによって許可されるSMBクライアントからのセキュリティトークンの最小レベルです。

タスクの内容

- ワークグループモードのSMBサーバでは、NTLM認証のみがサポートされます。Kerberos認証はサポートされていません。
- LMCompatibilityLevelはSMBクライアント認証にのみ適用され、管理者認証には適用されません。

最低限の認証セキュリティレベルは、サポートされている4つのセキュリティレベルのいずれかに設定できます。

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

手順

1. 最小認証セキュリティレベルを設定します。 `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 認証セキュリティレベルが目的のレベルに設定されていることを確認します。 `vserver cifs security show -vserver` *`vserver_name`*

関連情報

Kerberosベースの通信用のAES暗号化の有効化と無効化

Kerberosベースの通信による最大限のセキュリティを確保するには、SMBサーバでAES-256暗号化とAES-128暗号化を有効にします。デフォルトでは、SVMでのSMBサーバの作成時にAdvanced Encryption Standard（AES）暗号化は無効になっています。AES暗

号化が提供する強固なセキュリティを活用するには、AES暗号化を有効にする必要があります。

SMBのKerberos関連の通信は、SVMでSMBサーバを作成する際や、SMBセッションのセットアップフェーズで使用されます。SMBサーバでは、Kerberos通信で次の暗号化タイプがサポートされます。

- AES 256
- AES 128
- デス
- RC4-HMAC

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

SMBサーバを作成すると、ドメインコントローラによってActive Directoryにコンピュータマシンアカウントが作成されます。この時点で、KDCは特定のマシンアカウントの暗号化機能を認識します。その後、認証時にクライアントがサーバに提示するサービスチケットを暗号化するために、特定の暗号化タイプが選択されます。

ONTAP 9 .12.1以降では、Active Directory（AD）KDCにアドバタイズする暗号化タイプを指定できます。オプションを使用すると `-advertised-enc-types`、推奨される暗号化タイプを有効にしたり、弱い暗号化タイプを無効にしたりできます。方法をご確認ください"Kerberosベースの通信の暗号化タイプを有効または無効にします"。

SMB 3.0で使用できるIntel AES New Instructions（Intel AES NI）は、AESアルゴリズムを強化し、サポートされているプロセッサファミリーでのデータ暗号化を高速化します。SMB 3.1.1以降では、SMB暗号化で使用されるハッシュアルゴリズムとしてAES-128-CCMに代わってAES-128-GCMが使用されます。

関連情報

CIFSサーバのKerberosセキュリティ設定の変更

Kerberosベースの通信用の**AES**暗号化の有効化または無効化

Kerberosベースの通信で最も強力なセキュリティを活用するには、SMBサーバでAES-256暗号化とAES-128暗号化を使用する必要があります。ONTAP 9.13.1以降では、AES暗号化がデフォルトで有効になります。SMBサーバでActive Directory（AD）KDCとのKerberosベースの通信にAES暗号化タイプを選択したくない場合は、AES暗号化を無効にすることができます。

AES暗号化がデフォルトで有効になっているかどうかと、暗号化タイプを指定できるかどうかは、ONTAPのバージョンによって異なります。

ONTAPのバージョン	**AES**暗号化が有効になっている...	暗号化タイプを指定できますか。
9.13.1以降	デフォルト	○
9.12.1	シユトウ	○
9.11.1以前	シユトウ	いいえ

ONTAP 9 .12.1以降では、AES暗号化はオプションを使用して有効または無効にでき `-advertised-enc -types`ます。このオプションを使用すると、AD KDCにアドバタイズされる暗号化タイプを指定できます。デフォルトの設定はと `des`です `rc4`が、AESタイプを指定するとAES暗号化が有効になります。オプションを使用して、弱いRC4およびDES暗号化タイプを明示的に無効にすることもできます。AES.11.1以前でONTAP 9は、オプションを使用してAES暗号化を有効または無効にする必要があります `-is-aes-encryption-enabled`。暗号化タイプを指定することはできません。

セキュリティを強化するために、Storage Virtual Machine（SVM）はAESセキュリティオプションが変更されるたびにAD内のマシンアカウントのパスワードを変更します。パスワードを変更するには、マシンアカウントを含む組織単位（OU）の管理ADクレデンシャルが必要になる場合があります。

IDが保持されないディザスタリカバリデスティネーションとしてSVMが設定されている場合（SnapMirrorの設定でオプションがに設定されている `false`場合 `-identity-preserve`）、デフォルト以外のSMBサーバセキュリティ設定はデスティネーションにレプリケートされません。ソースSVMでAES暗号化を有効にした場合は、AES暗号化を手動で有効にする必要があります。

例 **1.** 手順

ONTAP 9.12.1以降

1. 次のいずれかを実行します。

Kerberos 通信の **AES** 暗号化タイプの設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
無効にする	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

*注:*この `-is-aes-encryption-enabled`オプションはONTAP 9 12.1では廃止されており、今後のリリースで削除される可能性があります。

2. AES暗号化が必要に応じて有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

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

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信の **AES** 暗号化タイプの設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
無効にする	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. AES暗号化が必要に応じて有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

> `is-aes-encryption-enabled`フィールドには、
> AES暗号化が有効になっているかどうかと `false`無効になっているかが表示されます `true`。

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

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

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

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

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

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

関連情報

"ドメインユーザがDomain-Tunnelを使用するクラスタにログインできない"

SMB署名を使用したネットワークセキュリティの強化

SMB署名を使用したネットワークセキュリティの概要の強化

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

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

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

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

- `Microsoft network client: Digitally sign communications (if server agrees)`

  この設定は、クライアントのSMB署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定がクライアントで無効になっている場合、クライアントのCIFSサーバとの通信は、CIFSサーバのSMB署名の設定によって異なります。

- `Microsoft network client: Digitally sign communications (always)`

  この設定は、クライアントがサーバとの通信に SMB 署名を必要とするかどうかを制御します。デフォルトでは無効になっています。この設定がクライアントで無効になっている場合、SMB署名の動作は、のポリシー設定とCIFSサーバの設定に基づき `Microsoft network client: Digitally sign communications (if server agrees)`ます。

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

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

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

クライアント	**ONTAP —** 署名は不要	**ONTAP —** 署名が必要
署名は無効になっており、不要です	署名されません	署名済み
署名が有効になっており、不要である	署名されません	署名済み
署名が無効になっており、必要です	署名済み	署名済み
署名が有効になっており、必要です	署名済み	署名済み

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

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

SMB 2.x クライアントと SMB 3.0 クライアントでは、 SMB 署名は常に有効になります。無効にすることはできません。

クライアント	**ONTAP —** 署名は不要	**ONTAP —** 署名が必要
署名は不要です	署名されません	署名済み
署名が必要です	署名済み	署名済み

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

プロトコル	ハッシュアルゴリズム	有効 / 無効を切り替えられます	必須 / 不要	クライアントのデフォルト	サーバのデフォルト	**DC** のデフォルト
SMB 1.0	MD5	○	○	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	○	不要	不要	必須
SMB 3.0	AES-CMAC ：	いいえ	○	不要	不要	必須

Microsoftでは、または `Digitally sign communications (if server agrees)`グループポリシー設定の使用を推奨していません `Digitally sign communications (if client agrees)`。Microsoftでは、レジストリ設定の使用も推奨していません `EnableSecuritySignature`。これらのオプションはSMB 1の動作にのみ影響し、グループポリシー設定または `RequireSecuritySignature`レジストリ設定に置き換えることができます。`Digitally sign communications (always)`詳細については、Microsoftのブログを参照してください。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The SMB署名の基礎（SMB1とSMB2の両方をカバー）]

SMB署名のパフォーマンスへの影響

SMBセッションでSMB署名を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行しているクラスタノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワークトラフィックの量に変化はありませんが、クライアントとサーバの両方でCPU使用率が増加したことを示しています。

パフォーマンスへの影響の程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9 .7以

降では、新しい暗号化オフロードアルゴリズムによって署名済みSMBトラフィックのパフォーマンスを向上させることができます。SMB署名オフロードは、SMB署名が有効になっている場合はデフォルトで有効になります。

SMB署名のパフォーマンス向上には、AES-NIオフロード機能が必要です。お使いのプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証できます。

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

SMB署名の設定に関する推奨事項

SMBクライアントとCIFSサーバの間のSMB署名の動作は、セキュリティ要件に応じて設定できます。CIFSサーバでSMB署名を設定する際に選択する設定は、セキュリティ要件によって異なります。

SMB署名はクライアントとCIFSサーバのどちらでも設定できます。SMB署名を設定する際は、次の推奨事項を考慮してください。

状況	推奨事項
クライアントとサーバ間の通信のセキュリティを強化する	クライアントのセキュリティ設定を有効にして、クライアントでSMB署名を必須にします `Require Option (Sign always)`。
特定のStorage Virtual Machine（SVM）へのすべてのSMBトラフィックに署名する	セキュリティ設定でSMB署名を必須にするように設定して、CIFSサーバでSMB署名を必須にします。

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

複数のデータ**LIF**が設定されている場合の**SMB**署名に関するガイドライン

SMB サーバで SMB 署名要求を有効または無効にするときは、 SVM に複数のデータ LIF が設定されている場合のガイドラインに注意する必要があります。

SMB サーバを設定する際に、複数のデータ LIF が設定されていることがあります。その場合、DNSサーバにはCIFSサーバのレコードエントリが複数含まれ `A`、SMBサーバホスト名はすべて同じですが、IPアドレスはそれぞれ一意です。たとえば、2つのデータLIFが設定されているSMBサーバには、次のDNSレコードエントリがあり `A`ます。

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

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

次の例を考えてみましょう。

1. client1は、パスを使用してSMB署名を必要とせずに共有に接続します `O:\`。
2. ストレージ管理者が、 SMB 署名を要求するように SMB サーバの設定を変更したとします。
3. Client1は、パスを使用して（パスを使用した接続は維持したまま `O:\`）、SMB署名を使用して同じ共有に接続します `S:\`。
4. その結果、ドライブと `S:\`ドライブの両方でデータにアクセスするときにSMB署名が使用され `O:\`ます。

受信**SMB**トラフィックの**SMB**署名要求を有効または無効にする

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

タスクの内容

デフォルトでは、SMB署名要求は無効になっています。SMB署名要求はいつでも有効または無効にできます。

次の状況では、SMB署名はデフォルトで無効になりません。

1. SMB署名要求が有効になっており、クラスタがSMB署名をサポートしていないバージョンのONTAPにリバートされた。
2. その後、クラスタがSMB署名をサポートするバージョンのONTAPにアップグレードされた。

   この場合、サポートされているバージョンのONTAPで最初に設定されたSMB署名の設定は、リバートとその後のアップグレードを通じて保持されます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップする際にコマンドのオプション `snapmirror create`で選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

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

このオプションを（非ID保持）に `false`設定する `-identity-preserve`と、SMB署名のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションのCIFSサーバセキュリティ設定

はデフォルト値に設定されます。ソースSVMでSMB署名要求を有効にした場合は、デスティネーションSVMでSMB署名要求を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

SMB 署名要求の設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -is-signing-required true`
無効にする	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

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

例

次の例では、SVM vs1でSMB署名要求を有効にします。

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

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

暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

SMBセッションが署名されているかどうかの確認

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

手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定したStorage Virtual Machine（SVM）上の署名されたすべてのセッション	`vserver cifs session show -vserver vserver_name -is-session-signed true`
SVM上の特定のSession IDを使用する署名されたセッションの詳細	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

例

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

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

次のコマンドは、Session IDが2のSMBセッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報を表示します。

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

関連情報

SMB署名済みセッションの統計の監視

SMB署名済みセッションの統計の監視

SMBセッションの統計を監視して、確立されたセッションのうち、署名されているセッションと署名されていないセッションを確認できます。

タスクの内容

advanced権限レベルでコマンドを実行する `statistics`と、署名済みSMBセッションの数を監視するためのカウンタが提供され `signed_sessions`ます。この `signed_sessions`カウンタでは、次の統計オブジェクトを使用できます。

- `cifs`すべてのSMBセッションについてSMB署名を監視できます。
- `smb1`SMB 1.0セッションのSMB署名を監視できます。
- `smb2`SMB 2.xセッションとSMB 3.0セッションのSMB署名を監視できます。

  オブジェクトの出力にはSMB 3.0の統計が表示され `smb2`ます。

署名されたセッションの数をセッションの総数と比較する場合は、カウンタの出力とカウンタの出力 `established_sessions`を比較できます `signed_sessions`。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなけれ

ば、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を特定するのに役立ちます。

手順

1. 権限レベルをadvancedに設定します。+
`set -privilege advanced`
2. データ収集を開始します。+
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id`はテキスト文字列です。同じCLIセッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以前のデフォルトサンプルが上書きされます。

   必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。
3. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。
4. SMB署名統計を表示します。

表示する情報	入力するコマンド
署名されたセッション	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	署名されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   単一のノードの情報のみを表示する場合は、オプションのパラメータを指定します `-node`。
5. admin権限レベルに戻ります。+
`set -privilege admin`

例

次の例は、vs1というStorage Virtual Machine（SVM）について、SMB 2.xとSMB 3.0の署名統計を監視する方法を示しています。

次のコマンドは、advanced権限レベルに移行します。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

次のコマンドは、ノードごとに署名されたSMBセッションと確立されたSMBセッションをサンプルから表示します。

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

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

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

次のコマンドは、node2の署名済みSMBセッションをサンプルから表示します。

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

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

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

次のコマンドは、admin権限レベルに戻ります。

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

関連情報

SMBセッションが署名されているかどうかの確認

"パフォーマンスの監視と管理の概要"

SMBを介したデータ転送での**SMB**サーバでの**SMB**暗号化要求の設定

SMBアンコウカノカイヨウ

SMBを介したデータ転送でのSMB暗号化は、SMBサーバで有効または無効にできるセキュリティ強化です。共有プロパティ設定を使用して、共有ごとに必要なSMB暗号化を設定することもできます。

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

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

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

- SMBサーバのセキュリティ オプション：SVMでこの機能を有効にする
- SMB共有プロパティ：共有ごとにSMB暗号化を設定する

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

実際に適用されるSMB暗号化設定は、この2つの設定の組み合わせによって決まります。次の表を参照してください。

SMB サーバ **SMB** 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しい	正しくない	SVMのすべての共有でサーバレベルの暗号化が有効になっています。この設定では、SMBセッション全体で暗号化が行われます。
正しい	正しい	共有レベルの暗号化に関係なく、SVMのすべての共有でサーバレベルの暗号化が有効になります。この設定では、SMBセッション全体で暗号化が行われます。
正しくない	正しい	特定の共有で共有レベルの暗号化が有効になっている。この設定では、ツリー接続から暗号化が行われます。

SMB サーバ SMB 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しくない	正しくない	暗号化は有効になっていません。

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

暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

SMB暗号化のパフォーマンスへの影響

SMBセッションでSMB暗号化を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行しているクラスタノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワークトラフィックの量に変化はありませんが、クライアントとサーバの両方でCPU使用率が増加したことを示しています。

パフォーマンスへの影響の程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9 .7以降では、新しい暗号化オフロードアルゴリズムにより、暗号化されたSMBトラフィックのパフォーマンスを向上させることができます。SMB暗号化オフロードは、SMB暗号化が有効になっている場合はデフォルトで有効になります。

SMB暗号化のパフォーマンスを強化するには、AES-NIオフロード機能が必要です。お使いのプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB暗号化のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証できます。

SMB暗号化は、SMBサーバではデフォルトで無効になっています。SMB暗号化は、暗号化を必要とするSMB共有またはSMBサーバでのみ有効にしてください。SMB暗号化では、ONTAPは要求を復号化し、要求ごとに応答を暗号化する追加の処理を実行します。そのため、SMB暗号化は必要な場合にのみ有効にしてください。

受信**SMB**トラフィックの**SMB**暗号化要求の有効化または無効化

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

タスクの内容

CIFS サーバ上で SMB 暗号化を有効にすることができます。この場合、 CIFS サーバ上のすべての共有が環境によって暗号化されます。CIFS サーバ上のすべての共有で SMB 暗号化要求を有効にしない場合、または受信 SMB トラフィックの SMB 暗号化要求を共有ごとに有効にする場合は、 CIFS サーバ上で SMB 暗号化要求を無効にすることができます。

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

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

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

手順

1. 次のいずれかを実行します。

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

2. CIFSサーバでのSMB暗号化要求が必要に応じて有効または無効になっていることを確認します。`vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

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

例

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

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

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

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

タスクの内容

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

- `unencrypted`

  SMB セッションは暗号化されません。Storage Virtual Machine（SVM）レベルの暗号化も共有レベルの暗号化も設定されません。

- `partially-encrypted`

  ツリー接続が行われると、暗号化が開始されます。共有レベルの暗号化が設定されています。SVM レベルの暗号化は有効になりません。

- `encrypted`

  SMB セッションは完全に暗号化されます。SVM レベルの暗号化が有効です。共有レベルの暗号化は、有効になる場合とならない場合があります。SVM レベルの暗号化設定は、共有レベルの暗号化設定よりも優先されます。

手順

1. 次のいずれかを実行します。

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

例

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

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

SMB暗号化統計の監視

SMB暗号化の統計を監視して、確立されたセッションと共有接続のうち、暗号化されているものと暗号化されていないものを確認できます。

タスクの内容

advanced権限レベルでコマンドを実行する `statistics`と次のカウンタが表示され、暗号化されたSMBセッションおよび共有接続の数を監視できます。

カウンタ名	説明
encrypted_sessions	暗号化されたSMB 3.0セッションの数
encrypted_share_connections	ツリー接続が行われた暗号化された共有の数を示します。
rejected_unencrypted_sessions	クライアントの暗号化機能がないために拒否されたセッションセットアップの数
rejected_unencrypted_shares	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

- `cifs`すべてのSMB 3.0セッションについてSMB暗号化を監視できます。

  オブジェクトの出力にはSMB 3.0の統計が表示され `cifs`ます。暗号化されたセッション数をセッションの合計数と比較する場合は、カウンタの出力とカウンタの出力 `established_sessions`を比較できます `encrypted_sessions`。

  暗号化された共有接続の数を共有接続の総数と比較するには、カウンタの出力とカウンタの出力 `connected_shares`を比較します `encrypted_share_connections`。

- `rejected_unencrypted_sessions`SMB暗号化をサポートしていないクライアントから暗号化を必要とするSMBセッションの確立が試行された回数を示します。
- `rejected_unencrypted_shares`SMB暗号化をサポートしていないクライアントから暗号化が必要なSMB共有への接続が試行された回数を示します。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を特定するのに役立ちます。

手順

1. 権限レベルをadvancedに設定します。+
   `set -privilege advanced`
2. データ収集を開始します。+
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id`はテキスト文字列です。同じCLIセッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以前のデフォルトサンプルが上書きされます。

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

3. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。
4. SMB暗号化統計を表示します。

表示する情報	入力するコマンド
暗号化されたセッション	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	暗号化されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	暗号化された共有接続

表示する情報	入力するコマンド
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
暗号化された共有接続と接続された共有	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒否された非暗号化セッション	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒否された非暗号化共有接続
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

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

5. admin権限レベルに戻ります。+
`set -privilege admin`

例

次の例は、「vs1」というStorage Virtual Machine（SVM）について、SMB 3.0暗号化統計情報を監視する方法を示しています。

次のコマンドは、advanced権限レベルに移行します。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

次のコマンドは、指定したノードについて、暗号化されたSMBセッションと確立されたSMBセッションをサンプルから表示します。

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

次のコマンドは、指定したノードについて、拒否された暗号化されていないSMBセッション数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

次のコマンドは、指定したノードについて、接続されているSMB共有と暗号化されたSMB共有の数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

次のコマンドは、指定したノードについて、拒否された暗号化されていないSMB共有接続の数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

関連情報

使用可能な統計オブジェクトと統計カウンタの確認

"パフォーマンスの監視と管理の概要"

セキュアな**LDAP**セッション通信

LDAPの署名と封印の概念

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへのクエリに

対してLDAPセッションセキュリティを有効にすることができます。Storage Virtual Machine（SVM）のCIFSサーバセキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、シークレットキーテクノロジを使用してLDAPペイロードデータの整合性を確認します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。LDAPトラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトはです `none`。

CIFSトラフィックに対するLDAPの署名と封印は、コマンドのオプションを `vserver cifs security modify`使用して`SVM`で有効にします `-session-security-for-ad-ldap`。

CIFSサーバで**LDAP**の署名と封印を有効にする

CIFS サーバで Active Directory LDAP サーバとのセキュアな通信に署名と封印を使用するためには、 CIFS サーバのセキュリティ設定を変更して LDAP の署名と封印を有効にする必要があります。

開始する前に

AD サーバ管理者に問い合わせて、適切なセキュリティ設定値を決定する必要があります。

手順

1. Active Directory LDAPサーバとのトラフィックの署名と封印を有効にするCIFSサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   署名(`sign`、データ整合性）、署名と封印(`seal`、データの整合性と暗号化を有効にすることができます。また、 `none`署名と封印のどちらも有効にしないことも可能です。デフォルト値はです `none`。

2. LDAPの署名と封印のセキュリティ設定が正しく設定されていることを確認します。 `vserver cifs security show -vserver` *`vserver_name`*

> SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、コマンドのオプション `vserver services name-service ldap client modify`で対応する設定を有効にする必要があります。 `-session-security`

LDAP over TLSの設定

自己署名ルート**CA**証明書のコピーをエクスポートする

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

開始する前に

CIFSサーバが属しているドメイン用にActive Directory証明書サービスがインストールされ、設定されている必要があります。Active Director証明書サービスのインストールと設定については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNetライブラリ：technet.microsoft.com"

ステップ

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

   "Microsoft TechNetライブラリ：technet.microsoft.com"

終了後

SVMに証明書をインストールします。

関連情報

"Microsoft TechNetライブラリ"

自己署名ルート**CA**証明書を**SVM**にインストールする

LDAPサーバへのバインド時にTLSを使用したLDAP認証が必要な場合は、最初に自己署名ルートCA証明書をSVMにインストールする必要があります。

タスクの内容

LDAP over TLSが有効な場合、SVM上のONTAP LDAPクライアントでは、ONTAP 9 .0および9.1の破棄された証明書はサポートされません。

ONTAP 9 .2以降では、TLS通信を使用するONTAP内のすべてのアプリケーションで、オンライン証明書ステータスプロトコル（OCSP）を使用してデジタル証明書ステータスを確認できます。OCSPがLDAP over TLSに対して有効になっている場合、失効した証明書は拒否され、接続は失敗します。

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. 証明書ファイルをテキストエディタで開き `.pem`、で始まる行とで終わる `-----END CERTIFICATE-----`行を含めて証明書をコピーし `-----BEGIN CERTIFICATE-----`、コマンドプロンプトのあとに証明書を貼り付けます。
   c. 証明書が正しく表示され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たことを確認します。 `security certificate show -vserver vserver_name`

サーバで **LDAP over TLS** を有効にします

SMBサーバでActive Directory LDAPサーバとのセキュアな通信にTLSを使用するには、SMBサーバのセキュリティ設定を変更してLDAP over TLSを有効にする必要があります。

10.1以降では、**ONTAP 9**チャネルバインドが**Active Directory**（**AD**）接続とネームサービス**LDAP**接続の両方でデフォルトでサポートされます。**ONTAP**は、**Start-TLS**または**LDAPS**が有効で、セッションセキュリティが署名または封印のいずれかに設定されている場合にのみ、**LDAP**接続でチャネルバインディングを試行します。**AD**サーバとの**LDAP**チャネルバインディングを無効または再度有効にするには、コマンドでパラメータを `**vserver cifs security modify**`使用し `**-try-channel-binding-for-ad-ldap**`ます。

詳細については、以下を参照してください。

- "LDAPの概要"
- "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"です。

手順

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

> SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、コマンドを使用してオプションを `vserver services name-service ldap client modify`変更する必要もあります。 `-use-start-tls`

パフォーマンスと冗長性を確保するための**SMB**マルチチャネルの設定

ONTAP 9 .4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。

開始する前に

SMBマルチチャネル機能は、クライアントがSMB 3.0以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMBサーバではSMB 3.0以降がデフォルトで有効になっています。

タスクの内容

SMBクライアントは、ONTAPクラスタで適切な設定が見つかると、複数のネットワーク接続を自動的に検出して使用します。

SMBセッションでの同時接続数は、導入しているNICによって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

  クライアントはNICごとに1つの接続を確立し、すべての接続にセッションをバインドします。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

  クライアントはNICごとに最大4つの接続を確立し、すべての接続にセッションをバインドします。クライアントは、10G以上の容量の複数のNICで接続を確立できます。

また、次のパラメータを変更することもできます（advanced権限）。

- `-max-connections-per-session`

  マルチチャネルセッションごとに許可される最大接続数。デフォルトの接続数は32です。

  デフォルトよりも多くの接続を有効にする場合は、クライアント設定を調整する必要があります（デフォルトの接続数は32）。

- `-max-lifs-per-session`

  マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。デフォルトは256のネットワークインターフェイスです。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAPがSMBマルチチャネルセッションを報告していることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、すべてのSMBセッションに関する情報を表示します。1つのセッションに対する複数の接続が表示されています。

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

次の例は、セッションID 1のSMBセッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

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

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

タスクの内容

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

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

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

手順

1. デフォルトのUNIXユーザを設定します。

状況	入力するコマンド
デフォルトの UNIX ユーザ「 pcuser 」を使用する	`vserver cifs options modify -default -unix-user pcuser`
別の UNIX ユーザアカウントをデフォルトユーザとして使用します	`vserver cifs options modify -default -unix-user user_name`
デフォルトのUNIXユーザを無効にする	`vserver cifs options modify -default -unix-user ""`

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

2. デフォルトのUNIXユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

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

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

```
Vserver: vs1

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

ゲスト**UNIX**ユーザの設定

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

タスクの内容

ゲスト UNIX アカウントを設定する場合は、次の点に注意する必要があります。

- ホームドメイン、信頼できるドメイン、またはローカルデータベースのドメインコントローラに対してCIFSサーバがユーザを認証できない場合、このオプションが有効になっていると、CIFSサーバはそのユーザをゲストユーザとみなして、指定したUNIXユーザにユーザをマッピングします。
- このオプションを null 文字列に設定すると、ゲスト UNIX ユーザは無効になります。
- いずれかのStorage Virtual Machine（SVM）ネームサービスデータベースで、ゲストUNIXユーザとして使用するUNIXユーザを作成する必要があります。
- ゲストユーザとしてログインしたユーザは、自動的に CIFS サーバの BUILTIN\guests グループのメンバーになります。
- 「 homedirs-public 」オプションは、認証されたユーザにのみ適用されます。ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。

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
ゲストUNIXユーザの設定	`vserver cifs options modify -guest -unix-user` *`unix_name`*
ゲスト UNIX ユーザを無効にします	`vserver cifs options modify -guest -unix-user ""`

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

2. ゲストUNIXユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

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

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

   ```
   Vserver: vs1

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

ルートへの**Administrators**グループのマッピング

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

タスクの内容

ただし、ストレージシステムがNTFS専用としてセットアップされている場合は `/etc`、ディレクトリにファイルレベルのACLがあり、Administratorsグループはこのを使用してONTAP構成ファイルにアクセスできます。

手順

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

状況	そしたら...。
管理者グループメンバーをルートにマッピングします	`vserver cifs options modify -vserver *vserver_name* -is-admin-users-mapped-to-root-enabled true`アカウントをrootにマッピングするエントリがない場合でも、Administratorsグループ内のすべてのアカウントはrootとみなされ `/etc/usermap.cfg`ます。Administrators グループに属するアカウントを使用してファイルを作成する場合、 UNIX クライアントからファイルを表示するときに、ファイルはルートによって所有されます。
Administrators グループメンバーのルートへのマッピングを無効にします	`vserver cifs options modify -vserver *vserver_name* -is-admin-users-mapped-to-root-enabled false`Administratorsグループ内のアカウントがrootにマッピングされなくなります。ルートへのマッピングは、単一のユーザに対して明示的にのみ実行できます。

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

SMBセッションを介して接続しているユーザのタイプに関する情報を表示する

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

タスクの内容

SMBセッションを介して接続できるユーザのタイプは次のとおりです。

- `local-user`

  ローカル CIFS ユーザとして認証されている

- `domain-user`

  ドメインユーザとして（ CIFS サーバのホームドメインまたは信頼できるドメインから）認証されている

- `guest-user`

  ゲストユーザとして認証されています

- `anonymous-user`

  匿名ユーザまたは null ユーザとして認証されています

手順

1. SMBセッションを介して接続しているユーザのタイプを確認します。 `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

確立されたセッションのユーザタイプ情報を表示する対象	入力するコマンド
指定したユーザタイプのすべてのセッション	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	特定のユーザの場合

例

次のコマンドを実行すると、ユーザ「 iepubs\user1 」によって確立された SVM vs1 上のセッションのユーザタイプに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Windowsクライアントの過剰なリソース消費を制限するコマンドオプション

コマンドのオプションを `vserver cifs options modify`使用すると、Windowsクライアントのリソース消費を制御できます。これは、ファイルオープン、セッションオープン、Change Notify要求が異常に多い場合など、通常の範囲を超えてリソースを消費するクライアントがある場合に役立ちます。

Windowsクライアントのリソース消費を制御するために、コマンドに次のオプション `vserver cifs options modify`が追加されました。いずれかのオプションの最大値を超えると、要求は拒否され、EMSメッセージが送信されます。これらのオプションに設定されている制限の80%に達したときにも、EMS警告メッセージが送信されます。

- `-max-opens-same-file-per-tree`

  CIFSツリーあたりの同一ファイルに対する最大オープン数

- `-max-same-user-sessions-per-connection`

  接続ごとに同じユーザが開いたセッションの最大数

- `-max-same-tree-connect-per-session`

  同じ共有に対するセッションあたりの最大ツリー接続数

- `-max-watches-set-per-tree`

  ツリーごとに確立されるウォッチの最大数（別名 *change notifier*）

デフォルトの制限と現在の設定を表示するには、マニュアルページを参照してください。

ONTAP 9.4 以降では、 SMB バージョン 2 以降を実行しているサーバで、クライアントからサーバに SMB 接続で送信できる未処理要求（ _SMB クレジット _ ）の数を制限することができます。SMBクレジットの管理はクライアントによって開始され、サーバによって制御されます。

SMB接続で許可できる未処理要求の最大数は、オプションで制御され `-max-credits`ます。このオプションのデフォルト値は128です。

従来の**oplock**および**oplock**リースでクライアントパフォーマンスを向上

従来の**oplock**および**oplock**リースでクライアントパフォーマンスを向上させる方法の概要

便宜的 oplock と oplock リースでは、先読み、あと書き、ロックの各情報を SMB クライアント側でキャッシングできるよう、特定のファイル共有シナリオでそのクライアントを有効にします。クライアントは、対象のファイルへのアクセスが必要であることをサーバに定期的に通知することなく、ファイルの読み取りや書き込みを行うことができます。これにより、ネットワークトラフィックが軽減され、パフォーマンスが向上します。

oplockリースはoplockを強化したもので、SMB 2.1以降のプロトコルで使用できます。oplockリースを使用すると、クライアントが自身を起点とする複数のSMBオープンでクライアントのキャッシュ状態を取得して保持できます。

oplock は次の 2 つの方法で制御できます。

- 共有プロパティ。共有の作成時にコマンドを使用するか、 `vserver share properties`作成後にコマンドを使用し `vserver cifs share create`ます。
- qtreeプロパティ。qtreeの作成時にコマンドを使用するか、 `volume qtree oplock`作成後にコマンドを使用し `volume qtree create`ます。

oplockを使用する場合の書き込みキャッシュデータ損失に関する考慮事項

状況によっては、あるプロセスがファイルに対して排他的なoplockを持っていて、別のプロセスがそのファイルを開こうとすると、最初のプロセスがキャッシュされたデータを無効にし、書き込みとロックをフラッシュしなければならないことがあります。その後、クライアントはoplockを放棄してファイルにアクセスする必要があります。このフラッシュ中にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われる可能性があります。

- データ損失の可能性

データの書き込みがキャッシュされるアプリケーションでは、次の場合にそのデータを失う可能性があります。

- 接続は SMB 1.0 を使用して確立されます。
- ファイルに対して排他的な oplock を使用している場合
- oplock を解除するか、ファイルを閉じるように指示された場合
- 書き込みキャッシュをフラッシュするプロセスで、ネットワークまたはターゲットシステムにエラーが発生した場合

- エラー処理および書き込みの完了

  キャッシュ自体にエラー処理機能はなく、アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行う場合、書き込みは必ず完了します。キャッシュがネットワークを介してターゲットシステムに書き込みを行う場合、書き込みが完了していないとデータが失われるため、書き込みが完了したと想定する必要があります。

SMB共有の作成時にoplockを有効または無効にする

oplockを使用すると、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるため、ファイル操作のパフォーマンスが向上します。Storage Virtual Machine（SVM）上にあるSMB共有ではoplockが有効になります。場合によっては、oplockの無効化が必要になることがあります。oplockは共有ごとに有効または無効にできます。

タスクの内容

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームのoplock設定よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。

oplock共有プロパティに加えて、他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する操作を実行します。

状況	そしたら...。
共有の作成時に共有でoplockを有効にする	次のコマンドを入力します。 `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` 共有でデフォルトの共有プロパティ（、、、 `changenotify`）のみを有効にする場合 `oplocks`は、 `browsable`SMB共有の作成時にパラメータを指定する必要はありません `-share-properties`。デフォルト以外の共有プロパティを組み合わせて使用する場合は、パラメータとその共有に使用する共有プロパティのリストを指定する必要があります `-share-properties`。
共有の作成時に共有でoplockを無効にする	次のコマンドを入力します。 `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` oplockを無効にする場合は、共有の作成時に共有プロパティのリストを指定する必要がありますが、プロパティは指定しないで `oplocks`ください。

関連情報

既存のSMB共有でのoplockの有効化と無効化

oplockステータスの監視

ボリュームおよび**qtree**で**oplock**を有効または無効にするコマンド

oplockを使用すると、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるため、ファイル操作のパフォーマンスが向上します。ここでは、ボリュームまたはqtreeでoplockを有効または無効にするコマンドについて説明します。また、ボリュームおよびqtreeでoplockを有効または無効にできるタイミングについても把握しておく必要があります。

- ボリュームでは、oplockがデフォルトで有効になっています。
- ボリュームの作成時にoplockを無効にすることはできません。

- 既存のSVMのボリュームでは、oplockをいつでも有効または無効にできます。
- SVMのqtreeではoplockを有効にできます。

  oplockモードの設定は、すべてのボリュームに含まれるデフォルトのqtreeであるqtree ID 0のプロパティです。qtreeの作成時にoplock設定を指定しない場合、qtreeは親ボリュームのoplock設定（デフォルトで有効）を継承します。ただし、新しいqtreeでoplock設定を指定した場合は、ボリュームのoplock設定よりも優先されます。

状況	使用するコマンド
ボリュームまたはqtreeでoplockを有効にする	`volume qtree oplocks`パラメータがに設定されている `enable`場合 `-oplock-mode`
ボリュームまたはqtreeでoplockを無効にする	`volume qtree oplocks`パラメータがに設定されている `disable`場合 `-oplock-mode`

関連情報

oplockステータスの監視

既存の**SMB**共有での**oplock**の有効化または無効化

Storage Virtual Machine（SVM）上のSMB共有では、oplockがデフォルトで有効になっています。状況によっては、oplockの無効化が必要になることがあります。また、以前に共有でoplockを無効にしたことがある場合は、oplockを再度有効にすることもできます。

タスクの内容

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームでのoplockの有効化よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。既存の共有では、oplockをいつでも有効または無効にできます。

ステップ

1. 該当する操作を実行します。

状況	そしたら...。
既存の共有を変更して共有でoplockを有効にする	次のコマンドを入力します。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` 追加する共有プロパティをカンマで区切って追加指定できます。 新しく追加したプロパティは、既存の共有プロパティのリストに追加されます。以前に指定した共有プロパティは有効なままです。
既存の共有を変更して共有でoplockを無効にする	次のコマンドを入力します。 `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` 削除する共有プロパティをカンマで区切って追加指定できます。 削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しない設定済みの共有プロパティは有効なままです。

例

次のコマンドは、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 Engineering 」という名前の共有の oplock を有効にします。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

次のコマンドは、 SVM vs1 上の「 Engineering 」という名前の共有の oplock を無効にします。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

関連情報

SMBキヨウユウノサクセイシノoplockノユウコウカトムコウカ

oplockステータスの監視

既存のSMB共有に対する共有プロパティの追加または削除

oplockステータスを監視する

oplockステータスに関する情報を監視および表示できます。この情報を使用して、oplockが設定されているファイル、oplockレベルとoplock状態レベル、およびoplockリースが使用されているかどうかを確認できます。また、手動での解除が必要になる可能性があるロックに関する情報を確認することもできます。

タスクの内容

すべてのoplockに関する情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、指定したクライアントIPアドレスまたは指定したパスを持つロックのみを出力に返すように指定できます。

従来のoplockおよびoplockリースについて、次の情報を表示できます。

- oplockが有効なSVM、ノード、ボリューム、LIF
- ロックUUID
- oplockが有効なクライアントのIPアドレス
- oplockが有効なパス
- ロックのプロトコル（SMB）とタイプ（oplock）
- ロックの状態
- oplockレベル
- 接続状態とSMBの有効期限
- oplockリースが許可されている場合のOpen Group ID

各パラメータの詳細については、のマニュアルページを参照して `vserver oplocks show`ください。

手順

1. コマンドを使用して、oplockステータスを表示します `vserver locks show`。

例

次のコマンドは、すべてのロックに関するデフォルトの情報を表示します。表示されたファイルのoplockにはoplockレベルが設定されてい `read-batch`ます。

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

次の例は、パスのファイルに対するロックに関する詳細情報を表示します `/data2/data2_2/intro.pptx`。このファイルでは、IPアドレスがのクライアントに対してoplockレベルで `10.3.1.3`oplockリースが許可されてい `batch`ます。

詳細情報を表示する場合は、oplockと共有ロックの情報を個別に出力します。この例は、oplockセクションの出力のみを示しています。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

関連情報

SMBキヨウユウノサクセイシノoplockノユウコウカトムコウカ

既存のSMB共有でのoplockの有効化と無効化

ボリュームおよびqtreeでoplockを有効または無効にするコマンド

SMBサーバへのグループポリシーオブジェクトの適用

SMBサーバへのグループポリシーオブジェクトの適用の概要

SMBサーバは、グループポリシーオブジェクト（GPO）をサポートしています。GPOは、Active Directory環境のコンピュータに適用される_グループポリシー属性_と呼ばれる一連のルールです。GPOを使用して、同じActive Directoryドメインに属するクラスタ上のすべてのStorage Virtual Machine（SVM）の設定を一元管理できます。

SMBサーバでGPOが有効になっている場合、ONTAPはActive DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。SMBサーバに適用可能なGPO定義がある場合、Active Directoryサーバは次のGPO情報を

返します。

- GPO名
- 現在のGPOバージョン
- GPO定義の場所
- GPOポリシーセットのUUID（Universally Unique Identifier）のリスト

関連情報

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

"SMBおよびNFSの監査とセキュリティトレース"

サポートされる**GPO**

すべてのグループポリシーオブジェクト（GPO）をCIFS対応のStorage Virtual Machine（SVM）に適用できるわけではありませんが、SVMでは関連するGPOを認識して処理することができます。

SVMで現在サポートされているGPOは次のとおりです。

- 監査ポリシーの詳細設定：

  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

  次の設定を含む、集約型アクセスポリシー（CAP）のステージングで監査対象となるイベントのタイプを指定します。

  - 監査しないでください
  - 成功イベントのみ監査
  - 失敗イベントのみ監査
  - 成功イベントと失敗イベントの両方を監査します

  > 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

  GPOの設定 `Advanced Audit Policy Configuration/Audit Policies/Object Access`を使用して設定します `Audit Central Access Policy Staging`。

  > 高度な監査ポリシー構成GPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- レジストリ設定：

  - CIFS 対応の SVM のグループポリシーの更新間隔

    GPOを使用して設定し`Registry`ます。

- グループポリシーの更新間隔のランダムオフセット

  GPOを使用して設定し `Registry`ます。

- BranchCache のハッシュの発行

  BranchCacheのハッシュの発行GPOは、BranchCacheの動作モードに対応しています。次の3つの動作モードがサポートされています。

  - 共有ごと
  - all-shares
  - Disabled GPOを使用して設定します `Registry`。

- BranchCache のハッシュバージョンサポート

  次の3つのハッシュバージョン設定がサポートされています。

  - BranchCache バージョン 1.7
  - BranchCache バージョン 1.7
  - BranchCacheバージョン1および2 GPOを使用して設定されます `Registry`。

> BranchCache GPO設定を使用するには、その設定を適用するCIFS対応のSVMでBranchCacheを構成する必要があります。SVMでBranchCacheが構成されていない場合、GPO設定は適用されず、破棄されます。

- セキュリティ設定

  - 監査ポリシーとイベントログ

    - ログオンイベントを監査します

      次の設定を含む監査対象のログオンイベントのタイプを指定します。

      - 監査しないでください
      - 成功イベントのみ監査
      - 障害イベントの監査
      - GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit logon events`。

      > 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

    - オブジェクトへのアクセスを監査する

      次の設定を含む、監査対象のオブジェクトアクセスのタイプを指定します。

      - 監査しないでください
      - 成功イベントのみ監査

- 障害イベントの監査
- GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit object access`。

> 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- ログの保持方法

  次の設定を含む監査ログの保持方法を指定します。

  - ログファイルのサイズが最大ログサイズを超えたら、イベントログを上書きします
  - GPOの設定を `Event Log`使用して設定されたイベントログを上書きしないでください（ログを手動でクリア） `Retention method for security log`。
- 最大ログサイズ

  監査ログの最大サイズを指定します。

  GPOの設定 `Event Log`を使用して設定します `Maximum security log size`。

> 監査ポリシーとイベントログGPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

◦ ファイルシステムのセキュリティ

GPOを介してファイルセキュリティが適用されるファイルまたはディレクトリのリストを指定します。

GPOを使用して設定し `File System`ます。

> SVM内にファイルシステムセキュリティGPOを設定するボリュームパスが存在している必要があります。

◦ Kerberos ポリシー

- 最大クロックスキュー

  コンピュータクロック同期の最大許容値を分単位で指定します。

  GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum tolerance for computer clock synchronization`。

- チケットの有効期間

  ユーザチケットの最大有効期間を時間単位で指定します。

  GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum lifetime for user ticket`。

- チケットの更新の有効期間

  ユーザチケット更新の最大有効期間を日数で指定します。

GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum lifetime for user ticket renewal`。

◦ ユーザ権限の割り当て（権限）

- 所有権の取得

  セキュリティ保護可能なオブジェクトの所有権を取得する権限を持つユーザおよびグループのリストを指定します。

  GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Take ownership of files or other objects`。

- セキュリティ権限

  ファイル、フォルダ、Active Directoryオブジェクトなど、個 々 のリソースのオブジェクトアクセスの監査オプションを指定できるユーザとグループのリストを指定します。

  GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Manage auditing and security log`。

- 通知権限の変更（トラバースチェックのバイパス）

  ユーザとグループにトラバースするディレクトリに対する権限がない場合でも、ディレクトリツリーをトラバースできるユーザとグループのリストを指定します。

ユーザがファイルおよびディレクトリの変更通知を受信するには、同じ権限が必要です。GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Bypass traverse checking`。

◦ レジストリ値

- 署名要求設定

  SMB署名要求が有効になっているか無効になっているかを示します。

GPOの設定 `Security Options`を使用して設定します `Microsoft network server: Digitally sign communications (always)`。

◦ restrict anonymous （匿名の制限

匿名ユーザに対する制限を指定します。次の3つのGPO設定が含まれます。

- Security Account Manager （ SAM ）アカウントを列挙しない：

  このセキュリティ設定は、コンピュータへの匿名接続に対して許可される追加の権限を決定します。このオプションが有効になっている場合は、ONTAPでと表示され`no-enumeration`ます。

GPOの設定 `Local Policies/Security Options`を使用して設定します `Network access: Do not allow anonymous enumeration of SAM accounts`。

- SAM アカウントと共有は列挙しません

  このセキュリティ設定では、SAMアカウントと共有の匿名列挙を許可するかどうかを指定します。このオプションが有効になっている場合は、ONTAPでと表示され`no-enumeration`ます。

  GPOの設定 `Local Policies/Security Options`を使用して設定します `Network access: Do not allow anonymous enumeration of SAM accounts and shares`。

- 共有と名前付きパイプへの匿名アクセスを制限します

  共有とパイプへの匿名アクセスを制限します。このオプションが有効になっている場合は、ONTAPでと表示され`no-access`ます。

  GPOの設定 `Local Policies/Security Options`を使用して設定します `Network access: Restrict anonymous access to Named Pipes and Shares`。

  定義済みおよび適用済みのグループポリシーに関する情報を表示する場合、出力フィールドには、3つのrestrict anonymous GPO設定による制限に関する情報が表示 `Resultant restriction for anonymous user`されます。考えられる制限は次のとおりです。

◦ `no-access`

匿名ユーザは、指定された共有と名前付きパイプへのアクセスを拒否され、SAMアカウントと共有を列挙できません。この制限は、GPOが有効になっている場合に発生し `Network access: Restrict anonymous access to Named Pipes and Shares`ます。

◦ `no-enumeration`

匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAMアカウントと共有を列挙することはできません。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- `Network access: Do not allow anonymous enumeration of SAM accounts`または `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPOが有効になっている。

◦ `no-restriction`

匿名ユーザにはフルアクセスが付与され、列挙を使用できます。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- GPOと `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPOの両方 `Network access: Do not allow anonymous enumeration of SAM accounts`が無効になっている。
  - 制限されたグループ

    制限されたグループを設定して、組み込みグループまたはユーザ定義グループのメンバーシッ

プを一元管理できます。グループポリシーを使用して制限されたグループを適用すると、CIFSサーバローカルグループのメンバーシップは、適用されたグループポリシーで定義されているメンバーシップリストの設定に一致するように自動的に設定されます。

GPOを使用して設定し `Restricted Groups`ます。

- 集約型アクセスポリシーの設定

  集約型アクセスポリシーのリストを指定します。集約型アクセスポリシーと関連付けられた集約型アクセスポリシールールによって、SVM上の複数のファイルに対するアクセス権限が決定されます。

関連情報

CIFSサーバでのGPOサポートの有効化と無効化

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

"SMBおよびNFSの監査とセキュリティトレース"

CIFSサーバのKerberosセキュリティ設定の変更

BranchCacheを使用したブランチオフィスでのSMB共有のコンテンツのキャッシュ

SMB署名を使用したネットワークセキュリティの強化

トラバースチェックのバイパスの設定

匿名ユーザに対するアクセス制限の設定

SMBサーバでGPOを使用するための要件

SMBサーバでグループポリシーオブジェクト（GPO）を使用するには、システムがいくつかの要件を満たしている必要があります。

- クラスタでSMBのライセンスが有効になっている必要があります。SMBライセンスはに含まれて い"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- SMBサーバが設定され、Windows Active Directoryドメインに追加されている必要があります。
- SMBサーバ管理ステータスがオンである必要があります。
- GPOが設定され、SMBサーバ コンピュータ オブジェクトを含むWindows Active Directoryの組織単位（OU）に適用されている必要があります。
- SMBサーバでGPOのサポートが有効になっている必要があります。

CIFSサーバ上でのGPOサポートの有効化と無効化

CIFSサーバでGroup Policy Object（GPO；グループポリシーオブジェクト）のサポートを有効または無効にすることができます。CIFSサーバでGPOのサポートを有効にすると、グループポリシー（CIFSサーバコンピュータオブジェクトを含む組織単位（OU）に適用されるポリシー）で定義されている該当するGPOがCIFSサーバに適用されます。

タスクの内容

GPOは、ワークグループモードのCIFSサーバでは有効にできません。

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
GPOを有効にする	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOを無効にする	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. GPOサポートが目的の状態になっていることを確認します。 `vserver cifs group-policy show -vserver +vserver_name_`

   ワークグループモードの CIFS サーバのグループポリシーステータスは「 disabled 」と表示されます。

例

次の例では、Storage Virtual Machine（SVM）vs1でGPOサポートを有効にします。

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

関連情報

サポートされるGPO

CIFSサーバでGPOを使用するための要件

CIFSサーバでのGPOの更新方法

CIFSサーバでのGPO設定の手動更新

GPO設定に関する情報の表示

SMBサアハテノ**GPO**ノコウシンホウホウ

CIFSサアハテノ**GPO**ノコウシンノカイヨウ

デフォルトでは、ONTAPはグループポリシーオブジェクト（GPO）の変更を90分ごとに取得して適用します。セキュリティ設定は16時間ごとに更新されます。ONTAPで自動

的に更新される前にGPOを更新して新しいGPOポリシー設定を適用する場合は、ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーできます。

- デフォルトでは、すべてのGPOが90分ごとに検証され、必要に応じて更新されます。

  この間隔は設定可能で、および `Random offset`GPO設定を使用して設定できます `Refresh interval`。

  ONTAPは、GPOの変更がないかどうかをActive Directoryに照会します。Active Directoryに記録されているGPOのバージョン番号がCIFSサーバ上のGPOのバージョン番号より大きい場合、ONTAPは新しいGPOを取得して適用します。バージョン番号が同じ場合、CIFSサーバ上のGPOは更新されません。

- セキュリティ設定のGPOは16時間ごとに更新されます。

  ONTAPは、変更の有無にかかわらず、16時間ごとにセキュリティ設定のGPOを取得して適用します。

  デフォルト値の16時間は、現在のONTAPバージョンでは変更できません。これはWindowsクライアントのデフォルト設定です。

- ONTAPコマンドを使用して、すべてのGPOを手動で更新できます。

  このコマンドは、Windowsの/force'コマンドをシミュレートし `gpupdate.exe``ます。

関連情報

CIFSサーバでのGPO設定の手動更新

CIFSサーバでの**GPO**設定の手動更新

CIFSサーバのGroup Policy Object（GPO；グループポリシーオブジェクト）設定をすぐに更新する場合は、設定を手動で更新できます。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

ステップ

1. 適切な操作を実行します。

更新する項目	入力するコマンド
GPO設定が変更されました	`vserver cifs group-policy update -vserver vserver_name`
すべてのGPO設定	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

関連情報

CIFSサーバでのGPOの更新方法

Active Directoryで定義されているグループポリシーオブジェクト（GPO）設定、およびCIFSサーバに適用されているGPO設定に関する情報を表示できます。

タスクの内容

CIFSサーバが属しているドメインのActive Directoryで定義されているすべてのGPO設定に関する情報を表示することも、CIFSサーバに適用されているGPO設定に関する情報のみを表示することもできます。

手順

1. 次のいずれかの操作を実行して、GPO設定に関する情報を表示します。

情報を表示するグループポリシー設定	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy show-defined -vserver vserver_name`
CIFS対応のStorage Virtual Machine（SVM）に適用されている	`vserver cifs group-policy show-applied -vserver vserver_name`

例

次の例は、CIFS対応のvs1という名前のSVMが属するActive Directoryで定義されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
------------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
```

```
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
```

```
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

次の例は、CIFS対応のSVM vs1に適用されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
------------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
```

```
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
```

```
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
```

関連情報

CIFSサーバでのGPOサポートの有効化と無効化

制限されたグループの**GPO**に関する詳細情報を表示する

Active Directoryでグループポリシーオブジェクト（GPO）として定義されている制限されたグループ、およびCIFSサーバに適用されている制限されたグループに関する詳細情報を表示できます。

タスクの内容

デフォルトでは、次の情報が表示されます。

- グループポリシー名
- グループポリシーバージョン
- リンク

  グループポリシーが設定されているレベルを指定します。指定可能な出力値は次のとおりです。

  - `Local`グループポリシーがONTAPで設定されている状況
  - `Site`グループポリシーがドメインコントローラのサイトレベルで設定されている場合
  - `Domain`グループポリシーがドメインコントローラのドメインレベルで設定されている場合
  - `OrganizationalUnit`グループポリシーがドメインコントローラのOrganizational Unit（OU；組織単位）レベルで設定されている場合
  - `RSOP`さまざまなレベルで定義されたすべてのグループポリシーから派生した一連のポリシー
- 制限されたグループ名
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ

- 制限されたグループが追加されているグループのリスト

  グループは、ここにリストされているグループ以外のグループのメンバーになることができます。

ステップ

1. 次のいずれかの操作を実行して、制限されたグループのすべてのGPOに関する情報を表示します。

情報を表示する制限されたグループのすべての**GPO**	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

例

次の例は、CIFS対応のvs1という名前のSVMが属するActive Directoryドメインで定義されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

次の例では、CIFS対応のSVM vs1に適用されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

関連情報

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報を表示する

Active Directoryで定義されている集約型アクセスポリシーに関する詳細情報を表示できます。また、Group Policy Object（GPO；グループポリシーオブジェクト）を介してCIFSサーバに適用されている集約型アクセスポリシーに関する情報も表示できます。

タスクの内容

デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセスポリシーの名前
- SID
- 説明
- 作成時間
- 更新日時
- メンバールール

ワークグループモードのCIFSサーバはGPOをサポートしていないため表示されません。

ステップ

1. 次のいずれかの操作を実行して、集約型アクセスポリシーに関する情報を表示します。

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
CIFSサアハニテキヨウ	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

例

次の例は、Active Directoryで定義されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

次の例は、クラスタ上のStorage Virtual Machine（SVM）に適用されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                  SID
-------- --------------------
---------------------------------------------
vs1      p1                    S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                    S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

関連情報

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

GPO設定に関する情報の表示

集約型アクセスポリシールールに関する情報の表示

集約型アクセスポリシールールに関する情報を表示する

Active Directoryで定義されている集約型アクセスポリシーに関連付けられている集約型アクセスポリシールールに関する詳細情報を表示できます。また、集約型アクセスポリシーのGPO（グループポリシーオブジェクト）を介してCIFSサーバに適用されている集約型アクセスポリシールールに関する情報も表示できます。

タスクの内容

定義済みおよび適用されている集約型アクセスポリシールールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 更新日時
- 現在の権限

- 推奨される権限
- ターゲットリソース

集約型アクセスポリシーに関連付けられた、情報を表示するすべての集約型アクセスポリシールール	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

例

次の例は、Active Directoryで定義されている集約型アクセスポリシーに関連付けられているすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

次の例は、クラスタ上のStorage Virtual Machine（SVM）に適用されている集約型アクセスポリシーに関連付けられているすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

関連情報

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

SMBサーバコンピュータアカウントパスワードの管理用コマンド

パスワードの変更、リセット、無効化、および自動更新スケジュールの設定に使用するコマンドについて説明します。SMBサーバでスケジュールを設定して自動的に更新することもできます。

状況	使用するコマンド
ONTAPがADサービスと同期されている場合のドメインアカウントパスワードの変更	`vserver cifs domain password change`
ONTAPがADサービスと同期されていない場合のドメインアカウントパスワードのリセット	`vserver cifs domain password reset`
SMBサーバでコンピュータアカウントパスワードの自動変更を設定する	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`

状況	使用するコマンド
SMBサーバでのコンピュータアカウントパスワードの自動変更の無効化	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

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。

ドメインコントローラ接続の管理

検出されたサーバに関する情報を表示する

CIFSサーバで検出されたLDAPサーバおよびドメインコントローラに関する情報を表示できます。

ステップ

1. 検出されたサーバに関する情報を表示するには、次のコマンドを入力します。 `vserver cifs domain discovered-servers show`

例

次の例は、SVM vs1で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

関連情報

サーバのリセットおよび再検出

CIFSサーバの停止と起動

サーバのリセットと再検出

CIFSサーバでサーバをリセットおよび再検出すると、LDAPサーバおよびドメインコントローラに関するCIFSサーバに格納されている情報が破棄されます。サーバ情報を破棄したあと、CIFSサーバはこれらの外部サーバに関する最新の情報を再取得します。これは、接続されているサーバが適切に応答しない場合に役立ちます。

手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. 再検出されたサーバに関する情報を表示します。 `vserver cifs domain discovered-servers show -vserver vserver_name`

例

次の例では、Storage Virtual Machine（SVM、旧Vserver）vs1のサーバをリセットして再検出します。

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

関連情報

検出されたサーバに関する情報の表示

CIFSサーバの停止と起動

ドメインコントローラの検出を管理します。

ONTAP 9 .3以降では、ドメインコントローラ（DC）の検出に使用するデフォルトプロセスを変更できます。これにより、検出対象をサイトまたは優先DCのプールに限定できます。これにより、環境によってはパフォーマンスが向上する可能性があります。

タスクの内容

デフォルトでは、動的検出プロセスによって、使用可能なすべてのDC（優先DC、ローカルサイト内のすべてのDC、およびすべてのリモートDCを含む）が検出されます。そのため、一部の環境では、認証時および共有へのアクセス時にレイテンシが発生する可能性があります。使用するDCのプールが決まっている場合、またはリモートDCが不適切またはアクセスできない場合、検出方法を変更することができます。

ONTAP 9 .3以降のリリースでは `discovery-mode`、コマンドのパラメータを `cifs domain discovered-servers`使用して次の検出オプションのいずれかを選択できます。

- ドメイン内のすべてのDCが検出されます。
- ローカルサイトのDCだけが検出されます。

SMBサーバのパラメータは、 `default-site`sites-and-servicesでサイトに割り当てられていないLIFでこのモードを使用するように定義できます。

- サーバ検出は実行されず、優先DCのみを使用してSMBサーバを設定します。

  このモードを使用するには、まずSMBサーバの優先DCを定義する必要があります。

開始する前に

advanced権限レベルが必要です。

ステップ

1. 目的の検出オプションを指定します。 `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

   パラメータのオプション `mode`：

   - `all`

     使用可能なすべてのDCを検出します（デフォルト）。

   - `site`

     DC検出をサイトに限定します。

   - `none`

     優先DCのみを使用し、検出は実行しません。

優先ドメインコントローラの追加

ONTAPは、DNSを介してドメインコントローラを自動的に検出します。必要に応じて、特定のドメインに対する優先ドメインコントローラのリストに1つ以上のドメインコントローラを追加できます。

タスクの内容

指定したドメインの優先ドメインコントローラリストがすでに存在する場合は、新しいリストが既存のリストにマージされます。

ステップ

1. 優先ドメインコントローラのリストに追加するには、次のコマンドを入力します。+
   `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, …+`

   `-vserver *vserver_name*`Storage Virtual Machine（SVM）名を示します。

   `-domain *domain_name*`指定したドメインコントローラが属するドメインの完全修飾Active Directory名を指定します。

   `-preferred-dc *IP_address*`、…には、優先ドメインコントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

例

次のコマンドでは、SVM vs1上のSMBサーバがcifs.lab.example.comドメインへの外部アクセスを管理するために使用する優先ドメインコントローラのリストに、ドメインコントローラ172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

関連情報

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラを追加、表示、削除するコマンドについて説明します。

状況	使用するコマンド
優先ドメインコントローラを追加する	`vserver cifs domain preferred-dc add`
優先ドメインコントローラを表示する	`vserver cifs domain preferred-dc show`
優先ドメインコントローラを削除する	`vserver cifs domain preferred-dc remove`

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。

関連情報

優先ドメインコントローラの追加

ドメインコントローラへの**SMB2**接続を有効にする

SMB.1以降では、ONTAP 9バージョン2.0からドメインコントローラへの接続を有効にすることができます。この処理は、ドメインコントローラでSMB 1.0を無効にしている場合に必要です。ONTAP 9 .2以降では、SMB2がデフォルトで有効になっています。

タスクの内容

コマンドオプションを使用すると、 `smb2-enabled-for-dc-connections`使用しているONTAPのリリースに応じたシステムデフォルトが有効になります。ONTAP 9 .1のシステムデフォルトでは、SMB 1.0では有効になり、SMB 2.0では無効になります。ONTAP 9 .2のシステムデフォルトは、SMB 1.0では有効、SMB 2.0では有効です。ドメインコントローラが最初にSMB 2.0をネゴシエートできない場合は、SMB 1.0を使用します。

SMB 1.0は、ONTAPからドメインコントローラに対して無効にすることができます。ONTAP 9 .1でSMB 1.0が無効になっている場合は、ドメインコントローラと通信するためにSMB 2.0を有効にする必要があります。

詳細については以下を参照してください。

- "有効なSMBのバージョンの確認"です。

- "サポートされるSMBのバージョンと機能"です。

> がwhileに `-smb1-enabled`設定されて `false`いる場合 `-smb1-enabled-for-dc-connections true`、ONTAPはクライアントとしてのSMB 1.0の接続を拒否しますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

手順

1. SMBセキュリティ設定を変更する前に、有効になっているSMBのバージョンを確認します。 `vserver cifs security show`
2. リストを下にスクロールしてSMBのバージョンを確認します。
3. オプションを使用して、該当するコマンドを実行し `smb2-enabled-for-dc-connections`ます。

SMB2 の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`
無効にする	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

ドメインコントローラへの暗号化接続を有効にする

ONTAP 9 .8以降では、ドメインコントローラへの接続を暗号化するように指定できます。

タスクの内容

このオプションをに設定 `true`すると、ONTAPでドメインコントローラ（DC）通信の暗号化が必要になります `-encryption-required-for-dc-connection`。デフォルトはです。 `false`暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されます。

暗号化されたDC通信が必要な場合、ONTAPはSMB3接続のみをネゴシエートするため、この `-smb2-enabled-for-dc-connections`オプションは無視されます。DCがSMB3と暗号化をサポートしていない場合、ONTAPは接続しません。

ステップ

1. DCとの暗号化通信を有効にします。 `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

非**Kerberos**環境でストレージにアクセスするには**null**セッションを使用します。

Kerberos以外の環境でストレージにアクセスする場合に**null**セッションを使用する概要

null セッションアクセスは、ローカルシステムで稼働しているクライアントベースのサービスにストレージシステムデータなどのネットワークリソースへのアクセスを提供し

ます。null セッションは、クライアントプロセスが「システム」アカウントを使用してネットワークリソースにアクセスするときに発生します。null セッション設定は非 Kerberos 認証に固有です。

ストレージシステムによる**null**セッションアクセスの提供方法

nullセッション共有は認証を必要としないため、nullセッションアクセスを必要とするクライアントは、ストレージシステム上でIPアドレスをマッピングする必要があります。

デフォルトでは、マッピングされていないnullセッションクライアントは、共有の列挙などの特定のONTAPシステムサービスにはアクセスできますが、ストレージシステムデータへのアクセスは制限されます。

> ONTAPでは、オプションを使用してWindows RestrictAnonymousレジストリ設定値をサポートしています `-restrict-anonymous`。これにより、マッピングされていないnullユーザがシステムリソースを表示またはアクセスできる範囲を制御できます。たとえば、共有の列挙とipc$共有（非表示の名前付きパイプ共有）へのアクセスを無効にすることができます。オプションの詳細については、 `vserver cifs options modify`および `vserver cifs options show`のマニュアルページを参照して `–restrict-anonymous`ください。

特に設定がないかぎり、 null セッションでストレージシステムアクセスを要求するローカルプロセスを実行しているクライアントは、「 everyone 」などの制限のないグループのみのメンバーとなります。nullセッションアクセスを選択したストレージシステムリソースに制限するには、すべてのnullセッションクライアントが属するグループを作成します。このグループを作成すると、ストレージシステムアクセスを制限し、nullセッションクライアントにのみ適用されるストレージシステムリソース権限を設定できます。

ONTAPのコマンドセットでは `vserver name-mapping`、nullユーザセッションを使用したストレージシステムリソースへのアクセスを許可するクライアントのIPアドレスを指定できます。nullユーザ用のグループを作成したら、nullセッションにのみ適用されるストレージシステムリソースおよびリソース権限に対するアクセス制限を指定できます。nullユーザは匿名ログオンとして識別されます。nullユーザはどのホームディレクトリにもアクセスできません。

マッピングされたIPアドレスからストレージシステムにアクセスするすべてのnullユーザには、マッピングされたユーザ権限が付与されます。nullユーザにマッピングされたストレージシステムへの不正アクセスを防止するために、適切な予防措置を検討してください。最大限の保護を実現するには、ストレージシステムと null ユーザによるストレージシステムアクセスが必要なすべてのクライアントを別のネットワークに配置し、 IP アドレス「 SVM 」の問題を解消します。

関連情報

匿名ユーザに対するアクセス制限の設定

nullユーザにファイルシステム共有へのアクセスを許可する

nullセッションクライアントによるストレージシステムリソースへのアクセスを許可するには、nullセッションクライアントが使用するグループを割り当て、nullセッションクライアントのIPアドレスを記録して、ストレージシステム上の、nullセッションを使用したデータアクセスを許可するクライアントのリストに追加します。

手順

1. コマンドを使用し `vserver name-mapping create`て、IP修飾子を使用して、有効なWindowsユーザにnullユーザをマッピングします。

次のコマンドは、有効なホスト名 google.com で user1 に null ユーザをマッピングします。

```
vserver name-mapping create –direction win-unix  -position 1 –pattern
“ANONYMOUS LOGON” –replacement user1 – hostname google.com
```

次のコマンドは、有効な IP アドレス 10.238.2.54/32 で user1 に null ユーザをマッピングします。

```
vserver name-mapping create –direction win-unix  -position 2 –pattern
“ANONYMOUS LOGON” –replacement user1 –address 10.238.2.54/32
```

2. コマンドを使用し `vserver name-mapping show`て、ネームマッピングを確認します。

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1       -                 10.72.40.83/32      Pattern: anonymous logon
                                          Replacement: user1
```

3. コマンドを使用し `vserver cifs options modify –win-name-for-null-user`て、nullユーザにWindowsメンバーシップを割り当てます。

   このオプションは、 null ユーザに有効なネームマッピングが設定されている場合にのみ使用できます。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. コマンドを使用し `vserver cifs options show`て、nullユーザがWindowsユーザまたはグループにマッピングされていることを確認します。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

SMBサーバのNetBIOSエイリアスを管理します。

SMBサーバ用のNetBIOSエイリアスの管理の概要

NetBIOSエイリアスは、SMBクライアントがSMBサーバに接続するときに使用でき

るSMBサーバの別名です。SMBサーバのNetBIOSエイリアスを設定すると、他のファイルサーバのデータをSMBサーバに統合し、SMBサーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

NetBIOSエイリアスのリストは、SMBサーバの作成時、またはSMBサーバの作成後にいつでも指定できます。リストにNetBIOSエイリアスを追加または削除することはいつでもできます。SMBサーバには、NetBIOSエイリアスリスト内の任意の名前を使用して接続できます。

関連情報

NetBIOS over TCP接続に関する情報の表示

SMBサーバに**NetBIOS**エイリアスのリストを追加する

エイリアスを使用してSMBサーバに接続できるようにするには、NetBIOSエイリアスのリストを作成するか、既存のNetBIOSエイリアスのリストにNetBIOSエイリアスを追加します。

タスクの内容

- NetBIOSエイリアス名は15文字以内で指定します。
- SMBサーバには最大200個のNetBIOSエイリアスを設定できます。
- 次の文字は使用できません。

  @ # * （） = +[] | ； ： " 、 <> \ / ？

手順

1. NetBIOSエイリアスを追加します。+
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - 1 つ以上の NetBIOS エイリアスをカンマで区切って指定します。
   - 指定した NetBIOS エイリアスが既存のリストに追加されます。
   - NetBIOSエイリアスのリストが現在空の場合は、新しいリストが作成されます。
2. NetBIOSエイリアスが正しく追加されたことを確認します。 `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
            NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
   ```

関連情報

NetBIOSエイリアスリストからのNetBIOSエイリアスの削除

CIFSサーバのNetBIOSエイリアスのリストの表示

NetBIOSエイリアスリストから**NetBIOS**エイリアスを削除する

CIFS サーバで特定の NetBIOS エイリアスが不要な場合、その NetBIOS エイリアスをリストから削除できます。リストからすべての NetBIOS エイリアスを削除することもできます。

タスクの内容

複数のNetBIOSエイリアスを削除するには、カンマで区切って指定します。パラメータの値に `-netbios-aliases`を指定すると、CIFSサーバ上のすべてのNetBIOSエイリアスを削除できます `-`。

手順

1. 次のいずれかを実行します。

削除する項目	入力するコマンド
リスト内の特定の NetBIOS エイリアス	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios-aliases _NetBIOS_alias_,...`
リスト内のすべての NetBIOS エイリアス	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 指定したNetBIOSエイリアスが削除されたことを確認します。 `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

CIFSサーバの**NetBIOS**エイリアスのリストを表示します。

NetBIOSエイリアスのリストを表示できます。これは、SMBクライアントがCIFSサーバへの接続に使用できる名前のリストを確認する場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
CIFSサーバのNetBIOSエイリアス	`vserver cifs show -display-netbios -aliases`
NetBIOSエイリアスのリスト（CIFSサーバの詳細情報の一部）	`vserver cifs show -instance`

次の例は、CIFSサーバのNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

次の例は、NetBIOSエイリアスのリストを含む詳細なCIFSサーバ情報を表示します。

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                               Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

詳細については、コマンドのマニュアルページを参照してください。

関連情報

CIFSサーバへのNetBIOSエイリアスのリストの追加

CIFSサーバの管理用コマンド

SMBクライアントが**NetBIOS**エイリアスを使用して接続しているかどうかの確認

SMB クライアントが NetBIOS エイリアスを使用して接続しているかどうか、および使用している場合はその NetBIOS エイリアスを確認できます。これは、接続の問題をトラ

ブルシューティングするときに役立ちます。

タスクの内容

SMB接続に関連付けられているNetBIOSエイリアス（ある場合）を表示するには、パラメータを使用する必要があります `-instance`。CIFSサーバの名前またはIPアドレスを使用してSMB接続を確立している場合、フィールドの出力 `NetBIOS Name`は（ハイフン）になります `-`。

ステップ

1. 必要な操作を実行します。

表示する **NetBIOS** 情報	入力するコマンド
SMBセツソク	`vserver cifs session show -instance`
指定した NetBIOS エイリアスを使用する接続：	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

次の例は、Session ID 1とのSMB接続に使用されるNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                  Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

その他の**SMB**サーバタスクの管理

ユーザがSMB共有を介してデータにアクセスしていない間にタスクを実行する場合は、SVM上のCIFSサーバを停止すると便利です。SMBアクセスを再開するには、CIFSサーバを起動します。CIFSサーバを停止することによって、Storage Virtual Machine（SVM）で許可されているプロトコルを変更することもできます。

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
CIFSサーバを停止する	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	CIFSサーバを起動する
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground`コマンドをフォアグラウンドとバックグラウンドのどちらで実行するかを指定します。このパラメータを入力しない場合、このパラメータはに設定され `true`、フォアグラウンドでコマンドが実行されます。

2. コマンドを使用して、CIFSサーバの管理ステータスが正しいことを確認します `vserver cifs show`。

例

次のコマンドは、SVM vs1でCIFSサーバを起動します。

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

関連情報

検出されたサーバに関する情報の表示

サーバのリセットおよび再検出

別のOUへのCIFSサーバの移動

CIFSサーバの作成プロセスでは、別のOUを指定しないかぎり、セットアップ時にデフォルトの組織単位（OU）CN=Computersが使用されます。CIFSサーバはセットアップ後に別のOUに移動できます。

手順

1. Windows サーバーで、 * Active Directory ユーザーとコンピューター * ツリーを開きます。
2. Storage Virtual Machine（SVM）のActive Directoryオブジェクトを探します。
3. オブジェクトを右クリックし、 * 移動 * （ * Move * ）を選択します。
4. SVMに関連付けるOUを選択します。

結果

選択したOUにSVMオブジェクトが配置されます。

SMBサーバ移動前にSVM上の動的DNSドメインを変更する

SMBサーバを別のドメインに移動するときに、Active Directory統合DNSサーバでSMBサーバのDNSレコードがDNSに動的に登録されるようにするには、SMBサーバを移動する前にStorage Virtual Machine（SVM）の動的DNS（DDNS）を変更する必要があります。

開始する前に

SMB サーバコンピュータアカウントを含む新しいドメインのサービスロケーションレコードを含む DNS ドメインを使用するには、 SVM で DNS ネームサービスを変更する必要があります。セキュアDDNSを使用している場合は、Active Directoryに統合されたDNSネームサーバを使用する必要があります。

タスクの内容

DDNS （ SVM 上で設定されている場合）はデータ LIF の DNS レコードを新しいドメインに自動的に追加しますが、元のドメインの DNS レコードは元の DNS サーバから自動的には削除されません。手動で削除する必要があります。

SMBサーバを移動する前にDDNSの変更を完了するには、次のトピックを参照してください。

"動的DNSサービスの設定"

SVMのActive Directoryドメインへの参加

コマンドを使用してドメインを変更すると、既存のSMBサーバを削除せずにStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify`。現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

開始する前に

- SVM の DNS 設定が完了している必要があります。
- SVM の DNS 設定がターゲットドメインを提供できる必要があります。

DNSサーバには、ドメインLDAPサーバとドメインコントローラサーバのサービスロケーションレコード（SRV）が含まれている必要があります。

タスクの内容

- Active Directory ドメインの変更を続行するには、 CIFS サーバの管理ステータスを「所有」に設定する必要があります。
- コマンドが正常に完了すると、管理ステータスは自動的に「 up 」に設定されます。
- ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

手順

1. SVMをCIFSサーバドメインに追加します。 `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   詳細については、コマンドのマニュアルページを参照して `vserver cifs modify`ください。新しいドメイン用にDNSを再設定する必要がある場合は、コマンドのマニュアルページを参照して `vserver dns modify`ください。

   SMBサーバ用のActive Directoryマシンアカウントを作成するには、.comドメイン内のコンテナ *`example`* にコンピュータを追加するための十分な`Privileges`を備えた`Windows`アカウントの名前とパスワードを指定する必要があります `ou=` *`example`* `ou`。

   ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

2. CIFSサーバが目的のActive Directoryドメイン内にあることを確認します。 `vserver cifs show`

例

次の例では、 SVM vs1 上にある SMB サーバ「 CIFSSERVER1 」を keytab 認証を使用して example.com ドメインに追加します。

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

NetBIOS over TCP接続に関する情報を表示する

NetBIOS over TCP（NBT）接続に関する情報を表示できます。これは、NetBIOS関連の問題のトラブルシューティングに役立ちます。

ステップ

1. NetBIOS over TCP接続に関する情報を表示するには、コマンドを使用し `vserver cifs nbtstat`ます。

IPv6経由のNetBIOSネームサービス（NBNS）はサポートされていません。

例

次の例は、「 cluster1 」について表示される NetBIOS ネームサービスの情報を示しています。

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

SMBサーバの管理用コマンド

作成、表示、変更、停止、開始、 およびSMBサーバを削除しています。また、サーバのリセットと再検出、マシンアカウントパスワードの変更またはリセット、マシンアカウントパスワードのスケジュール変更、NetBIOSエイリアスの追加または削除を行うコマンドもあります。

状況	使用するコマンド

SMB サーバを作成	`vserver cifs create`
SMBサーバに関する情報を表示する	`vserver cifs show`
SMBサーバを変更する	`vserver cifs modify`
SMBサーバを別のドメインに移動する	`vserver cifs modify`
SMBサーバを停止する	`vserver cifs stop`
SMBサーバを起動する	`vserver cifs start`
SMBサーバを削除する	`vserver cifs delete`
SMBサーバ用のサーバのリセットと再検出	`vserver cifs domain discovered-servers reset-servers`
SMBサーバのマシンアカウントパスワードを変更する	`vserver cifs domain password change`
SMBサーバのマシンアカウントパスワードをリセットする	`vserver cifs domain password change`
SMBサーバのマシンアカウントの自動パスワード変更のスケジュールを設定する	`vserver cifs domain password schedule modify`
SMBサーバ用のNetBIOSエイリアスを追加する	`vserver cifs add-netbios-aliases`
SMBサーバのNetBIOSエイリアスを削除する	`vserver cifs remove-netbios-aliases`

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。

関連情報

"SMBサーバを削除したときのローカルユーザとローカルグループへの影響"

NetBIOSネームサービスを有効にする

ONTAP 9以降では、NetBIOSネームサービス（NBNS、Windowsインターネットネームサービスまたは WINSと呼ばれることもあります）はデフォルトで無効になっています。以前は、WINSがネットワークで有効になっているかどうかに関係なく、CIFS対応Storage Virtual Machine（SVM）が名前登録のブロードキャストを送信していました。このようなブロードキャストをNBNSが必要な構成に限定するには、新しいCIFSサーバに対してNBNSを明示的に有効にする必要があります。

開始する前に

- すでにNBNSを使用していて、ONTAP 9にアップグレードする場合は、このタスクを実行する必要はありません。NBNSは以前と同様に機能します。
- NBNSはUDP（ポート137）でイネーブルになっています。
- IPv6経由のNBNSはサポートされていません。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. CIFSサーバでNBNSを有効にします。

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. admin権限レベルに戻ります。

```
set -privilege admin
```

SMBアクセスとSMBサービスにIPv6を使用する

IPv6の使用要件

SMBサーバでIPv6を使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとライセンスの要件について確認しておく必要があります。

ONTAPのライセンス要件

SMBのライセンスがある場合、IPv6に特別なライセンスは必要ありません。SMBライセンスはに含まれて"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMBプロトコルのバージョン

- SVMについては、ONTAPですべてのバージョンのSMBプロトコルでIPv6がサポートされます。

IPv6経由のNetBIOSネームサービス（NBNS）はサポートされていません。

SMBアクセスとCIFSサービスでのIPv6のサポート

CIFSサーバでIPv6を使用する場合は、ONTAPによるSMBアクセスやCIFSサービスとのネットワーク通信でのIPv6のサポートについて確認しておく必要があります。

Windowsクライアントおよびサーバのサポート

ONTAPは、IPv6をサポートするWindowsサーバおよびクライアントをサポートします。次に、Microsoft Windowsクライアントおよびサーバの IPv6サポートについて説明します。

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012以降では、SMBファイル共有とActive Directoryサービス（DNS、LDAP、CLDAP、Kerberosの各サービス）の両方でIPv6がサポートされます。

  IPv6アドレスが設定されている場合、Windows 7およびWindows Server 2008以降のリリースでは、Active Directoryサービスにデフォルトで IPv6が使用されます。IPv6接続を介したNTLM認証とKerberos認証の両方がサポートされます。

  ONTAPでサポートされるWindowsクライアントは、いずれもIPv6アドレスを使用してSMB共有に接続できます。

ONTAPがサポートするWindowsクライアントの最新情報については、を参照して"Interoperability Matrix"ください。

NTドメインはIPv6ではサポートされていません。

その他の**CIFS**サービスのサポート

ONTAPでは、SMBファイル共有とActive Directoryサービスに加えて、次の項目に対してもIPv6をサポートしています。

- クライアント側のサービス（オフラインフォルダ、移動プロファイル、フォルダリダイレクト、以前のバージョン機能など）
- サーバ側のサービス：動的ホームディレクトリ（ホームディレクトリ機能）、シンボリックリンクとワイドリンク、BranchCache、ODXコピーオフロード、自動ノードリファーラル、以前のバージョン機能など
- ファイルアクセス管理サービス（Windowsのローカルユーザおよびローカルグループを使用したアクセス制御と権限の管理、CLIを使用したファイル権限と監査ポリシーの設定、セキュリティトレース、ファイルロックの管理、SMBアクティビティの監視など）
- NASのマルチプロトコルの監査
- FPolicy
- 共有の継続的可用性、監視プロトコル、およびリモートVSS（Hyper-V over SMB構成で使用）

ネームサービスと認証サービスのサポート

IPv6では、次のネームサービスとの通信がサポートされます。

- ドメインコントローラ
- DNSサーバ
- LDAPサーバ
- KDCサーバ
- NISサーバ

要件に応じた設定を作成するには、CIFSサーバが外部サーバへの接続を確立する際にIPv6がどのように使用されるかを確認しておく必要があります。

- 送信元アドレスの選択

  外部サーバに接続しようとする場合、選択する送信元アドレスは宛先アドレスと同じタイプである必要があります。たとえば、IPv6アドレスに接続する場合、CIFSサーバをホストするStorage Virtual Machine（SVM）には、ソースアドレスとして使用するIPv6アドレスを持つデータLIFまたは管理LIFが必要です。同様に、IPv4アドレスに接続する場合、SVMには、ソースアドレスとして使用するIPv4アドレスを持つデータLIFまたは管理LIFが必要です。

- DNSを使用して動的に検出されたサーバの場合、サーバ検出は次のように実行されます。
  - クラスタで IPv6 が無効になっている場合は、 IPv4 サーバアドレスのみが検出されます。
  - クラスタで IPv6 が有効になっている場合は、 IPv4 と IPv6 の両方のサーバアドレスが検出されます。アドレスが属するサーバが適切かどうか、およびIPv6またはIPv4のデータLIFまたは管理LIFが使用可能かどうかに応じて、どちらかのタイプが使用されます。動的サーバ検出は、ドメインコントローラとその関連サービス（LSA、NETLOGON、Kerberos、LDAPなど）の検出に使用されます。

- DNSサーバへの接続

  SVMがDNSサーバに接続するときにIPv6を使用するかどうかは、DNSネーム サービスの設定によって決まります。IPv6アドレスを使用するようにDNSサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、DNSサーバへの接続で引き続きIPv4アドレスを使用できるように、DNSネームサービスの設定でIPv4アドレスを使用できます。DNSネーム サービスの設定時には、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

- LDAPサーバへの接続

  SVMがLDAPサーバに接続するときにIPv6を使用するかどうかは、LDAPクライアントの設定によって異なります。IPv6アドレスを使用するようにLDAPクライアントが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、LDAPサーバへの接続で引き続きIPv4アドレスを使用できるように、LDAPクライアント設定でIPv4アドレスを使用できます。LDAPクライアントの設定時に、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

  LDAPクライアント設定は、UNIXユーザ、グループ、およびネットグループのネームサービス用にLDAPを設定するときに使用されます。

- NISサーバへの接続

  SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネームサービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、NISサーバへの接続で引き続きIPv4アドレスを使用できるように、NISネームサービスの設定でIPv4アドレスを使用できます。NISネームサービスの設定時に、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

  NISネームサービスは、UNIXユーザ、グループ、ネットグループ、およびホスト名オブジェクトを格納および管理するために使用されます。

関連情報

SMBでのIPv6の有効化（クラスタ管理者のみ）

IPv6 SMBセッション情報の監視および表示

SMBでのIPv6の有効化（クラスタ管理者のみ）

IPv6ネットワークはクラスタのセットアップ時に有効になりません。SMBでIPv6を使用するには、クラスタのセットアップ完了後にクラスタ管理者がIPv6を有効にする必要があります。クラスタ管理者がIPv6を有効にすると、IPv6はクラスタ全体で有効になります。

ステップ

1. IPv6を有効にします。 `network options ipv6 modify -enabled true`

   クラスタでの IPv6 の有効化と IPv6 LIF の設定の詳細については、 _ ネットワーク管理ガイド _ を参照してください。

   IPv6が有効になっています。SMBアクセス用のIPv6データLIFを設定できます。

関連情報

IPv6 SMBセッション情報の監視および表示

"ネットワーク管理"

SMBでのIPv6の無効化

クラスタでIPv6を有効にするにはネットワークオプションを使用しますが、同じコマンドを使用してSMBでIPv6を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後にIPv6を有効にしたインターフェイスを無効にすると、ONTAPはIPv6を無効にします。IPv6が有効なインターフェイスの管理については、クラスタ管理者に問い合わせてください。

クラスタでの IPv6 の無効化の詳細については、 _ ネットワーク管理ガイド _ を参照してください。

関連情報

"ネットワーク管理"

IPv6 SMBセッションに関する情報を監視および表示する

IPv6ネットワークを使用して接続されているSMBセッションに関する情報を監視および表示できます。この情報は、IPv6 SMBセッションに関するその他の有用な情報と同様に、IPv6を使用して接続しているクライアントを特定する場合に役立ちます。

ステップ

1. 必要な操作を実行します。

確認する項目	入力するコマンド
Storage Virtual Machine（SVM）へのSMBセッションはIPv6を使用して接続される	`vserver cifs session show -vserver vserver_name -instance`
IPv6は、指定したLIFアドレスを介したSMBセッションに使用されます。	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` `LIF_IP_address`は、データLIFのIPv6アドレスです。

SMBを使用したファイルアクセスのセットアップ

セキュリティ形式の設定

セキュリティ形式がデータアクセスに与える影響

セキュリティ形式とその影響

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式によって、データに対する権限の処理方法が異なります。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、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、ONTAPはマルチプロトコルに対応しているため、SMBクライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAPでは、UNIXクライアントのみが標準のツールを使用して変更できるUNIX権限が使用されます。

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		
NTFS	SMB	NTFS ACL	NTFS	
mixed	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
unified （ Infinite Volume のみ、 ONTAP 9.4 以前のリリース）	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVolでは、UNIX、NTFS、およびmixedのセキュリティ形式がサポートされます。セキュリティ形式がmixedまたはunifiedの場合、ユーザはセキュリティ形式を個別に設定するため、権限を最後に変更したクライアントのタイプによって有効な権限が異なります。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。

unifiedセキュリティ形式は、Infinite Volumeでのみ使用できます。Infinite Volumeは、ONTAP 9 .5以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

Windows.2以降では、コマンドのパラメータを `vserver security file-directory`使用して、指定したファイルまたはフォルダパスでONTAP 9 `show-effective-permissions`ユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータを `-share-name`使用すると、有効な共有権限を表示できます。

> ONTAPは、最初に一部のデフォルトのファイル権限を設定します。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は、セキュリティ形式はUNIXになり、アクセス権のタイプはUNIXモードビット（特に指定がないかぎり0755）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るようにクライアントによって設定されるまでの間です。デフォルトでは、NTFSセキュリティ形式のボリューム内のすべてのデータに対するセキュリティ形式はNTFSになり、すべてのユーザにフルコントロールを許可するACLが割り当てられます。

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両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

SVMで使用するセキュリティ形式を決定する

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。主な要因は、ファイルシステムを管理する管理者のタイプです。2番目の要因は、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。

ボリュームでセキュリティ形式を設定する場合は、最適なセキュリティ形式を選択し、権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定には、次の考慮事項が役立ちます。

セキュリティ形式	以下の場合に選択
UNIX	• ファイルシステムはUNIX管理者によって管理されます。 • 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は、UNIXユーザをサービスアカウントとして使用します。

セキュリティ形式	以下の場合に選択
NTFS	• ファイルシステムはWindows管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションでは、Windowsユーザをサービスアカウントとして使用します。
mixed	ファイルシステムはUNIX管理者とWindows管理者の両方によって管理され、ユーザはNFSクライアントとSMBクライアントの両方で構成されます。

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さまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む 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 ボリューム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 ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAPによる**UNIX**アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、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、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

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

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれ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できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 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できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限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 アクセス権を NTFS アクセス権に変更しています

  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のセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの 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。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式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。

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、コマンドで `-rootvolume-security-style`パラメータを使用し `vserver create`ます。

   ルートボリュームのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

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ボリューム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 volume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 ボリュームの状況	使用するコマンド
まだ存在しません	`volume create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

FlexVol volumeセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

FlexVol volume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。

コマンドまたは `volume modify`コマンドの詳細については `volume create`、を参照してください"論理ストレージ管理"。

2. 作成したFlexVol volume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ボリューム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
まだ存在しません	`volume qtree create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume qtree modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

qtreeのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

コマンドまたは `volume qtree modify`コマンドの詳細については `volume qtree create`、を参照してください"論理ストレージ管理"。

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`

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ネームスペースでのデータボリュームの作成と管理の概要

NAS環境でファイルアクセスを管理するには、Storage Virtual Machine（SVM）上でデータボリュームと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。

ジャンクションポイントを指定してデータボリュームを作成する

ジャンクションポイントは、データボリュームの作成時に指定できます。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。

> ジャンクションパスに次の文字を使用することはできません。 * # <> < | ? \
>
> また、ジャンクションパスの長さは255文字以下にする必要があります。

手順

1. ジャンクションポイントを設定して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、ディレクトリと結合されたボリュームの両方を含めることができます。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任意です。セキュリティ形式を指定しない場合、ONTAP はStorage Virtual Machine（SVM）のルートボリューム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適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、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が区別されません。はと同じ `/eng`です。 `/ENG`CIFS共有を作成する場合、Windowsではジャンクションパスは大文字と小文字が区別されるかのように扱われます。たとえば、ジャンクションがの場合、 `/ENG`CIFS共有のパスははではなくで `/eng`始まる必要があります `/ENG`。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。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 `volume create`ください。

2. 目的のジャンクションポイントで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である「home4」という名前のボリュームをSVM vs1上に作成し`/eng/home`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を指定せずにデータボリュームを作成する

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アクセス用に設定することもできません。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、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任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリューム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適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、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。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。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`volume create`ください。

2. ボリュームがジャンクションポイントなしで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ネームスペースで既存のボリュームをマウントまたはアンマウントする

Storage Virtual Machine（SVM）ボリュームに格納されたデータへのNASクライアントから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。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームをアンマウントすることもできます。

タスクの内容

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、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。

> ボリュームへのNASクライアントアクセスを中止するには、ボリュームをアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次のナレッジベースの記事を参照してください。 "ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"

ボリュームをアンマウントしてオフラインにしても、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と、ボリュームまたはディレクトリに作成された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は保持されます。アンマウントしたボリュームを再マウントすると、NASクライアント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に格納されているデータにアクセスできます。

手順

1. 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` *`svm_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 svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例は、SVM「vs1」にある「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」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

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の情報を表示します。

Storage Virtual Machine（SVM）のマウントボリューム、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。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ネームスペースを理解し、管理することができます。

手順

1. 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のマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver vserver_name -junction`
SVM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に関する詳細情報	`volume show -vserver vserver_name -volume volume_name -instance`
SVM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に関する特定の情報	a. 必要に応じて、次のコマンドを使用してパラメータの有効なフィールドを表示できます `-fields。 volume show -fields ?` b. パラメータを使用して、必要な情報を表示し `-fields`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
```

次の例は、SVM vs2上に配置された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
```

ネームマッピングの設定

ネームマッピングの設定の概要

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クライアントとCIFSクライアントのどちらから接続しているかに関係なく、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。

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、ボリュームで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。
- 代わりにデフォルトユーザを使用するように設定します。

  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個別に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ないことに注意してください。

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という語で開始または終了するすべての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。

ネームマッピングの仕組み

ONTAPで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は、まずローカルのネームマッピングデータベースとLDAPサーバで既存のマッピングの有無を確認します。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、SVMのネームサービスの設定で決まります。

- 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、ONTAPは小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。見つからない場合は、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、ONTAPはSMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合は、デフォルトのSMB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。

マシンアカウントは、デフォルトで指定されたデフォルトのUNIXユーザにマッピングされます。デフォルトのUNIXユーザが指定されていない場合、マシンアカウントのマッピングは失敗します。

- ONTAP 9 .5以降では、マシンアカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9 .4以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントのネームマッピングが定義されていても、それらのマッピングは無視されます。

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

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。また、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ONTAPとどのように連携するかを理解しておく必要があります。CIFSサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、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されます。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するユーザを認証および許可できます。その逆も同様です。

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間で双方向の信頼関係が確立された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、ホームドメインはもう一方のドメインを信頼します。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す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実行時に _not_searched になります。

- 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するユーザを認証または許可できません。

  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実行時に _not_searched になります。

ワイルドカード（*）を使用したネームマッピング用のマルチドメイン検索の設定方法

マルチドメインネームマッピングの検索は、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することで簡単に実行できます。次の表に、ネームマッピングエントリのドメイン部分でワイルドカードを使用してマルチドメイン検索を有効にする方法を示します。

パターン	交換	結果
root	*\\administrator	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。

パターン	交換	結果
*	\ * \\ *	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。 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

マルチドメイン名の検索に使用する信頼できるドメインのリストを決定するには、次の2つの方法のいずれかを選択します。

- ONTAPによってコンパイルされた自動検出双方向信頼リストを使用する
- コンパイルした信頼できるドメインの優先リストを使用する

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、マッピングされたWindowsユーザはこの検索リストでのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係が確立されたすべてのドメインでWindowsユーザの検索が行われます。
- ホームドメインに双方向の信頼関係が確立されたドメインがない場合は、ホームドメインでユーザの検索が行われます。

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、ホームドメインでWindowsユーザの検索が行われます。

ネームマッピングの変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 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プログラムのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed`。

ネームマッピングを作成する

コマンドを使用すると、ネームマッピングを作成できます `vserver name-mapping`

create。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。

タスクの内容

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`

   および `-replacement`ステートメントは、 `-pattern`正規表現として記述できます。また、ステートメントを使用して、`null`の置換文字列（スペース文字）を使用してユーザへのマッピングを明示的に拒否する `" "`こともできます `-replacement`。詳細については、のマニュアルページを参照して `vserver name-mapping create` ください。

   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 ONTAP システムに接続していたすべての SMB 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、優先順位リストの1番目にあります。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 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。パターンとリプレースメントには正規表現が使用されています。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 LDAP 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"
```

次のコマンドは、 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。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

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。または、マッピングされていないユーザの認証を失敗させる場合は、デフォルトユーザを設定しないでください。

タスクの内容

CIFS認証で、各Windowsユーザを個 々 のUNIXユーザにマッピングしない場合は、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 々 のWindowsユーザにマッピングしない場合は、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`*

ネームマッピングの管理用コマンド

ONTAPには、ネームマッピングを管理するため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`

状況	使用するコマンド
2つのネームマッピングの位置を交換する IP修飾子エントリを使用してネームマッピングが設定されている場合、スワップは許可されません。	`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`
ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

詳細については、各コマンドのマニュアルページを参照してください。

マルチドメインネームマッピング検索の設定

マルチドメインネームマッピングの検索を有効または無効にする

マルチドメインネームマッピングの検索では、 UNIX ユーザから Windows ユーザへのネームマッピングを設定するときに、 Windows 名のドメイン部分にワイルドカード（ * ）を使用できます。名前のドメイン部分にワイルドカード（ * ）を使用すると、 ONTAP で、 CIFS サーバのコンピュータアカウントが含まれるドメインと双方向の信頼関係が確立されているすべてのドメインを検索できるようになります。

タスクの内容

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。信頼できるドメインのリストを設定すると、ONTAPは双方向の信頼関係が確立された検出ドメインの代わりに、信頼できるドメインのリストを使用してマルチドメインネームマッピングの検索を実行します。

- マルチドメインネームマッピングの検索は、デフォルトで有効になっています。
- このオプションは、advanced権限レベルで使用できます。

手順

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。

マルチドメインネームマッピングの検索の設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

使用できるSMBサーバオプション

信頼できるドメインのリセットと再検出

すべての信頼できるドメインを強制的に再検出することができます。これは、信頼できるドメインサーバが適切に応答しない場合や、信頼関係が変更された場合に役立ちます。ホームドメイン（CIFSサーバのコンピュータアカウントを含むドメイン）と双方向の信頼関係が確立されたドメインのみが検出されます。

ステップ

1. コマンドを使用して、信頼できるドメインをリセットして再検出し `vserver cifs domain trusts rediscover` ます。

```
vserver cifs domain trusts rediscover -vserver vs1
```

関連情報

検出された信頼できるドメインに関する情報の表示

検出された信頼できるドメインに関する情報を表示する

CIFSサーバのホームドメイン（CIFSサーバのコンピュータアカウントが含まれているドメイン）で検出された信頼できるドメインに関する情報を表示できます。この情報は、検出された信頼できるドメインと、検出された信頼できるドメインのリスト内でのそれらの順序を確認する場合に役立ちます。

タスクの内容

ホームドメインと双方向の信頼関係が確立されたドメインのみが検出されます。ホームドメインのドメインコントローラ（DC）は、信頼できるドメインのリストをDCが決定した順序で返すため、リスト内のドメインの順序を予測することはできません。信頼できるドメインのリストを表示することで、マルチドメインネームマッピングの検索での検索順序を確認できます。

表示される信頼できるドメインの情報は、ノードおよびStorage Virtual Machine（SVM）別にグループ化されます。

ステップ

1. コマンドを使用して、検出された信頼できるドメインに関する情報を表示します `vserver cifs domain trusts show`。

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ------------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ------------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

関連情報

信頼できるドメインのリセットおよび再検出

信頼できるドメインの優先リスト内の信頼できるドメインの追加、削除、置換

SMBサーバの信頼できるドメインの優先リストに対して信頼できるドメインを追加または削除したり、現在のリストを変更したりできます。信頼できるドメインの優先リストを設定すると、マルチドメインネームマッピングの検索を実行するときに、検出された双方向の信頼できるドメインの代わりにこのリストが使用されます。

タスクの内容

- 信頼できるドメインを既存のリストに追加する場合は、新しいリストが既存のリストにマージされ、新しいエントリが末尾に追加されます。信頼できるドメインは、リスト内の順序で検索されます。
- 信頼できるドメインを既存のリストから削除する際にリストを指定しないと、指定したStorage Virtual Machine（SVM）の信頼できるドメインのリスト全体が削除されます。
- 信頼できるドメインの既存のリストを変更すると、新しいリストで上書きされます。

> 信頼できるドメインのリストには、双方向の信頼関係が確立されたドメインだけを入力してください。アウトバウンドまたはインバウンドの信頼ドメインを優先ドメインリストに入力することはできますが、マルチドメインネームマッピングの検索では使用されません。ONTAPは単方向ドメインのエントリをスキップし、リスト内の次の双方向の信頼関係が確立されたドメインに移動します。

ステップ

1. 次のいずれかを実行します。

信頼できるドメインのリストに対して行う操作	使用するコマンド
信頼できるドメインをリストに追加する	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
信頼できるドメインをリストから削除する	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
既存のリストを変更する	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

例

次のコマンドは、SVM vs1で使用される信頼できるドメインの優先リストに2つの信頼できるドメイン（cifs1.example.comおよびcifs2.example.com）を追加します。

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1で使用されるリストから信頼できるドメインを2つ削除します。

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1で使用される信頼できるドメインのリストを変更します。元のリストが新しいリストに置き換えられます。

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

関連情報

信頼できるドメインの優先リストに関する情報の表示

信頼できるドメインの優先リストに関する情報を表示する

信頼できるドメインの優先リストに含まれている信頼できるドメインに関する情報、およびマルチドメインネームマッピングの検索が有効な場合の信頼できるドメインの検索順序に関する情報を表示できます。自動検出された信頼できるドメインの優先リストを

使用する代わりに、信頼できるドメインの優先リストを設定することもできます。

手順

1. 次のいずれかを実行します。

表示する情報	使用するコマンド
Storage Virtual Machine（SVM）別にグループ化されたクラスタ内のすべての信頼できる優先ドメイン	`vserver cifs domain name-mapping-search show`
指定したSVMのすべての信頼できる優先ドメイン	`vserver cifs domain name-mapping-search show -vserver vserver_name`

次のコマンドは、クラスタ上のすべての信頼できる優先ドメインに関する情報を表示します。

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
--------------   ----------------------------------
vs1              CIFS1.EXAMPLE.COM
```

関連情報

信頼できるドメインの優先リスト内の信頼できるドメインの追加、削除、または置換

SMB共有の作成と設定

SMB共有の作成と設定の概要

ユーザやアプリケーションがSMB経由でCIFSサーバ上のデータにアクセスできるようにするには、SMB共有を作成して設定する必要があります。SMB共有は、ボリューム内の指定されたアクセスポイントです。共有をカスタマイズするには、共有パラメータと共有プロパティを指定します。既存の共有はいつでも変更できます。

SMB共有を作成すると、すべてのメンバーにフルコントロール権限が設定されたACLがONTAPによってデフォルトで作成されます。

SMB共有は、Storage Virtual Machine（SVM）上のCIFSサーバに関連付けられます。SVMが削除された場合、または関連付けられているCIFSサーバがSVMから削除された場合、SMB共有は削除されます。SVMにCIFSサーバを再作成する場合は、SMB共有を再作成する必要があります。

関連情報

SMBを使用したファイルアクセスの管理

"Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"

ボリュームでのSMBファイル名の変換のための文字マッピングの設定

Storage Virtual Machine（SVM）上にCIFSサーバを作成すると、デフォルトの管理共有が自動的に作成されます。これらのデフォルトの共有とその用途について理解しておく必要があります。

CIFSサーバを作成すると、ONTAPによって次のデフォルトの管理共有が作成されます。

ONTAP 9 .8以降では、admin$共有はデフォルトで作成されなくなりました。

- IPC$
- admin$（ONTAP 9.7以前のみ）
- c$

$文字で終わる共有は非表示の共有であるため、デフォルトの管理共有は[マイコンピュータ]には表示されませんが、[共有フォルダ]を使用して表示できます。

ipc$**および**admin$デフォルト共有の使用方法

ipc$共有とadmin$共有はONTAPが使用するものであり、Windows管理者がSVM上のデータにアクセスするために使用することはできません。

- ipc$共有

  ipc$共有は、プログラム間の通信に不可欠な名前付きパイプを共有するリソースです。ipc$共有は、コンピュータのリモート管理中およびコンピュータの共有リソースを表示するときに使用されます。ipc$共有の共有設定、共有プロパティ、ACLは変更できません。また、ipc$共有の名前を変更したり削除したりすることもできません。

- admin$共有（ONTAP 9.7以前のみ）

  ONTAP 9 .8以降では、admin$共有はデフォルトで作成されなくなりました。

  admin$共有は、SVMのリモート管理に使用されます。このリソースのパスは、常にSVMルートへのパスです。admin$共有の共有設定、共有プロパティ、ACLは変更できません。また、admin$共有の名前変更や削除もできません。

c$テフオルトキヨウユウノシヨウホウホウ

c$共有は、クラスタ管理者またはSVM管理者がSVMルートボリュームへのアクセスと管理に使用できる管理共有です。

c$共有の特徴は次のとおりです。

- この共有のパスは、常にSVMルートボリュームへのパスであり、変更することはできません。
- c$共有のデフォルトのACLは、Administrator/Full Controlです。

  このユーザはBUILTIN\administratorです。デフォルトでは、BUILTIN\administratorを共有にマッピングし、マッピングされたルートディレクトリ内のファイルやフォルダを表示、作成、変更、削除できます。

このディレクトリ内のファイルとフォルダを管理する場合は、注意が必要です。

- c$共有のACLは変更できます。
- c$共有設定と共有プロパティを変更できます。
- c$共有は削除できません。
- SVM管理者は、ネームスペースジャンクションを横断することで、マッピングされたc$共有から残りのSVMネームスペースにアクセスできます。
- c$共有には、Microsoft管理コンソールを使用してアクセスできます。

関連情報

Windowsの[セキュリティ]タブを使用した詳細なNTFSファイル権限の設定

SMB共有の命名要件

SMBサーバでSMB共有を作成するときは、ONTAP共有の命名要件に注意してください。

ONTAPの共有の命名規則はWindowsの命名規則と同じで、次の要件があります。

- 各共有名はSMBサーバで一意である必要があります。
- 共有名では大文字と小文字は区別されません。
- 共有名の最大文字数は80文字です。
- 共有名はUnicodeに対応しています。
- $文字で終わる共有名は非表示の共有です。
- ONTAP 9 .7以前の場合、admin$、ipc$、およびc$管理共有はすべてのCIFSサーバで自動的に作成され、共有名が予約されています。ONTAP 9 .8以降では、admin$共有は自動的に作成されなくなりました。
- 共有の作成時に共有名ONTAP _ ADMIN$を使用することはできません。
- 共有名ではスペースの使用がサポートされます。
  - 共有名の先頭または末尾の文字をスペースにすることはできません。
  - スペースを含む共有名は引用符で囲む必要があります。

    単一引用符は共有名の一部とみなされ、引用符の代わりに使用することはできません。

- SMB共有の名前では次の特殊文字がサポートされます。

  なんだ? @ #$%&'__ 。~ （） { }

- SMB共有の名前では、次の特殊文字はサポートされません。
  - "/\\:;|<> 、 ? * =

マルチプロトコル環境で共有を作成する際のディレクトリの大文字と小文字の区別

名前に大文字と小文字の違いしかないディレクトリ名を区別するために 8.3 の命名方法が使用されている SVM に共有を作成する場合は、クライアントが必要なディレクトリ

パスに接続できるように共有パスに 8.3 の名前を使用する必要があります。

次の例では、 Linux クライアント上に「 testdir 」と「 testdir 」という名前の 2 つのディレクトリが作成されています。ディレクトリを含むボリュームのジャンクションパスは、です `/home`。最初の出力は Linux クライアントで、 2 番目の出力は SMB クライアントで行います。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

2 番目のディレクトリへの共有を作成する場合、共有パスに 8.3 の名前を使用する必要があります。この例では、最初のディレクトリの共有パスはで `/home/testdir`、2番目のディレクトリの共有パスはです `/home/TESTDI~1`。

SMB共有プロパティを使用する

SMB共有プロパティの使用の概要

SMB 共有のプロパティをカスタマイズすることができます。

使用可能な共有プロパティは次のとおりです。

共有プロパティ	説明
`oplocks`	共有で便宜的ロック（クライアント側キャッシュ）を使用することを指定します。
`browsable`	Windowsクライアントが共有を参照することを許可します。
`showsnapshot`	クライアントがSnapshotコピーを表示およびトラバースできることを指定します。
`changenotify`	共有が変更通知要求をサポートすることを指定します。SVM 上の共有では、これはデフォルトの初期プロパティです。

共有プロパティ	説明
attributecache	属性にすばやくアクセスできるように SMB 共有でのファイル属性のキャッシュを有効にします。デフォルトでは、属性のキャッシュは無効になっています。このプロパティは、 SMB 1.0 経由で共有に接続するクライアントがある場合にのみ有効にしてください。クライアントが SMB 2.x または SMB 3.0 経由で共有に接続している場合、この共有プロパティは適用されません。
continuously-available	このプロパティは、サポートするSMBクライアントが永続的な方法でファイルを開くことを許可します。この方法で開いたファイルは、フェイルオーバーやギブバックなど、システムを停止させるイベントから保護されます。
branchcache	共有内のファイルに対するBranchCacheハッシュの要求をクライアントに許可します。このオプションが役立つのは、 CIFS の BranchCache 設定で動作モードとして「共有ごと」を指定した場合だけです。
access-based-enumeration	このプロパティは、この共有で _ アクセスベースの列挙 _ （ ABE ）を有効にするように指定します。ABEでフィルタリングされた共有フォルダは、個 々 のユーザのアクセス権に基づいてユーザに表示されるため、ユーザがアクセス権を持っていないフォルダやその他の共有リソースは表示されません。
namespace-caching	共有に接続するSMBクライアントが、CIFSサーバから返されるディレクトリの列挙結果をキャッシュできることを指定します。これにより、パフォーマンスが向上します。デフォルトでは、 SMB 1 のクライアントはディレクトリの列挙結果をキャッシュしません。SMB 2 および SMB 3 クライアントはデフォルトでディレクトリ列挙結果をキャッシュするため、この共有プロパティを指定してパフォーマンスが向上するのは SMB 1 クライアント接続のみです。
encrypt-data	この共有へのアクセス時にSMB暗号化を使用する必要があることを指定します。SMB データへのアクセスで暗号化をサポートしていない SMB クライアントは、この共有にアクセスできません。

既存の**SMB**共有に対する共有プロパティの追加または削除

共有プロパティを追加または削除することで、既存のSMB共有をカスタマイズできます。これは、環境内の要件の変化に合わせて共有設定を変更する場合に便利です。

開始する前に

プロパティを変更する共有が存在している必要があります。

タスクの内容

共有プロパティの追加に関するガイドラインは次のとおりです。

- カンマで区切って1つ以上の共有プロパティを追加できます。
- 以前に指定した共有プロパティは有効なままです。

  新しく追加したプロパティは、既存の共有プロパティのリストに追加されます。

- 共有にすでに適用されている共有プロパティに新しい値を指定した場合は、元の値が新たに指定した値に置き換えられます。
- コマンドを使用して共有プロパティを削除することはできません `vserver cifs share properties add`。

  共有プロパティを削除するには、コマンドを使用し `vserver cifs share properties remove`ます。

共有プロパティの削除に関するガイドラインは次のとおりです。

- カンマで区切って1つ以上の共有プロパティを削除できます。
- 以前に指定した共有プロパティは、削除しないかぎり有効なままです。

手順

1. 該当するコマンドを入力します。

状況	入力するコマンド
共有プロパティを追加する	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
共有プロパティを削除する	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 共有プロパティの設定を確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドを実行すると、SVM vs1上の「`share1`」という名前の共有に共有プロパティが追加され `showsnapshot`ます。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share1   /share1    oplocks      -          Everyone / Full
Control
                               browsable
                               changenotify
                               showsnapshot
```

次のコマンドは、SVM vs1上の「`share2'」という名前の共有から共有プロパティを削除し`browsable`ます。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share2   /share2    oplocks      -          Everyone / Full
Control
                               changenotify
```

関連情報

SMB共有の管理用コマンド

force-group共有設定を使用した**SMB**ユーザアクセスの最適化

ONTAP コマンドラインから、 UNIX 対応のセキュリティを使用するデータへの共有を作成するときに、 SMB ユーザがその共有内に作成するすべてのファイルが、 *force-group* と呼ばれる同じグループに属するように指定できます。このグループは、 UNIX グループデータベースで事前に定義されている必要があります。force-groupを使用すると、さまざまなグループに属するSMBユーザがファイルにアクセスできるようになります。

force-groupの指定が意味を持つのは、共有がUNIXまたはmixed qtree内にある場合のみです。NTFSボリュームまたはqtreeの共有内のファイルへのアクセスはUNIXのGIDではなくWindows権限によって決定されるため、これらの共有にforce-groupを設定する必要はありません。

共有にforce-groupが指定されている場合、共有は次のようになります。

- この共有にアクセスするforce-group内のSMBユーザは、force-groupのGIDに一時的に変更されます。

  このGIDを使用すると、プライマリGIDまたはUIDでは通常アクセスできない共有内のファイルにアクセスできます。

- SMBユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリGIDに関係なく、同じforce-groupに属します。

SMBユーザがNFSで作成されたファイルにアクセスしようとすると、SMBユーザのプライマリGIDによってアクセス権が決定されます。

force-groupは、NFSユーザがこの共有内のファイルにアクセスする方法には影響しません。NFSで作成されたファイルは、ファイル所有者からGIDを取得します。アクセス権限は、ファイルにアクセスしようとしているNFSユーザのUIDとプライマリGIDに基づいて決定されます。

force-groupを使用すると、さまざまなグループに属するSMBユーザがファイルにアクセスできるようになります。たとえば、会社の Web ページを保存する共有を作成し、 Engineering グループと Marketing グループのユーザに書き込みアクセス権を付与する必要がある場合、共有を作成して、「 webgroup1 」という名前の force-group に書き込み権限を与えます。force-group が指定されているため、 SMB ユーザがこの共有内に作成するすべてのファイルは「 webgroup1 」グループによって所有されます。また、ユーザが共有にアクセスするときは、「 webgroup1 」グループの GID が自動的に割り当てられます。その結果、すべてのユーザがこの共有に書き込むことができます。エンジニアリング部門とマーケティング部門のユーザのアクセス権を管理する必要はありません。

関連情報

force-group共有設定を使用したSMB共有の作成

force-group共有設定を使用して**SMB**共有を作成する

UNIXファイルセキュリティ形式のボリュームまたはqtree上のデータにアクセスするSMBユーザが、ONTAPで同じUNIXグループに属しているとみなされるようにするには、force-group共有設定を使用してSMB共有を作成します。

ステップ

1. SMB共有を作成します。 `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   (`\\servername\sharename\filepath`共有のUNCパスの文字数が256文字を超えている場合（UNCパスの先頭の""は除く\\）、Windowsの[プロパティ]ボックスの*[セキュリティ]*タブは使用できません。これは、ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないでください。

   共有の作成後にforce-groupを削除する場合は、いつでも共有を変更し、パラメータの値として空の文字列（""）を指定でき`-force-group-for-create`ます。共有を変更してforce-groupを削除した場合、この共有への既存のすべての接続には、引き続き以前に設定されたforce-groupがプライマリGIDとして使用されます。

例

次のコマンドは、SMBユーザが作成するすべてのファイルがwebgroup1グループに割り当てられるディレクトリに、Webからアクセス可能な「webpages」共有を作成し`/corp/companyinfo`ます。

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

関連情報

force-group共有設定を使用したSMBユーザアクセスの最適化

Microsoft 管理コンソール（ MMC ）を使用して SVM の SMB 共有情報を表示し、いくつかの管理タスクを実行できます。共有を表示する前に、 MMC を SVM に接続する必要があります。

タスクの内容

MMC を使用すると、 SVM 内の共有に対して次のタスクを実行できます。

- 共有を表示します
- アクティブなセッションを表示します
- 開いているファイルを表示します
- システムのセッション、ファイル、およびツリー接続のリストを列挙します
- 開いているファイルを閉じます
- 開いているセッションを閉じます
- 共有を作成 / 管理します

> 上記の機能によって表示されるビューは、クラスタではなくノードに固有のものです。そのため、 MMC を使用して SMB サーバホスト名（ cifs01.domain.local ）に接続すると、 DNS の設定に基づいてクラスタ内の単一の LIF にルーティングされます。

次の機能は、 MMC for ONTAP ではサポートされていません。

- 新しいローカルユーザ / グループを作成しています
- 既存のローカルユーザ / グループの管理 / 表示
- イベントまたはパフォーマンスログを表示する
- ストレージ
- サービスとアプリケーション

サポートされていない処理では、エラーが発生することがあり `remote procedure call failed`ます。

"FAQ ： ONTAP で Windows MMC を使用する"

手順

1. 任意の Windows サーバーでコンピュータの管理 MMC を開くには、 [コントロールパネル] で、 [管理ツール *]>[コンピュータの管理 *] を選択します。
2. 「 * アクション * > * 別のコンピューターに接続 * 」を選択します。

   [コンピュータの選択] ダイアログボックスが表示されます。
3. ストレージ・システムの名前を入力するか、または * Browse * をクリックしてストレージ・システムを検索します。
4. [OK]*をクリックします。

   MMC が SVM に接続します。

5. ナビゲーションペインで、 * 共有フォルダ * > * 共有 * をクリックします。

   右側の表示ペインに SVM の共有のリストが表示されます。

6. 共有の共有プロパティを表示するには、共有をダブルクリックして * プロパティ * ダイアログボックスを開きます。
7. MMC を使用してストレージシステムに接続できない場合は、ストレージシステムで次のいずれかのコマンドを使用して、 BUILTIN\Administrators グループまたは BUILTIN\Power Users グループにユーザを追加できます。

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

SMB共有の管理用コマンド

SMB共有を管理するには、コマンドと `vserver cifs share properties`コマンドを使用し `vserver cifs share`ます。

状況	使用するコマンド
SMB共有を作成する	`vserver cifs share create`
SMB共有を表示する	`vserver cifs share show`
SMB共有を変更する	`vserver cifs share modify`
SMB共有を削除する	`vserver cifs share delete`
既存の共有に共有プロパティを追加する	`vserver cifs share properties add`
既存の共有から共有プロパティを削除する	`vserver cifs share properties remove`
共有プロパティに関する情報を表示する	`vserver cifs share properties show`

詳細については、各コマンドのマニュアルページを参照してください。

SMB共有のACLを使用したファイルアクセスの保護

SMB共有レベルACLの管理に関するガイドライン

共有レベルの ACL を変更すると、共有に設定するアクセス権を強化したり、軽減したりできます。Windows のユーザとグループまたは UNIX のユーザとグループのいずれかを

使用して共有レベルの ACL を設定できます。

デフォルトでは、共有レベルのACLによって、Everyoneという名前の標準グループにフルコントロールが付与されます。ACLにフルコントロールを指定すると、ドメインおよびすべての信頼できるドメインのすべてのユーザに共有へのフルアクセスが許可されます。共有レベルACLのアクセスレベルは、を使用して制御できます"WindowsクライアントまたはONTAPコマンドライン上のMicrosoft管理コンソール（MMC）"。

MMC を使用する際には、次の点に留意してください。

- 指定するユーザ名およびグループ名はWindows名である必要があります。
- Windows の権限だけを指定できます。

ONTAP コマンドラインを使用する際には、次の点に留意してください。

- ユーザ名およびグループ名には、 Windows 名または UNIX 名を使用できます。

  ACL の作成時または変更時に指定されない場合、デフォルトのタイプは Windows のユーザとグループです。

- Windows の権限だけを指定できます。

SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List（ACL；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前、またはUNIXユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があり `Everyone / Full Control`ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。'vserver cifs share access-control delete -vserver <vserver_name>-share <share_name>-user-or-group everyone'
2. 新しいACLを設定します。

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIXユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIXグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com」SVM上の「sales」共有に対するWindowsグループ「sales Team」に権限を付与します `Change`。

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

次のコマンドは `Read`、「vs2.example.com」SVM上の「eng」共有に対して「engineering」UNIXグループに権限を付与します。

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

次のコマンドは `Change Full_Control`、SVM「vs1」上の「datavol5」共有に対して「Tiger Team」という名前のローカルWindowsグループに権限と「Sue Chang」という名前のローカルWindowsユーザに権限を付与します。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- -------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

SMB共有アクセス制御リストの管理用コマンド

Access Control List（ACL；アクセス制御リスト）の作成、表示、変更、削除など、SMBのAccess Control List（ACL；アクセス制御リスト）を管理するためのコマンドについて説明します。

状況	使用するコマンド
新しいACLを作成する	`vserver cifs share access-control create`
ACL を表示します	`vserver cifs share access-control show`
ACL を変更します	`vserver cifs share access-control modify`
ACL を削除します	`vserver cifs share access-control delete`

ファイル権限を使用したファイルアクセスの保護

Windowsの**[**セキュリティ**]**タブを使用した詳細な**NTFS**ファイル権限の設定

Windows の [プロパティ] ウィンドウの [Windows セキュリティ *] タブを使用して、ファイルおよびフォルダの標準 NTFS ファイルアクセス権を構成できます。

開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

タスクの内容

NTFSファイル権限を設定するには、Windowsホストで、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。これらのタスクはWindows GUIで自動的に処理されます。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * 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に入力します。
   a. ドライブ文字を選択します。
   b. [* フォルダ *] ボックスに、権限を適用するデータと共有名を含む共有を含む CIFS サーバー名を入力します。

      CIFSサーバ名が「CIFS_SERVER」で、共有の名前が「'share1'」の場合は、と入力します。
      `\\CIFS_SERVER\share1`

      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、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

3. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * 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。

   Security タブには、 NTFS アクセス権が設定されているユーザーおよびグループのリストが表示されます。[* アクセス許可の対象 *] ボックスには、選択した各ユーザーまたはグループに対して有効な [許可] と [拒否] のアクセス許可のリストが表示されます。

6. 「 * 詳細設定 * 」をクリックします。

   Windowsの[プロパティ]ウィンドウには、ユーザおよびグループに割り当てられている既存のファイル権限に関する情報が表示されます。

7. [権限の変更 *] をクリックします。

   [権限]ウィンドウが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループの詳細なNTFS権限を設定する	a. [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、追加するユーザー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の詳細なNTFS権限を変更する	a. [* アクセス権エントリ： *] ボックスで、詳細なアクセス権を変更するユーザーまたはグループを選択します。 b. [編集（ Edit ）] をクリックします。
ユーザまたはグループの詳細なNTFS権限を削除する	a. [* アクセス許可エントリ： *] ボックスで、削除するユーザーまたはグループを選択します。 b. [削除（ Remove ）] をクリックします。 c. 手順13に進みます。

   新しいユーザまたはグループに詳細な NTFS 権限を追加する場合、または既存のユーザまたはグループの NTFS 詳細権限を変更する場合は、 <Object> の権限エントリボックスが開きます。

9. [* 適用先 *] ボックスで、この NTFS ファイル許可エントリを適用する方法を選択します。

   1 つのファイルに NTFS ファイル権限を設定する場合、 * Apply to * ボックスはアクティブになりません。[* 適用先 * （ Apply to * ）] 設定のデフォルトは、 * このオブジェクトのみ * です。

10. [* アクセス許可 *] ボックスで、このオブジェクトに設定する詳細なアクセス許可の [* 許可 *] または [* 拒否 *] ボックスを選択します。

- 指定したアクセスを許可するには、 * 許可 * ボックスを選択します。
- 指定されたアクセスを許可しない場合は、 * Deny * ボックスを選択します。次の詳細な権限に対して権限を設定できます。
- * フルコントロール *

  この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます（それらの権限が許可または拒否されます）。

- * フォルダの移動 / ファイルの実行 *
- * フォルダのリスト / 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 *
- * 読み取り許可 *
- * 権限の変更 *
- * 所有権を取りなさい *

  いずれかの詳細な権限ボックスが選択できない場合は、権限が親オブジェクトから継承されるためです。

11. このオブジェクトのサブフォルダとファイルにこれらのアクセス権を継承させる場合は、 [このコンテナ内のオブジェクトまたはコンテナにこれらのアクセス権を適用する *] ボックスをオンにします。
12. [OK]*をクリックします。
13. NTFS権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。

    - [このオブジェクトの親から継承可能な権限を含める *] ボックスをオンにします。

      これがデフォルトです。

    - [このオブジェクトから継承可能な権限ですべての子オブジェクトを置換する *] ボックスをオンにします。

      この設定は、単一ファイルに対してNTFSファイル権限を設定する場合は[権限]ボックスに表示されません。

この設定を選択する場合は注意が必要です。この設定では、すべての子オブジェクトに対する既存の権限がすべて削除され、このオブジェクトの権限設定に置き換えられます。削除したくない権限を誤って削除する可能性があります。これは、mixedセキュリティ形式のボリュームまたはqtreeで権限を設定する場合に特に重要です。子オブジェクトがUNIX対応のセキュリティ形式を使用している場合に、これらの子オブジェクトにNTFSアクセス権を適用すると、ONTAPによってこれらのオブジェクトがUNIXセキュリティ形式からNTFSセキュリティ形式に変更され、これらの子オブジェクトのすべてのUNIXアクセス権がNTFSアクセス権に置き換えられます。

- 両方のボックスを選択します。
- どちらのボックスも選択しない。

14. **OK** をクリックして、 *Permissions * ボックスを閉じます。
15. OK * をクリックして、 * <Object>* の高度なセキュリティ設定ボックスを閉じます。

詳細なNTFS権限の設定方法の詳細については、Windowsのマニュアルを参照してください。

関連情報

CLIを使用したNTFSファイルおよびフォルダに対するファイルセキュリティの設定と適用

NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

mixedセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

UNIXセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

ONTAP CLIを使用した**NTFS**ファイル権限の設定

ONTAP CLIを使用して、ファイルおよびディレクトリに対してNTFSファイル権限を設定できます。これにより、WindowsクライアントでSMB共有を使用してデータに接続することなくNTFSファイル権限を設定できます。

NTFSファイル権限を設定するには、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。

コマンドラインを使用して設定できるのはNTFSファイル権限のみです。CLIを使用してNFSv4 ACLを設定することはできません。

手順

1. NTFSセキュリティ記述子を作成します。

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. NTFSセキュリティ記述子にDACLを追加します。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
```

```
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
{this-folder|sub-folders|files}
```

3. ファイルやディレクトリのセキュリティポリシーを作成します。

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

SMB経由でファイルにアクセスする際のUNIXファイル権限によるアクセス制御方法

FlexVol ボリュームのセキュリティ形式は、 NTFS 、 UNIX 、 mixed の 3 種類のいずれかにすることができます。セキュリティ形式に関係なく SMB 経由でデータにアクセスできますが、 UNIX 対応のセキュリティを使用するデータにアクセスするには、適切な UNIX ファイル権限が必要になります。

SMB 経由でのデータへのアクセス時には、いくつかのアクセス制御を使用して、要求した操作を実行する権限がユーザにあるかどうかが判断されます。

- エクスポート権限

  SMB アクセスに関するエクスポート権限の設定はオプションです。

- 共有権限
- ファイル権限

  ユーザが操作を実行するデータには、次のタイプのファイル権限を適用できます。

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX モードビット

NFSv4 ACL または UNIX モードビットが設定されたデータの場合は、 UNIX 形式のアクセス権を使用してデータへのファイルアクセス権が決定されます。SVM 管理者は、適切なファイル権限を設定して、ユーザに目的のアクションを実行する権限が付与されるようにする必要があります。

> mixed セキュリティ形式のボリューム内のデータでは、 NTFS または UNIX 対応のセキュリティ形式を使用できます。UNIX 対応のセキュリティ形式を使用するデータの場合は、データに対するファイル権限を判断するときに NFSv4 権限または UNIX モードビットが使用されます。

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護の概要

ダイナミックアクセス制御を使用してアクセスを保護できます。Active Directoryで集約型アクセスポリシーを作成し、適用されたGPOを使用してSVM上のファイルとフォルダにそのポリシーを適用します。集約型アクセスポリシーのステージングイベントを使用するように監査を設定すると、集約型アクセスポリシーの変更を適用する前にその影響を確認できます。

CIFSクレデンシャルへの追加

ダイナミックアクセス制御が導入される前は、CIFSクレデンシャルにセキュリティプリンシパル（ユーザ）のIDとWindowsグループメンバーシップが含まれていました。ダイナミックアクセス制御では、さらに3種類の情報（デバイスID、デバイス要求、およびユーザ要求）がクレデンシャルに追加されます。

- デバイスID

  ユーザーのID情報と類似していますが、ユーザーがログインしているデバイスのIDとグループメンバーシップが異なります。

- デバイスの信頼性

  デバイスセキュリティプリンシパルに関するアサーション。たとえば、デバイスが特定のOUのメンバーであることが要求される場合があります。

- ユーザの信頼性

  ユーザセキュリティプリンシパルに関するアサーション。たとえば、ADアカウントが特定のOUのメンバーであることをユーザが要求する場合があります。

集約型アクセスポリシー

ファイルの集約型アクセスポリシーを使用すると、ユーザグループ、ユーザ要求、デバイス要求、およびリソースプロパティを使用した条件式を含む許可ポリシーを一元的に導入および管理できます。

たとえば、ビジネスに影響の大きいデータにアクセスするには、フルタイムの従業員であり、管理対象デバイスからのみデータにアクセスできる必要があります。集約型アクセスポリシーはActive Directoryで定義され、GPOメカニズムを介してファイルサーバに配布されます。

高度な監査を使用した集約型アクセスポリシーのステージング

集約型アクセスポリシーは「集約型」にすることができます。この場合、ファイルアクセスチェック時に「what if 」方式で評価されます。ポリシーが有効になっていた場合に発生した結果、および現在の設定とどのように異なるかが監査イベントとして記録されます。このようにして、管理者は、実際にポリシーを有効にする前に、監査イベントログを使用してアクセスポリシーの変更による影響を調べることができます。アクセスポリシーの変更による影響を評価したら、GPOを使用して目的のSVMにポリシーを導入できます。

関連情報

サポートされるGPO

CIFSサーバへのグループ ポリシー オブジェクトの適用

CIFSサーバでのGPOサポートの有効化と無効化

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

CIFSサーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御セキュリティに関する情報の表示

"SMBおよびNFSの監査とセキュリティトレース"

サポートされるダイナミックアクセス制御機能

CIFSサーバでダイナミックアクセス制御（DAC）を使用する場合は、ONTAPがActive Directory環境でどのようにダイナミックアクセス制御機能をサポートするかを理解しておく必要があります。

ダイナミックアクセス制御でサポート

CIFSサーバでダイナミックアクセス制御が有効になっている場合、ONTAPは次の機能をサポートします。

機能	コメント
ファイルシステムへの要求	クレームは単純な名前と値のペアで、ユーザーについての真実を記述します。ユーザクレデンシャルにはクレーム情報が含まれており、ファイルのセキュリティ記述子はクレームチェックを含むアクセスチェックを実行できます。これにより、管理者は誰がファイルにアクセスできるかをより細かく制御できます。
ファイルアクセスチェック用の条件式	ファイルのセキュリティパラメータを変更する場合、ユーザは任意に複雑な条件式をファイルのセキュリティ記述子に追加できます。条件式には、クレームのチェックを含めることができます。
集約型アクセスポリシーによるファイルアクセスの一元管理	集約型アクセスポリシーは、Active Directoryに格納されるACLの一種で、ファイルへのタグ付けが可能です。ファイルへのアクセスは、ディスクのセキュリティ記述子とタグ付けされた集約型アクセスポリシーの両方のアクセスチェックでアクセスが許可されている場合にのみ許可されます。これにより、管理者は、ディスクのセキュリティ記述子を変更することなく、一元的な場所（AD）からファイルへのアクセスを制御できます。
集約型アクセスポリシーのステージング	集約型アクセスポリシーへの変更を「集約型アクセスポリシー」し、監査レポートで変更の影響を確認することで、実際のファイルアクセスに影響を与えずにセキュリティの変更を試す機能を追加します。
ONTAP CLIを使用した集約型アクセスポリシーセキュリティに関する情報の表示のサポート	コマンドを拡張し `vserver security file-directory show`て、適用されている集約型アクセスポリシーに関する情報を表示します。

機能	コメント
集約型アクセスポリシーを含むセキュリティトレース	コマンドファミリーを拡張し、`vserver security trace`適用されている集約型アクセスポリシーに関する情報を含む結果を表示します。

ダイナミックアクセス制御でサポートされない

CIFSサーバでダイナミックアクセス制御が有効になっている場合、ONTAPは次の機能をサポートしません。

機能	コメント
NTFSファイルシステムオブジェクトの自動分類	これは、ONTAPでサポートされていないWindowsファイル分類インフラストラクチャの拡張機能です。
集約型アクセスポリシーのステージング以外の高度な監査	高度な監査では、集約型アクセスポリシーのステージングのみがサポートされます。

CIFSサーバでダイナミックアクセス制御と集約型アクセスポリシーを使用する際の考慮事項

CIFS サーバ上のファイルとフォルダを保護するために Dynamic Access Control （ DAC ；ダイナミックアクセス制御）と集約型アクセスポリシーを使用する際は、一定の考慮事項に注意する必要があります。

ポリシールール「環境 **domain\administrator user** 」の場合、 **root** に対して **NFS** アクセスが拒否されることがあります

特定の状況では、 root ユーザがアクセスしようとしているデータに集約型アクセスポリシーセキュリティが適用されていると、 root に対して NFS アクセスが拒否されることがあります。問題は、集約型アクセスポリシーに domain\administrator に適用されるルールが含まれており、 root アカウントが domain\administrator アカウントにマッピングされている場合に実行されます。

domain\administrator ユーザにルールを適用する代わりに、 domain\administrators グループなど、管理者権限を持つグループにルールを適用してください。これにより、 root を domain\administrator アカウントにマッピングしても、 root はこの問題の影響を受けなくなります。

適用された集約型アクセスポリシーが**Active Directory**に見つからないと、**CIFS**サーバの**BUILTIN\Administrators**グループにリソースへのアクセスが許可されます

CIFS サーバに格納されたリソースに集約型アクセスポリシーが適用されている場合に、 CIFS サーバが集約型アクセスポリシーの SID を使用して Active Directory から情報を取得しようとしても、 SID が Active Directory 内の既存の集約型アクセスポリシーの SID と一致しないことがあります。このような場合、 CIFS サーバはそのリソースにローカルのデフォルトのリカバリポリシーを適用します。

ローカルのデフォルトのリカバリポリシーでは、 CIFS サーバの BUILTIN\Administrators グループにそのリソースへのアクセスが許可されます。

ダイナミックアクセス制御の有効化または無効化の概要

ダイナミックアクセス制御（DAC）を使用してCIFSサーバ上のオブジェクトを保護でき

るオプションは、デフォルトでは無効になっています。CIFSサーバでダイナミックアクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFSサーバに格納されたオブジェクトの保護にダイナミックアクセス制御を使用しない場合は、オプションを無効にすることができます。

タスクの内容

ダイナミックアクセス制御を有効にすると、ダイナミックアクセス制御関連のエントリを含むACLをファイルシステムに含めることができます。ダイナミックアクセス制御を無効にすると、現在のダイナミックアクセス制御エントリは無視され、新しいエントリは許可されません。

このオプションは、advanced権限レベルでのみ使用できます。

ステップ

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ダイナミックアクセス制御の設定	入力するコマンド
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
無効にする	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 管理者権限レベルに戻ります。 `set -privilege admin`

関連情報

CIFSサーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御が無効な場合にダイナミックアクセス制御**ACE**を含む**ACL**を管理します。

ダイナミックアクセス制御ACEが適用されたACLが設定されたリソースがある場合にStorage Virtual Machine（SVM）でダイナミックアクセス制御を無効にすると、ダイナミックアクセス制御ACEを削除してから、そのリソースの非ダイナミックアクセス制御ACEを管理する必要があります。

タスクの内容

ダイナミックアクセス制御を無効にした場合、既存のダイナミックアクセス制御 ACE を削除するまでは、既存の非ダイナミックアクセス制御 ACE の削除や新しい非ダイナミックアクセス制御 ACE の追加はできません。

これらの手順は、通常 ACL の管理に使用している任意のツールを使用して実行できます。

手順

1. リソースに適用されているダイナミックアクセス制御 ACE を確認します。
2. リソースからダイナミックアクセス制御 ACE を削除します。

3. 必要に応じて、リソースに対して非ダイナミックアクセス制御 ACE を追加または削除します。

CIFSサーバ上のデータを保護する集約型アクセスポリシーを設定する

集約型アクセスポリシーを使用してCIFSサーバ上のデータへのアクセスを保護するには、CIFSサーバでのダイナミックアクセス制御（DAC）の有効化、Active Directoryでの集約型アクセスポリシーの設定、GPOを含むActive Directoryコンテナへの集約型アクセスポリシーの適用、CIFSサーバでのGPOの有効化など、いくつかの手順を実行する必要があります。

開始する前に

- 集約型アクセスポリシーを使用するようにActive Directoryを設定する必要があります。
- 集約型アクセスポリシーを作成し、CIFSサーバを含むコンテナにGPOを作成して適用するには、Active Directoryドメインコントローラに対する十分なアクセスが必要です。
- 必要なコマンドを実行するには、Storage Virtual Machine（SVM）に対する十分な管理アクセスが必要です。

タスクの内容

集約型アクセスポリシーは、Active Directoryのグループポリシーオブジェクト（GPO）に定義されて適用されます。集約型アクセスポリシーとGPOの設定手順については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNetライブラリ"

手順

1. コマンドを使用して、SVMのダイナミックアクセス制御を有効にしていない場合は有効にし `vserver cifs options modify`ます。

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. コマンドを使用して、CIFSサーバでグループポリシーオブジェクト（GPO）を有効にしていない場合は有効にし `vserver cifs group-policy modify`ます。

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Active Directoryで集約型アクセスルールと集約型アクセスポリシーを作成します。
4. グループポリシーオブジェクト（GPO）を作成して、Active Directoryに集約型アクセスポリシーを導入します。
5. CIFSサーバのコンピュータアカウントが配置されているコンテナにGPOを適用します。
6. コマンドを使用して、CIFSサーバに適用されたGPOを手動で更新します `vserver cifs group-policy update`。

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. コマンドを使用して、CIFSサーバ上のリソースにGPO集約型アクセスポリシーが適用されていることを確認します `vserver cifs group-policy show-applied`。

   次の例は、デフォルトのドメインポリシーに2つの集約型アクセスポリシーがあり、それらがCIFSサーバ

に適用されていることを示しています。

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
------------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
```

```
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

関連情報

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

ダイナミックアクセス制御の有効化と無効化

ダイナミックアクセス制御セキュリティに関する情報を表示する

NTFSボリューム、およびmixedセキュリティ形式のボリューム上のNTFS対応セキュリティを使用するデータのダイナミックアクセス制御（DAC）セキュリティに関する情報を表示できます。これには、条件付きACE、リソースACE、集約型アクセスポリシーACEに関する情報が含まれます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
出力にはグループSIDとユーザSIDが表示されます。	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
16進数のビットマスクがテキスト形式に変換されるファイルおよびディレクトリのファイルおよびディレクトリのセキュリティについて	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

例

次の例では、SVM vs1のパスに関するダイナミックアクセス制御セキュリティの情報を表示します `/vol1`。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

関連情報

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

ダイナミックアクセス制御のリバートに関する考慮事項

ダイナミックアクセス制御（ DAC ）をサポートしないバージョンの ONTAP にリバートする場合に発生する状況と、リバートの前後に必要な処理を把握しておく必要があります。

ダイナミックアクセス制御がサポートされていないバージョンの ONTAP にクラスタをリバートし、 1 つ以上の Storage Virtual Machine （ SVM ）でダイナミックアクセス制御が有効になっている場合、リバート前に次の処理を実行する必要があります。

- クラスタでダイナミックアクセス制御が有効になっているすべての SVM で、ダイナミックアクセス制御を無効にする必要があります。
- イベントタイプを含むクラスタでは、イベントタイプのみを使用するように `file-op`監査の設定を変更する必要があります `cap-staging`。

ダイナミックアクセス制御 ACE が設定されているファイルやフォルダについて、リバートに関する重要な考慮事項を理解し、対応する必要があります。

- クラスタをリバートした場合、既存のダイナミックアクセス制御 ACE は削除されませんが、ファイルアクセスチェックで無視されます。
- リバート後はダイナミックアクセス制御 ACE は無視されるため、ダイナミックアクセス制御 ACE が設定されたファイルへのアクセスには変更が発生します。

  これにより、ユーザは以前にアクセスできなかったファイルにアクセスできるようになり、以前にアクセスできたファイルにアクセスできなくなる可能性があります。

- 以前のセキュリティレベルに戻すには、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する必要があります。

  この処理は、リバート前またはリバート完了直後に実行できます。

> リバート後はダイナミックアクセス制御 ACE は無視されるため、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する際にダイナミックアクセス制御 ACE を削除する必要はありません。ただし、必要に応じて手動で削除することもできます。

ダイナミックアクセス制御と集約型アクセスポリシーの設定および使用に関する詳細情報の参照先

ダイナミックアクセス制御と集約型アクセスポリシーを設定および使用する方法については、その他のリソースを参照してください。

Active Directoryに対するダイナミックアクセス制御と集約型アクセスポリシーの設定方法については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNet ：「ダイナミックアクセス制御のシナリオの概要"

"Microsoft TechNet ：「集約型アクセスポリシーのシナリオ"

ダイナミックアクセス制御と集約型アクセスポリシーを使用してサポートするようにSMBサーバを設定するには、次の資料を参照することができます。

- * SMBサーバーでのGPOの使用*

  SMBサーバへのグループポリシーオブジェクトの適用

- * SMBサーバでのNAS監査の設定*

"SMBおよびNFSの監査とセキュリティトレース"

エクスポートポリシーを使用したSMBアクセスの保護

SMBアクセスでのエクスポートポリシーの使用方法

SMBサーバでSMBアクセスのエクスポートポリシーが有効になっている場合は、SMBクライアントによるSVMボリュームへのアクセスを制御する際にエクスポートポリシーが使用されます。データにアクセスするには、SMBアクセスを許可するエクスポートポリシーを作成し、SMB共有を含むボリュームにそのポリシーを関連付けます。

エクスポートポリシーには、データへのアクセスを許可するクライアント、および読み取り専用アクセスと読み取り/書き込みアクセスでサポートされる認証プロトコルを指定するルールが1つ以上適用されます。エクスポートポリシーを設定して、すべてのクライアント、クライアントのサブネット、または特定のクライアントにSMB経由のアクセスを許可し、データへの読み取り専用アクセスと読み取り/書き込みアクセスを決定する際にKerberos認証、NTLM認証、またはKerberosとNTLMの両方を使用した認証を許可できます。

ONTAPは、エクスポートポリシーに適用されたすべてのエクスポートルールを処理したあと、クライアントにアクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポートルールは、Windowsのユーザおよびグループではなく、クライアントマシンに適用されます。エクスポートルールは、Windowsのユーザおよびグループベースの認証および許可に代わるものではありません。エクスポートルールは、共有権限とファイルアクセス権限に加えて、アクセスセキュリティのもう1つのレイヤを提供します。

ボリュームへのクライアントアクセスを設定するには、ボリュームごとにエクスポートポリシーを1つ関連付けます。各 SVM には複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームを備えた SVM に対して次の操作を実行できます。

- SVM のボリュームごとに異なるエクスポートポリシーを割り当て、 SVM の各ボリュームへのクライアントアクセスを個別に制御する。
- SVM の複数のボリュームに同じエクスポートポリシーを割り当て、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。

各 SVM には、「デフォルト」という名前のエクスポートポリシーが少なくとも 1 つあります。これにはルールは含まれません。このエクスポートポリシーは削除できませんが、名前や変更は可能です。デフォルトでは、 SVM 上の各ボリュームはデフォルトのエクスポートポリシーに関連付けられています。SVM で SMB アクセスのエクスポートポリシーが無効になっている場合、「 default 」エクスポートポリシーは SMB アクセスには影響しません。

NFSホストとSMBホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポートポリシーに関連付けることができます。エクスポートポリシーを、NFSホストとSMBホストの両方がアクセスする必要があるデータが格納されたボリュームに関連付けることができます。または、SMBクライアントのみがアクセスを必要とするボリュームがある場合は、SMBプロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証にKerberosまたはNTLMのみ（またはその両方）を使用するルールを含むエクスポートポリシーを設定できます。その後、このエクスポートポリシーをSMBアクセスのみが必要なボリュームに関連付けます。

SMBのエクスポートポリシーが有効になっている場合に、クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示されて要求は失敗します。クライアントがボリュームのエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポートポリシーが空の場合、すべてのアクセスが暗黙的に拒否されます。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、SMB共有を含むボリュームで少なくと

も以下を許可するようにエクスポートポリシーを設定する必要があります。

- すべてのクライアントまたは適切なクライアントサブセットへのアクセスを許可する
- SMB経由のアクセスを許可する
- Kerberos認証またはNTLM認証（またはその両方）を使用して、適切な読み取り専用アクセスと書き込みアクセスを許可する

詳細はこちらをご覧ください "エクスポートポリシーの設定と管理"。

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、ボリュームへのクライアントアクセス要求が設定した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、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。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序で処理されます。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した場合、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用してクライアントアクセス権限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）。

  フィールドの最大サイズ `-clientmatch`は4096文字です。

- 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いる場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

例
エクスポートポリシーには、次のパラメータを持つ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が一致していても、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サブネットとは異なるサブネットに属しています。そのため、クライアント一致は失敗し、このルールはこのクライアントには適用されません。

例

エクスポートポリシーには、次のパラメータを持つ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アドレスが指定したサブネットにあります。したがって、クライアント一致は成功し、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は、次のパラメータを持つ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。

両方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アドレスが一致している。読み取り専用パラメータでは、認証に使用し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が許可されます。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クライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

SMB経由のアクセスを制限または許可するエクスポートポリシールールの例

以下の例は、 SMB アクセスのエクスポートポリシーが有効になっている SVM で SMB 経由のアクセスを制限または許可するエクスポートポリシールールを作成する方法を示しています。

SMB アクセスに関するエクスポートポリシーは、デフォルトでは無効になっています。SMB 経由のアクセスを制限または許可するエクスポートポリシールールは、 SMB アクセスのエクスポートポリシーを有効にしている場合にのみ設定する必要があります。

SMB アクセスのみのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifs1
- インデックス番号： 1.
- クライアント一致： 192.168.1.0/24 ネットワーク上のクライアントにのみ一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM 認証または Kerberos 認証を使用するクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証を使用するクライアントに許可します

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB および **NFS** アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifsnfs1
- インデックス番号： 2.
- クライアント一致：すべてのクライアントに一致します
- プロトコル： SMB アクセスと NFS アクセス
- 読み取り専用アクセス：すべてのクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証（ NFS および SMB ）または NTLM 認証（ SMB ）を使用するクライアントに許可
- UNIX ユーザ ID 0 （ゼロ）のマッピング：ユーザ ID 65534 （通常ユーザ名 nobody にマッピングされる）にマッピング
- suid と sgid のアクセス：許可しています

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

NTLM のみを使用する **SMB** アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：ntlm1
- インデックス番号： 1.
- クライアント一致：すべてのクライアントに一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM を使用するクライアントにのみ許可されます

- 読み取り / 書き込みアクセス： NTLM を使用するクライアントにのみ許可されます

> NTLM のみを使用するアクセスに読み取り専用オプションまたは読み取り / 書き込みオプションを設定する場合は、クライアント一致オプションで IP アドレスベースのエントリを使用する必要があります。そうしないと、エラーが発生し `access denied`ます。これは、 ONTAP がホスト名を使用してクライアントの権限を確認するときに、 Kerberos Service Principal Name （ SPN ；サービスプリンシパル名）を使用するためです。NTLM 認証では、 SPN 名はサポートされません。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

SMBアクセスに関するエクスポートポリシーの有効化または無効化

Storage Virtual Machine （ SVM ）での SMB アクセスに関するエクスポートポリシーを有効または無効にすることができます。エクスポートポリシーを使用したリソースへの SMB アクセスの制御はオプションです。

開始する前に

SMB のエクスポートポリシーを有効にするための要件は次のとおりです。

- クライアントのエクスポートルールを作成する前に、そのクライアントの「 PTR 」レコードが DNS に登録されている必要があります。
- SVM が NFS クライアントにアクセスを提供し、 NFS アクセスに使用するホスト名が CIFS サーバ名と異なる場合は、ホスト名に対して「 A 」レコードと「 PTR 」レコードのセットが追加で必要です。

タスクの内容

SVM に新しい CIFS サーバをセットアップするとき、 SMB アクセスに関するエクスポートポリシーの使用はデフォルトで無効になります。認証プロトコル、クライアント IP アドレス、またはホスト名に基づいてアクセスを制御する場合は、 SMB アクセスのエクスポートポリシーを有効にできます。SMB アクセスに関するエクスポートポリシーはいつでも有効または無効にできます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. エクスポートポリシーを有効または無効にします。
   - エクスポートポリシーを有効にします。 `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled true`
   - エクスポートポリシーを無効にします。 `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled false`
3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、エクスポートポリシーを使用したSVM vs1上のリソースへのSMBクライアントアクセスの制御を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

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

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

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 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：すべての NAS プロトコルから適用されるストレージオブジェクトへの環境アクセスを保護します。

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

ストレージレベルのアクセス保護の動作

- ストレージレベル環境のアクセス保護：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を保護します。

  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、ボリューム内のファイルのみ、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とファイルを環境に格納します。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を環境します。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には影響しません。

  - 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を環境します。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には影響しません。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

- 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。

  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 SVM で CIFS サーバが設定されている場合に限られます。
- ボリュームがボリュームジャンクションパス以下にマウントされていて、そのパスにストレージレベルのアクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。
- 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 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れらのサーバに対しては、ストレージレベルのアクセス保護によってオブジェクトへのアクセスが拒否されていても、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。

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権限の各影響の組み合わせによって決まります。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/フォルダのAccess Control List（ACL；アクセス制御リスト）、NFSv4 ACL、またはUNIXモードビット

ストレージレベルのアクセス保護の使用のユースケース

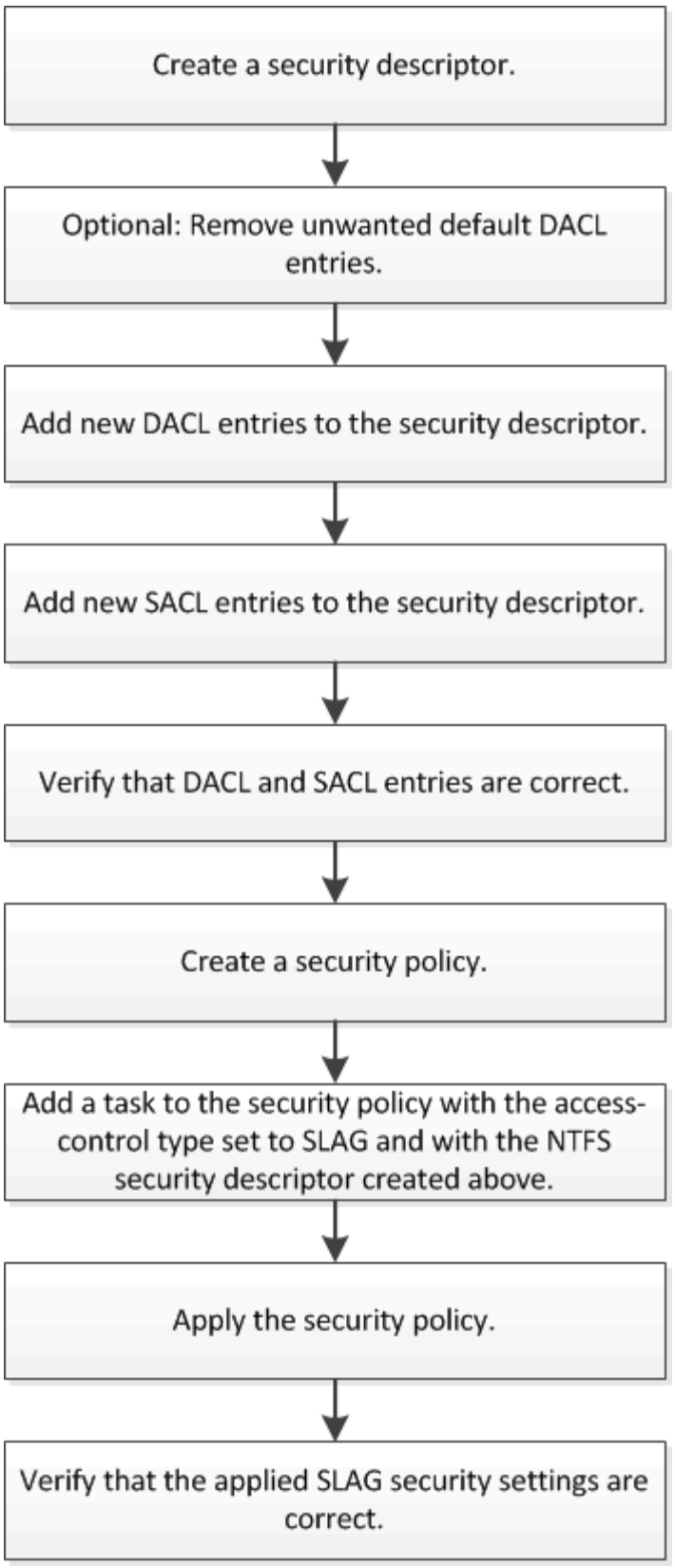
ストレージレベルのアクセス保護は、ストレージレベルでの追加セキュリティを提供します。このセキュリティはクライアント側からは見えないため、ユーザや管理者がデスクトップから取り消すことはできません。一部のユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

この機能の一般的なユースケースとしては、次のようなシナリオがあります。

- すべてのユーザーのアクセスをストレージ・レベルで監査および制御することにより ' 知的財産を保護します
- 銀行や証券会社など、金融サービス企業のストレージの場合
- 部門ごとに個別のファイルストレージを使用する行政サービス
- すべての学生のファイルを保護する大学

ストレージレベルのアクセス保護の設定ワークフロー

ストレージレベルのアクセス保護（SLAG）を設定するワークフローでは、NTFSファイル権限と監査ポリシーの設定に使用するONTAP CLIコマンドと同じコマンドを使用します。対象のファイルやディレクトリのアクセスを設定する代わりに、対象のStorage Virtual Machine（SVM）ボリュームのSLAGを設定します。



関連情報

ストレージレベルのアクセス保護の設定

ボリュームまたはqtreeにストレージレベルのアクセス保護を設定するには、いくつかの手順に従う必要があります。ストレージレベルのアクセス保護は、ストレージレベルで設定されるアクセスセキュリティのレベルを提供します。すべてのNASプロトコルから適用先のストレージオブジェクトへのすべてのアクセスに適用されるセキュリティを提供します。

手順

1. コマンドを使用して、セキュリティ記述子を作成し `vserver security file-directory ntfs create`ます。

   ```
   vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver
   security file-directory ntfs show -vserver vs1
   ```

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   セキュリティ記述子は、次の4つのデフォルトDACL Access Control Entry（ACE；アクセス制御エントリ）で作成されます。

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   ストレージレベルのアクセス保護の設定時にデフォルトのエントリを使用しない場合は、セキュリティ記述子に独自のACEを作成して追加する前に、デフォルトのエントリを削除できます。

2. セキュリティ記述子から、ストレージレベルのアクセス保護セキュリティで設定したくないデフォルト

のDACL ACEを削除します。

a. コマンドを使用して、不要なDACL ACEを削除します `vserver security file-directory ntfs dacl remove`。

   この例では、セキュリティ記述子から BUILTIN\Administrators 、 BUILTIN\Users 、 CREATOR OWNER の 3 つのデフォルト DACL ACE を削除しています。

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. コマンドを使用して、ストレージレベルのアクセス保護セキュリティに使用しないDACL ACEがセキュリティ記述子から削除されたことを確認します `vserver security file-directory ntfs dacl show`。

   この例では、コマンドの出力によって、3つのデフォルトDACL ACEがセキュリティ記述子から削除され、NT AUTHORITY\SYSTEMデフォルトDACL ACEエントリのみが残されていることが確認されます。

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access           Apply To
                     Type     Rights
    --------------   -------  -------          -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. コマンドを使用して、セキュリティ記述子に1つ以上のDACLエントリを追加します `vserver security file-directory ntfs dacl add`。

   この例では、セキュリティ記述子に2つのDACL ACEを追加しています。

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. コマンドを使用して、セキュリティ記述子に1つ以上のSACLエントリを追加します `vserver security file-directory ntfs sacl add`。

   この例では、セキュリティ記述子に2つのSACL ACEを追加しています。

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. コマンドと `vserver security file-directory ntfs sacl show`コマンドを使用して、DACL ACEとSACL ACEがそれぞれ正しく設定されていることを確認します `vserver security file-directory ntfs dacl show。

   この例では、次のコマンドを実行すると、セキュリティ記述子「`d1"」の DACL エントリに関する情報が表示されます。

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   この例では、次のコマンドを実行すると、セキュリティ記述子「`d1"」の SACL エントリに関する情報が表示されます。

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. コマンドを使用して、セキュリティポリシーを作成し `vserver security file-directory policy create`ます。

   次に、「 policy1 」という名前のポリシーを作成する例を示します。

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. コマンドを使用して、ポリシーが正しく設定されていることを確認します `vserver security file-directory policy show`。

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. コマンドでパラメータをに設定 `slag`して `-access-control`、セキュリティ記述子が関連付けられたタスクをセキュリティポリシーに追加します `vserver security file-directory policy task add`。

   ポリシーには複数のストレージレベルのアクセス保護タスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

   この例では ' セキュリティー記述子 "`d1" に割り当てられている "policy1 " という名前のポリシーにタスクが追加されますアクセス制御タイプが「`slag」に設定されたパスに割り当てられ `/datavol1`ます。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. コマンドを使用して、タスクが正しく設定されていることを確認します `vserver security file-directory policy task show`。

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. コマンドを使用して、ストレージレベルのアクセス保護セキュリティポリシーを適用し `vserver security file-directory apply`ます。

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    セキュリティポリシーを適用するジョブがスケジュールされます。

11. コマンドを使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認し `vserver security file-directory show`ます。

    この例では、コマンドの出力から、ストレージレベルのアクセス保護セキュリティがNTFSボリュームに適用されていることがわかります `/datavol1`。Everyoneにフルコントロールを許可するデフォルトのDACLは残っていますが、ストレージレベルのアクセス保護セキュリティは、ストレージレベルのアクセス保護設定で定義されたグループへのアクセスを制限（および監査）します。

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

関連情報

CLIを使用したSVMのNTFSファイルセキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理

ストレージレベルのアクセス保護の設定ワークフロー

ストレージレベルのアクセス保護に関する情報の表示

SLAGノテキヨウニカンスルマトリックス

SLAG は、ボリューム、 qtree 、またはその両方に対して設定できます。次の表に、さまざまな状況について、ボリュームまたは qtree に SLAG 構成を適用できるかどうかを示します。

	AFS 内のボリューム **SLAG**	**Snapshot** コピー内のボリューム **SLAG**	**AFS** 内の **qtree SLAG**	**Snapshot** コピー内の **qtree SLAG**
AFS 内のボリュームへのアクセス	はい	いいえ	N/A	N/A
Snapshot コピー内のボリュームへのアクセス	はい	いいえ	N/A	N/A
AFS 内の qtree へのアクセス（ qtree に SLAG が設定されている場合）	いいえ	いいえ	はい	いいえ
AFS 内の qtree へのアクセス（ qtree に SLAG が設定されていない場合）	はい	いいえ	いいえ	いいえ
Snapshot コピー内の qtree へのアクセス（ qtree に SLAG が設定されている場合）	いいえ	いいえ	はい	いいえ
Snapshot コピー内の qtree へのアクセス（ qtree に SLAG が設定されていない場合）	はい	いいえ	いいえ	いいえ

ストレージレベルのアクセス保護に関する情報を表示する

ストレージレベルのアクセス保護は、ボリュームまたは qtree に適用される 3 番目のセキュリティレイヤです。ストレージレベルのアクセス保護設定は、 Windows のプロパティウィンドウでは表示できません。ストレージレベルのアクセス保護セキュリティに関する情報を表示するには、 ONTAP CLI を使用する必要があります。この情報を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができ

ます。

タスクの内容

Storage Virtual Machine （ SVM ）の名前、およびストレージレベルのアクセス保護セキュリティ情報を表示するボリュームまたは qtree のパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

ステップ

1. ストレージレベルのアクセス保護セキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細を表示	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1のパスにあるNTFSセキュリティ形式のボリュームのストレージレベルのアクセス保護セキュリティ情報を表示します `/datavol1`。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

次の例では、SVM vs1のパスにあるmixedセキュリティ形式のボリュームに関するストレージレベルのアクセス保護の情報を表示します `/datavol5`。このボリュームの最上位には、 UNIX 対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ストレージレベルのアクセス保護の削除

ストレージレベルのアクセスセキュリティの設定が不要になった場合は、ボリュームやqtree からストレージレベルのアクセス保護を削除できます。ストレージレベルのアクセス保護を削除しても、通常の NTFS のファイルやディレクトリのセキュリティは変更されたり削除されたりしません。

手順

1. コマンドを使用して、ボリュームまたはqtreeにストレージレベルのアクセス保護が設定されていることを確認します `vserver security file-directory show`。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. コマンドを使用して、ストレージレベルのアクセス保護を削除します `vserver security file-directory remove-slag`。

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. コマンドを使用して、ボリュームまたはqtreeからストレージレベルのアクセス保護が削除されたことを確認します `vserver security file-directory show`。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

SMBを使用したファイルアクセスの管理

ローカルユーザとローカルグループを認証と許可に使用する

ONTAPでのローカルユーザとローカルグループの使用方法

ローカルユーザとローカルグループの概念

環境でローカルユーザとローカルグループを設定して使用するかどうかを決定する前に、ローカルユーザとローカルグループとは何か、およびそれらに関するいくつかの基本情報を把握しておく必要があります。

- * ローカルユーザー *

  一意のSecurity Identifier（SID；セキュリティ識別子）を持つユーザアカウント。そのユーザアカウントを作成したStorage Virtual Machine（SVM）上でのみ認識されます。ローカルユーザアカウントには、ユーザ名やSIDなどの一連の属性があります。ローカルユーザアカウントは、NTLM認証を使用してCIFSサーバ上でローカルに認証されます。

  ユーザアカウントには次のような用途があります。

  - ユーザに _ ユーザ権限の管理 _ 権限を付与するために使用します。
  - SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

- * ローカルグループ *

  一意のSIDを持つグループは、そのグループを作成したSVM上でのみ認識されます。グループには一連のメンバーが含まれます。メンバーには、ローカルユーザ、ドメインユーザ、ドメイングループ、およびドメインマシンアカウントを指定できます。グループは作成、変更、または削除できます。

  グループにはいくつかの用途があります。

  - メンバーに _User Rights Management_Privileges を付与するために使用します。
  - SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

- * ローカルドメイン *

  ローカルスコープを持つドメイン。SVMでバインドされています。ローカルドメインの名前はCIFSサーバの名前です。ローカルユーザとローカルグループはローカルドメイン内に格納されます。

- * Security Identifier （ SID ；セキュリティ識別子） *

  SIDは可変長の数値で、Windows形式のセキュリティプリンシパルを識別します。たとえば、通常の SID の場合は、次のような形式になります。 S-1-5-21-3139654847-1303905135-2517279418-123456 。

- * NTLM 認証 *

  CIFSサーバでユーザを認証するために使用されるMicrosoft Windowsのセキュリティ方式。

- * 複製されたクラスタデータベース（ RDB ） *

  クラスタ内の各ノードにインスタンスがあるレプリケートされたデータベース。ローカルユーザオブジェクトとローカルグループオブジェクトはRDBに格納されます。

ローカルユーザおよびローカルグループを作成する理由

Storage Virtual Machine（SVM）でローカルユーザやローカルグループを作成する理由はいくつかあります。たとえば、ドメインコントローラ（DC）を使用できない場合でも、ローカルユーザアカウントを使用してSMBサーバにアクセスできます。また、ローカルグループを使用してPrivilegesを割り当てたり、SMBサーバがワークグループに含まれている場合もあります。

ローカルユーザアカウントを作成する理由は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメインユーザを使用できません。

  ワークグループを設定するにはローカルユーザが必要です。

- ドメインコントローラを使用できない場合に、SMBサーバで認証してログインできるようにする。

  ドメインコントローラがダウンしている場合や、ネットワークの問題によってSMBサーバからドメインコントローラに接続できない場合は、ローカルユーザはNTLM認証を使用してSMBサーバに認証できます。

- ローカル・ユーザに _ ユーザ権限の管理 _ 権限を割り当てる

User Rights Management は、ユーザとグループに付与する SVM の権限を SMB サーバ管理者が制御できる機能です。ユーザにPrivilegesを割り当てるには、ユーザのアカウントにPrivilegesを割り当てるか、ユーザをそのPrivilegesを含むローカルグループのメンバーにします。

ローカルグループを作成する理由は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメイングループを使用できません。

  ローカルグループはワークグループ構成では必要ありませんが、ローカルワークグループユーザのアクセスPrivilegesの管理に役立ちます。

- 共有とファイルアクセスの制御にローカルグループを使用して、ファイルおよびフォルダリソースへのアクセスを制御する。
- カスタマイズした _ ユーザ権限の管理 _ 権限を持つローカルグループを作成する。

  一部の組み込みユーザグループには、Privilegesが事前に定義されています。カスタマイズしたPrivilegesセットを割り当てるには、ローカルグループを作成し、そのグループに必要なPrivilegesを割り当てます。その後、ローカルユーザ、ドメインユーザ、およびドメイングループをそのローカルグループに追加できます。

関連情報

ローカルユーザ認証の仕組み

サポートされるPrivilegesのリスト

ローカルユーザ認証の仕組み

ローカルユーザがCIFSサーバ上のデータにアクセスする前に、認証されたセッションを作成する必要があります。

SMBはセッションベースであるため、ユーザのIDはセッションの最初のセットアップ時に1回だけ確認できます。CIFSサーバでは、ローカルユーザの認証時にNTLMベースの認証が使用されます。NTLMv1とNTLMv2の両方がサポートされています。

ONTAPは、3つのユースケースでローカル認証を使用します。それぞれのユースケースは、ユーザ名のドメイン部分（domain\user形式）がCIFSサーバのローカルドメイン名（CIFSサーバ名）と一致するかどうかによって異なります。

- ドメイン部分が一致する

  データへのアクセスを要求するときにローカルユーザクレデンシャルを指定したユーザは、CIFSサーバでローカルに認証されます。

- ドメイン部分が一致しません

  ONTAPは、CIFSサーバが属しているドメインのドメインコントローラでNTLM認証を試行します。認証に成功した場合は、ログインが完了します。成功しなかった場合、次に何が起こるかは、認証が成功しなかった理由によって異なります。

  たとえば、ユーザがActive Directoryに存在するにもかかわらず、パスワードが無効であるか期限切れになっている場合、ONTAPはCIFSサーバ上の対応するローカルユーザアカウントの使用を試みません。代わ

りに、認証は失敗します。NetBIOSドメイン名が一致しなくても、ONTAPがCIFSサーバ上の対応するローカルアカウント（存在する場合）を認証に使用するケースは他にもあります。たとえば、一致するドメインアカウントが存在するが無効になっている場合、ONTAPはCIFSサーバ上の対応するローカルアカウントを認証に使用します。

- ドメイン部分が指定されていません

  ONTAPは最初にローカルユーザとしての認証を試行します。ローカルユーザとしての認証に失敗した場合、ONTAPはCIFSサーバが属しているドメインのドメインコントローラでユーザを認証します。

ローカルユーザまたはドメインユーザの認証が完了すると、ONTAPはローカルグループメンバーシップとPrivilegesを考慮した完全なユーザアクセストークンを構築します。

ローカルユーザのNTLM認証の詳細については、Microsoft Windowsのマニュアルを参照してください。

関連情報

ローカルユーザ認証の有効化と無効化

ユーザアクセストークンの構成方法

ユーザが共有をマッピングすると、認証された SMB セッションが確立され、ユーザアクセストークンが構成されます。このトークンには、ユーザ、ユーザのグループメンバーシップ、累積権限、マッピングされた UNIX ユーザのそれぞれについて、情報が格納されています。

この機能が無効になっていないかぎり、ローカルユーザとローカルグループの両方の情報がユーザアクセストークンに追加されます。アクセストークンの構成方法は、ローカルユーザのログインと Active Directory ドメインユーザのログインでは、方法が異なります。

- ローカルユーザログイン

  ローカルユーザは複数のローカルグループのメンバーになることができますが、ローカルグループを他のローカルグループのメンバーにすることはできません。ローカルユーザアクセストークンは、その特定のローカルユーザが属するグループに割り当てられたすべての権限の組み合わせから構成されます。

- ドメイン・ユーザ・ログイン

  ドメインユーザのログインでは、 ONTAP は、ユーザの SID と、そのユーザが属するすべてのドメイングループの SID が格納されたユーザアクセストークンを取得します。ONTAP は、ユーザドメイングループのローカルメンバーシップ（存在する場合）が提供するアクセストークンとドメインユーザアクセストークンとの組み合わせを使用します。また、ドメインユーザに割り当てられた直接権限や、ドメイングループメンバーシップの直接権限も使用します。

ローカルユーザとドメインユーザの両方のログインで、プライマリグループ RID もユーザアクセストークン用に設定されています。デフォルトのRIDは（RID 513）です `Domain Users`。デフォルトは変更できません。

Windows から UNIX へのネームマッピングと、 UNIX から Windows へのネームマッピングのプロセスでは、ローカルアカウントとドメインアカウントのどちらについても同じルールが適用されます。

UNIX ユーザがローカルアカウントに自動的にマッピングされることはありません。このマッピングが必要な場合は、既存のネームマッピングコマンドを使用して明示的なマッピングルールを指定する必要があります。

ローカルグループを含む **SVM** での **SnapMirror** の使用に関するガイドラインを次に示します

ローカルグループを含む SVM によって所有されているボリュームで SnapMirror を設定する際は、一定のガイドラインに注意する必要があります。

SnapMirror によって別の SVM にレプリケートされるファイル、ディレクトリ、または共有に適用する ACE ではローカルグループを使用できません。SnapMirror 機能を使用して別の SVM 上のボリュームに対する DR ミラーを作成する場合に、そのボリュームにローカルグループの ACE があるときは、ミラーには ACE は適用されません。データが別の SVM にレプリケートされる場合、実質的に、そのデータは別のローカルドメインに格納されることになります。ローカルユーザとローカルグループに付与されるアクセス権は、そのオブジェクトが最初に作成された SVM のスコープ内でのみ有効です。

CIFSサーバを削除したときのローカルユーザとローカルグループへの影響

CIFSサーバを作成するとデフォルトの一連のローカルユーザとローカルグループが作成され、CIFSサーバをホストするStorage Virtual Machine（SVM）に関連付けられます。SVM管理者は、ローカルユーザやローカルグループをいつでも作成できます。CIFSサーバを削除した場合のローカルユーザとローカルグループへの影響について理解しておく必要があります。

ローカルユーザとローカルグループはSVMに関連付けられます。そのため、セキュリティ上の理由から、CIFSサーバを削除してもそれらが削除されることはありません。CIFSサーバを削除してもローカルユーザとローカルグループは削除されませんが、表示されません。SVMでCIFSサーバを再作成するまで、表示したり管理したりすることはできません。

CIFSサーバの管理ステータスは、ローカルユーザやローカルグループの表示には影響しません。

Microsoft 管理コンソールでのローカルユーザとローカルグループの情報の表示

Microsoft 管理コンソールを使用して、ローカルユーザとローカルグループのそれぞれの情報を表示できます。ONTAP の今回のリリースでは、 Microsoft 管理コンソールで、ローカルユーザとローカルグループに対する上記以外の管理タスクを実行することはできません。

リバートに関するガイドライン

ローカルユーザとグループを使用してファイルアクセスまたはユーザ権限を管理している場合に、ローカルユーザとグループをサポートしない ONTAP リリースにクラスタをリバートするときは、一定の考慮事項に注意する必要があります。

- セキュリティ上の理由から、 ONTAP をローカルユーザとグループの機能をサポートしないバージョンにリバートしても、設定されているローカルユーザ、グループ、および権限に関する情報は削除されません。

- ONTAP の以前のメジャーバージョンにリバートする際、 ONTAP では認証とクレデンシャルの作成時にローカルユーザとローカルグループは使用されません。
- ローカルユーザとローカルグループは、ファイルおよびフォルダの ACL からは削除されません。
- ローカルユーザまたはローカルグループに付与された権限に基づいて許可されるアクセスに依存するファイルアクセス要求は拒否されます。

  アクセスを許可するには、ローカルユーザとローカルグループオブジェクトではなく、ドメインオブジェクトに基づいてアクセスを許可するようにファイル権限を再設定する必要があります。

ローカル権限とは

サポートされる**Privileges**のリスト

ONTAPには、サポートされるPrivilegesのセットがあらかじめ定義されています。一部の事前定義されたローカルグループには、これらのPrivilegesの一部がデフォルトで追加されています。また、事前定義されたグループに対してPrivilegesを追加または削除したり、新しいローカルユーザまたはローカルグループを作成して、作成したグループや既存のドメインユーザおよびグループにPrivilegesを追加したりすることもできます。

次の表に、Storage Virtual Machine（SVM）でサポートされるPrivilegesの一覧と、Privilegesが割り当てられているBUILTINグループの一覧を示します。

権限の名前	デフォルトのセキュリティ設定	説明
`SeTcbPrivilege`	なし	オペレーティングシステムの一部として機能
`SeBackupPrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	ACLを無視してファイルとディレクトリをバックアップ
`SeRestorePrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	ACLを無視してファイルとディレクトリをリストア有効なユーザまたはグループのSIDをファイル所有者として設定する
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	ファイルやその他のオブジェクトの所有権を取得する
`SeSecurityPrivilege`	`BUILTIN\Administrators`	監査の管理 セキュリティ ログの表示、ダンプ、消去など。

権限の名前	デフォルトのセキュリティ設定	説明
SeChangeNotifyPrivilege	BUILTIN\Administrators BUILTIN\Backup Operators、、 BUILTIN\Power Users、、 BUILTIN\Users Everyone	トラバースチェックのバイパス この権限を持つユーザには、フォルダ、シンボリックリンク、ジャンクションをトラバースするためのトラバース（x）権限は必要ありません。

関連情報

- ローカルPrivilegesの割り当て
- トラバースチェックのバイパスの設定

Privilegesの割り当て

Privilegesは、ローカルユーザまたはドメインユーザに直接割り当てることができます。また、ユーザに付与する機能と一致するPrivilegesが割り当てられているローカルグループにユーザを割り当てることもできます。

- 作成したグループに一連の権限を割り当てることができます。

  次に、そのユーザに割り当てるPrivilegesを含むグループにユーザを追加します。

- また、デフォルトのPrivilegesがユーザに付与するPrivilegesと一致する事前定義されたグループに、ローカルユーザとドメインユーザを割り当てることもできます。

関連情報

- ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加
- ローカルまたはドメインのユーザまたはグループからのPrivilegesの削除
- ロオカルマタハトメインノユウサトクルウフノPrivilegesノリセツト
- トラバースチェックのバイパスの設定

BUILTINグループとローカル管理者アカウントの使用に関するガイドライン

BUILTINグループとローカル管理者アカウントを使用する場合は、一定のガイドラインに注意する必要があります。たとえば、ローカル管理者アカウントは、名前の変更は可能ですが、削除はできません。

- Administratorアカウントの名前は変更できますが、削除することはできません。
- AdministratorアカウントはBUILTIN\Administratorsグループから削除できません。
- 組み込みグループの名前は変更できますが、削除することはできません。

  BUILTINグループの名前を変更すると、既知の名前を使用して別のローカルオブジェクトを作成できますが、そのオブジェクトには新しいRIDが割り当てられます。

- ローカルGuestアカウントはありません。

関連情報

事前定義のBUILTINグループとデフォルトのPrivileges

ローカルユーザのパスワードの要件

デフォルトでは、ローカルユーザのパスワードは複雑さの要件を満たす必要があります。パスワードの複雑さの要件は、 Microsoft Windows_Local セキュリティポリシー _ で定義されている要件に似ています。

パスワードは次の基準を満たしている必要があります。

- 6文字以上にする必要があります
- ユーザアカウント名を含めることはできません
- 次の4つのカテゴリのうち、少なくとも3つの文字を含める必要があります。
  - 大文字のアルファベット（A~Z）
  - 小文字のアルファベット（a~z）
  - 10進数（0～9）
  - 特殊文字：

    ~@ # $ % { キャレット } & * _ + = \ | () []:;"<> 、 .? /

関連情報

ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化

CIFSサーバのセキュリティ設定に関する情報の表示

ローカルユーザアカウントのパスワードの変更

事前定義の**BUILTIN**グループとデフォルトの**Privileges**

ローカルユーザまたはドメインユーザのメンバーシップを、ONTAPの事前定義された一連のBUILTINグループに割り当てることができます。事前定義グループには事前定義Privilegesが割り当てられています。

次の表に、事前定義グループを示します。

事前定義の **BUILTIN** グループ	デフォルトの権限
BUILTIN\AdministratorsRID 544 最初に作成されたときに、RID 500のローカル Administrator`アカウントが自動的にこのグループのメンバーになります。Storage Virtual Machine（SVM）がドメインに参加すると、`domain\Domain Admins`グループがグループに追加されます。SVMがドメインから削除されると`domain\Domain Admins、グループはグループから削除されます。	• SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
BUILTIN\Power UsersRID 547 このグループには、最初に作成された時点ではメンバーがありません。このグループのメンバーには、次のような特徴があります。 • ローカルユーザとローカルグループを作成および管理できます。 • 自分自身や他のオブジェクトをグループに追加することはできません BUILTIN\Administrators。	SeChangeNotifyPrivilege
BUILTIN\Backup OperatorsRID 551 このグループには、最初に作成された時点ではメンバーがありません。このグループのメンバーは、バックアップ目的で開いたファイルやフォルダの読み取りおよび書き込み権限を上書きできます。	• SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
BUILTIN\UsersRID 545 最初に作成された時点では、このグループには（暗黙的な特殊グループ以外に）メンバーはありませ`Authenticated Users`ん。SVMがドメインに参加すると、`domain\Domain Users`グループがこのグループに追加されます。SVMがドメインから削除されると、`domain\Domain Users`グループはこのグループから削除されます。	SeChangeNotifyPrivilege
EveryoneSID S-1-1-0 このグループには、ゲストを含むすべてのユーザが含まれます（匿名ユーザは含まれません）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。	SeChangeNotifyPrivilege

関連情報

BUILTINグループとローカル管理者アカウントの使用に関するガイドライン

サポートされるPrivilegesのリスト

トラバースチェックのバイパスの設定

ローカルユーザとローカルグループ機能の有効化と無効化

ローカルユーザとローカルグループの有効化と無効化の機能の概要

NTFSセキュリティ形式データのアクセス制御にローカルユーザとローカルグループを使用する前に、ローカルユーザとローカルグループ機能を有効にする必要があります。また、SMB認証にローカルユーザを使用する場合は、ローカルユーザ認証機能を有効にする必要があります。

ローカルユーザとローカルグループ機能とローカルユーザ認証はデフォルトで有効になっています。有効になっていない場合は、ローカルユーザとローカルグループを設定して使用する前に有効にする必要があります。ローカルユーザとローカルグループ機能はいつでも無効にできます。

ローカルユーザとローカルグループ機能の明示的な無効化に加えて、ONTAPでは、クラスタ内のいずれかのノードがローカルユーザとローカルグループ機能をサポートしないONTAPリリースにリバートされた場合にローカルユーザとローカルグループ機能が無効になります。クラスタ内のすべてのノードでこの機能をサポートするバージョンのONTAPが実行されるまで、ローカルユーザとローカルグループ機能は有効になりません。

関連情報

ローカルユーザアカウントを変更する

ローカルグループの変更

ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加

ローカルユーザとローカルグループの有効化と無効化

Storage Virtual Machine（SVM）で、SMBアクセス用のローカルユーザとローカルグループを有効または無効にすることができます。ローカルユーザとローカルグループ機能はデフォルトで有効になっています。

タスクの内容

SMB共有およびNTFSファイル権限の設定時にローカルユーザとローカルグループを使用できます。必要に応じて、SMB接続の作成時の認証にローカルユーザを使用することもできます。認証にローカルユーザを使用するには、ローカルユーザとローカルグループ認証オプションも有効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ローカルユーザとローカルグループの設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、SVM vs1でローカルユーザとローカルグループ機能を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

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

関連情報

ローカルユーザ認証の有効化または無効化

ローカルユーザアカウントの有効化または無効化

ローカルユーザ認証の有効化または無効化

Storage Virtual Machine（SVM）でのSMBアクセスに関するローカルユーザ認証を有効または無効にすることができます。デフォルトでは、ローカルユーザ認証は許可されます。これは、SVMがドメインコントローラに接続できない場合や、ドメインレベルのアクセス制御を使用しない場合に役立ちます。

開始する前に

CIFSサーバでローカルユーザとローカルグループ機能を有効にする必要があります。

タスクの内容

ローカルユーザ認証はいつでも有効または無効にできます。SMB接続の作成時の認証にローカルユーザを使用する場合は、CIFSサーバのローカルユーザとローカルグループオプションも有効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`

2. 次のいずれかを実行します。

ローカル認証の設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、SVM vs1でローカルユーザ認証を有効にします。

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

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

関連情報

ローカルユーザ認証の仕組み

ローカルユーザとローカルグループの有効化と無効化

ローカルユーザアカウントを管理します。

ローカルユーザアカウントを変更する

既存のユーザのフルネームや概要を変更したり、ユーザアカウントを有効または無効にしたりする場合は、ローカルユーザアカウントを変更します。また、ユーザ名が侵害を受けたり、管理上の目的で名前の変更が必要になった場合にも、ローカルユーザアカウントの名前を変更できます。

状況	入力するコマンド
ローカルユーザのフルネームの変更	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -full-name text`フルネームにスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザの概要を変更します	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -description text`説明にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザアカウントを有効または無効にする	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account-disabled {true
false}`	ローカルユーザアカウントの名前を変更する

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上のローカルユーザ「 CIFS_SERVER\sue 」の名前を「 CIFS_SERVER\sue_new 」に変更します。

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

ローカルユーザアカウントの有効化または無効化

ユーザがStorage Virtual Machine（SVM）に格納されたデータにSMB接続経由でアクセスできるようにするには、ローカルユーザアカウントを有効にします。また、そのユーザがSVMのデータにSMB経由でアクセスできないようにするには、ローカルユーザアカウントを無効にします。

タスクの内容

ローカルユーザを有効にするには、ユーザアカウントを変更します。

ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
ユーザアカウントを有効にする	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account-disabled false`

状況	入力するコマンド
ユーザアカウントを無効にする	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

ローカルユーザアカウントのパスワードの変更

ローカルユーザのアカウントパスワードを変更できます。これは、ユーザのパスワードが侵害された場合や、ユーザがパスワードを忘れた場合に役立ちます。

ステップ

1. 適切な操作を実行してパスワードを変更します。 `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 に関連付けられたローカルユーザ「 CIFS_SERVER\sue 」のパスワードを設定します。

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

関連情報

ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化

CIFSサーバのセキュリティ設定に関する情報の表示

ローカルユーザに関する情報を表示する

すべてのローカルユーザのリストを要約形式で表示できます。特定のユーザに対して設定されているアカウント設定を確認する場合は、そのユーザの詳細なアカウント情報だけでなく、複数のユーザのアカウント情報も表示できます。この情報は、ユーザの設定を変更する必要があるかどうかを判断するのに役立ちます。また、認証やファイルアクセスに関する問題のトラブルシューティングにも役立ちます。

タスクの内容

ユーザのパスワードに関する情報は表示されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
Storage Virtual Machine（SVM）上のすべてのユーザに関する情報を表示する	`vserver cifs users-and-groups local-user show -vserver vserver_name`
特定のユーザの詳細なアカウント情報を表示する	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

他にも、コマンドの実行時に選択できるオプションのパラメータがあります。詳細については、のマニュアルページを参照してください。

例

次の例では、SVM vs1のすべてのローカルユーザに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

ローカルユーザのグループメンバーシップに関する情報を表示する

ローカルユーザが属しているローカルグループに関する情報を表示できます。この情報を使用して、ファイルやフォルダに対するユーザのアクセス権を決定できます。この情報は、ファイルやフォルダに対するユーザのアクセス権を決定する場合や、ファイルアクセスに関する問題のトラブルシューティングを行う場合に役立ちます。

タスクの内容

コマンドをカスタマイズして、必要な情報のみを表示することができます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
指定したローカルユーザのローカルユーザメンバーシップ情報を表示する	`vserver cifs users-and-groups local-user show-membership -user-name user_name`
このローカルユーザが属しているローカルグループのローカルユーザメンバーシップ情報を表示する	`vserver cifs users-and-groups local-user show-membership -membership group_name`

状況	入力するコマンド
指定したStorage Virtual Machine（SVM）に関連付けられているローカルユーザのユーザメンバーシップ情報を表示する	`vserver cifs users-and-groups local-user show-membership -vserver vserver_name`
指定したSVM上のすべてのローカルユーザに関する詳細情報を表示する	`vserver cifs users-and-groups local-user show-membership -instance -vserver vserver_name`

例

次の例は、 SVM vs1 上のすべてのローカルユーザのメンバーシップ情報を表示します。ユーザ「 CIFS_SERVER\Administrator 」は「 BUILTIN\Administrators 」グループのメンバーで、「 CIFS_SERVER\sue 」は「 CIFS_SERVER\g1 」グループのメンバーです。

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

ローカルユーザアカウントを削除する

Storage Virtual Machine（SVM）に対するローカルSMB認証やSVMに格納されたデータへのアクセス権の定義に使用するローカルユーザアカウントが不要になった場合は、SVMから削除することができます。

タスクの内容

ローカルユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

  このユーザーを参照するファイルおよびディレクトリのWindowsセキュリティ記述子は調整されません。

- ローカルユーザへの参照は、メンバーシップデータベースとPrivilegesデータベースからすべて削除されます。
- 一般的な標準ユーザ（Administratorなど）は削除できません。

手順

1. 削除するローカルユーザアカウントの名前を確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. ローカルユーザを削除します。 `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. ユーザアカウントが削除されたことを確認します。 `vserver cifs users-and-groups local-user`

```
show -vserver vserver_name
```

例

次の例は、 SVM vs1 に関連付けられたローカルユーザ「 CIFS_SERVER\su 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

ローカルグループを管理します。

ローカルグループの変更

既存のローカルグループの概要を変更するには、既存のローカルグループの名前を変更するか、グループの名前を変更します。

状況	使用するコマンド
ローカルグループの概要を変更します	`vserver cifs users-and-groups local-group modify -vserver *vserver_name* -group-name *group_name* -description text`説明にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルグループの名前を変更します	`vserver cifs users-and-groups local-group rename -vserver *vserver_name* -group-name *group_name* -new-group-name *new_group_name*`

例

次の例では ' ローカル・グループの名前を 'CIFS_server\engineering' から 'CIFS_server\engineering_new' に変更します

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

次の例では ' ローカル・グループの概要を変更します

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

ローカルグループに関する情報を表示する

クラスタまたは指定したStorage Virtual Machine（SVM）で設定されているすべてのローカルグループの一覧を表示できます。この情報は、SVMに格納されているデータへのファイルアクセスに関する問題やSVMのユーザ権限に関する問題のトラブルシューティングに役立ちます。

ステップ

1. 次のいずれかを実行します。

必要な情報	入力するコマンド
クラスタのすべてのローカルグループ	`vserver cifs users-and-groups local-group show`
SVMのすべてのローカルグループ	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例では、SVM vs1のすべてのローカルグループに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

ローカルグループメンバーシップを管理します。

ローカルグループメンバーシップの管理では、ローカルユーザまたはドメインユーザの追加と削除、またはドメイングループの追加と削除を行うことができます。これは、グループに設定されたアクセス制御に基づいてデータへのアクセスを制御する場合や、ユーザにそのグループにPrivilegesを関連付ける場合に便利です。

タスクの内容

ローカルグループへのメンバーの追加に関するガイドラインは次のとおりです。

- 特殊なグループ _Everyone にユーザーを追加することはできません。
- ユーザを追加するローカルグループが存在している必要があります。
- ローカルグループにユーザを追加する前に、そのユーザが存在している必要があります。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、Data ONTAPで名前をSIDに解決できる必要があります。

ローカルグループからのメンバーの削除に関するガイドラインは次のとおりです。

- 特殊なグループ _Everyone からメンバーを削除することはできません。
- メンバーを削除するグループが存在している必要があります。
- ONTAPは、グループから削除するメンバーの名前を対応するSIDに解決できる必要があります。

ステップ

1. グループのメンバーを追加または削除します。

状況	使用するコマンド
グループへのメンバーの追加	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]`ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループに追加できます。
グループからのメンバーの削除	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]`ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループから削除することができます。

次の例は、 SVM vs1 上のローカルグループ「 `S MB_server\sue` 」とドメイングループ「 AD_DOM\dom_eng 」をローカルグループ「 `S MB_server\engineering` 」に追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

次の例は、 SVM vs1 上のローカルグループ「 S MB_server\sue 」と「 S MB_server\james 」からローカルユーザ「 S MB_server\engineering 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

関連情報

ローカルグループのメンバーに関する情報の表示

ローカルグループのメンバーに関する情報を表示する

クラスタまたは指定したStorage Virtual Machine（SVM）で設定されているローカルグループのすべてのメンバーの一覧を表示できます。この情報は、ファイルアクセスの問題やユーザ権限の問題のトラブルシューティングに役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
クラスタのすべてのローカルグループのメンバー	`vserver cifs users-and-groups local-group show-members`
SVMのすべてのローカルグループのメンバー	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

例

次の例では、SVM vs1のすべてのローカルグループのメンバーに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ---------------------------- ------------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

ローカルグループを削除します。

Storage Virtual Machine（SVM）に関連付けられたデータへのアクセス権を定義するためのローカルグループが不要になった場合や、グループメンバーへのSVMユーザ権限（Privileges）の割り当てに必要なくなった場合は、SVMからローカルグループを削除できます。

タスクの内容

ローカルグループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

  このグループを参照するファイルおよびディレクトリのWindowsセキュリティ記述子は調整されません。

- グループが存在しない場合はエラーが返されます。
- special_every_group は削除できません。
- BUILTIN \ Administrators *BUILTIN\Users* などの組み込みのグループは削除できません。

手順

1. SVM上のローカルグループのリストを表示して、削除するローカルグループの名前を確認します。
   `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. ローカルグループを削除します。 `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. グループが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

例

次の例は、 SVM vs1 に関連付けられたローカルグループ「 CIFS_SERVER\sales 」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

ローカルデータベースでのドメインユーザ名とドメイングループ名の更新

CIFSサーバのローカルグループにドメインユーザやドメイングループを追加できます。これらのドメインオブジェクトは、クラスタのローカルデータベースに登録されます。ドメインオブジェクトの名前を変更する場合は、ローカルデータベースを手動で更新する必要があります。

タスクの内容

ドメイン名を更新するStorage Virtual Machine（SVM）の名前を指定する必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 適切な操作を実行します。

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループのうち、正常に更新されたものと更新できなかったものを表示する	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループが正常に更新されたことを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
更新に失敗したドメインユーザとドメイングループのみを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
更新に関するすべてのステータス情報を非表示にする	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、Storage Virtual Machine（SVM、旧Vserver）vs1に関連付けられているドメインユーザとドメイングループの名前を更新します。最後の更新では、依存する一連の名前を更新する必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

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

ローカル**Privileges**を管理します。

ローカルまたはドメインのユーザまたはグループへの**Privileges**の追加

ローカルまたはドメインのユーザやグループのユーザ権限を管理できます。追加した権限は、これらのオブジェクトに割り当てられていたデフォルトの権限よりも優先されます。これにより、ユーザまたはグループに付与する権限をカスタマイズして、セキュリティを強化できます。

開始する前に

権限を追加する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

オブジェクトに権限を追加すると、そのユーザまたはグループのデフォルトの権限は無効になります。権限を追加しても、以前に追加した権限は削除されません。

ローカルまたはドメインのユーザまたはグループに権限を追加する場合は、次の点に注意する必要があります。

- 権限は 1 つ以上追加できます。
- Privilegesをドメインユーザまたはグループに追加するときに、ONTAPがドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。

  ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに1つ以上のPrivilegesを追加します。 `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or -group-name name -privileges _privilege_[,...]`
2. 目的のPrivilegesがオブジェクトに適用されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 CIFS_SERVER\suueo 」ユーザに「 ````eTcbPrivilege] 」権限と「 `seeOwnershipPrivilege 」権限を追加します。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

ローカルまたはドメインのユーザやグループのユーザ権限を管理するには、権限を削除します。これにより、ユーザとグループに付与される最大権限をカスタマイズして、セキュリティを強化できます。

開始する前に

Privilegesを削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

ローカルまたはドメインのユーザやグループの権限を削除するときは、次の点に注意してください。

- 1 つ以上の権限を削除できます。
- ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続してドメインユーザまたはグループを検証することがあります。

  ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループから1つ以上のPrivilegesを削除します。 `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 目的のPrivilegesがオブジェクトから削除されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上のユーザ「 CIFS_SERVER\suueo 」から「 `s eTcbPrivilege 」および「 `s eTakeOwnershipPrivilege 」権限を削除します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

ローカルまたはドメインのユーザとグループの**Privileges**をリセットします。

ローカルまたはドメインのユーザやグループの権限をリセットできます。これは、ローカルまたはドメインのユーザやグループの権限に対して行った変更が不要になった場合や必要がなくなった場合に役立ちます。

タスクの内容

ローカルまたはドメインのユーザまたはグループの権限をリセットすると、そのオブジェクトの権限のエントリがすべて削除されます。

手順

1. ローカルまたはドメインのユーザまたはグループのPrivilegesをリセットします。 `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. オブジェクトでPrivilegesがリセットされたことを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上のユーザ「 CIFS_SERVER\sue 」の権限をリセットしています。デフォルトでは、標準ユーザのアカウントには権限は関連付けられません。

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

次の例では ' グループ ""BUILTIN\Administrators "" の特権をリセットし ' 実質的に特権エントリを削除します

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

権限の上書きに関する情報を表示する

ドメインまたはローカルのユーザアカウントまたはグループに割り当てられているカスタムPrivilegesに関する情報を表示できます。この情報は、必要なユーザー権限が適用されているかどうかを判断するのに役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
Storage Virtual Machine（SVM）のすべてのドメインおよびローカルのユーザとグループ用のカスタムPrivileges	`vserver cifs users-and-groups privilege show -vserver vserver_name`
SVMの特定のドメインまたはローカルのユーザとグループのカスタムPrivileges	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次のコマンドは、SVM vs1のローカルまたはドメインのユーザとグループに明示的に関連付けられているすべてのPrivilegesを表示します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

トラバースチェックのバイパスの設定

トラバースチェックのバイパスの設定の概要

トラバースチェックのバイパスは、トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできるかどうかを判断するユーザ権限です。トラバースチェックのバイパスを許可または拒否した場合の動作と、Storage Virtual Machine（SVM）でのユーザに対するトラバースチェックのバイパスの設定方法を理解しておく必要があります。

トラバースチェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとすると、中間ディレクトリのトラバース権限がONTAPでチェックされず、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、ONTAPはファイルのパスにあるすべてのディレクトリでトラバース（実行）権限をチェックします。

  中間ディレクトリのいずれかに「 X 」（トラバース権限）がない場合、 ONTAP はファイルへのアクセスを拒否します。

トラバースチェックのバイパスの設定

トラバースチェックのバイパスを設定するには、ONTAP CLIを使用するか、Active Directoryグループポリシーにこのユーザ権限を設定します。

権限は `SeChangeNotifyPrivilege`、ユーザにトラバースチェックのバイパスを許可するかどうかを制御します。

- この権限をSVMのローカルSMBユーザまたはグループ、ドメインユーザまたはグループに追加すると、トラバースチェックのバイパスを許可できます。
- この権限をSVMのローカルSMBユーザまたはグループ、ドメインユーザまたはグループから削除すると、トラバースチェックのバイパスが拒否されます。

SVMの次のBUILTINグループには、デフォルトでトラバースチェックのバイパス権限があります。

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`

- `BUILTIN\Users`
- `Everyone`

これらのいずれかのグループのメンバーにトラバースチェックのバイパスを許可しない場合は、グループからこの権限を削除する必要があります。

CLIを使用してSVMのローカルSMBユーザおよびグループのトラバースチェックのバイパスを設定する場合は、次の点に注意する必要があります。

- カスタムのローカルグループまたはドメイングループのメンバーにトラバースチェックのバイパスを許可する場合は、そのグループに権限を追加する必要があります `SeChangeNotifyPrivilege`。
- ローカルユーザまたはドメインユーザにトラバースチェックのバイパスを個別に許可し、そのユーザがその権限を持つグループのメンバーでない場合は、そのユーザアカウントに権限を追加できます `SeChangeNotifyPrivilege`。
- ローカルまたはドメインのユーザやグループに対するトラバースチェックのバイパスをいつでも無効にするには、権限を削除し `SeChangeNotifyPrivilege`ます。

> 特定のローカルまたはドメインのユーザまたはグループに対してトラバースチェックのバイパスを無効にするには、グループから権限 `Everyone`も削除する必要があります `SeChangeNotifyPrivilege`。

関連情報

ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する

ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する

ボリュームでのSMBファイル名の変換のための文字マッピングの設定

SMB共有のアクセス制御リストの作成

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

サポートされるPrivilegesのリスト

ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加

ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する

トラバースするディレクトリに対する権限がない場合でも、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできるようにするには、Storage Virtual Machine（SVM）のローカルSMBユーザまたはグループに権限を追加します `SeChangeNotifyPrivilege`。デフォルトでは、ユーザはディレクトリのトラバースチェックをバイパスできます。

開始する前に

- SVM上にSMBサーバが存在している必要があります。
- ローカルユーザとローカルグループのSMBサーバオプションが有効になっている必要があります。

- 権限を追加するローカルまたはドメインのユーザまたはグループ `SeChangeNotifyPrivilege`がすでに存在している必要があります。

タスクの内容

Privilegesをドメインユーザまたはグループに追加するときに、ONTAPがドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに権限を追加して、トラバースチェックのバイパスを有効にし `SeChangeNotifyPrivilege`ます。 `vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *name* -privileges SeChangeNotifyPrivilege`

   パラメータの値は `-user-or-group-name`、ローカルユーザまたはグループ、ドメインユーザまたはグループです。

2. 指定したユーザまたはグループでトラバースチェックのバイパスが有効になっていることを確認します。 `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

例

次のコマンドは、「example\eng'」グループに権限を追加することで、「example\eng'」グループに属するユーザがディレクトリのトラバースチェックをバイパスできるようにし `SeChangeNotifyPrivilege`ます。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

関連情報

ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスの禁止

ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する

トラバースするディレクトリに対する権限がないためにファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできないようにするには、Storage Virtual Machine（SVM）のローカルSMBユーザまたはグループから権限を削除します `SeChangeNotifyPrivilege`。

開始する前に

Privilegesを削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続してドメインユーザまたはグループを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. トラバースチェックのバイパスを禁止します。 `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   コマンドは、パラメータの値で指定したローカルまたはドメインのユーザまたはグループから権限を `-user-or-group-name` *`name`*`削除します `SeChangeNotifyPrivilege。

2. 指定したユーザまたはグループに対してトラバースチェックのバイパスが無効になっていることを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

次のコマンドを実行すると、「 EXAMPLE\eng 」グループに属するユーザに対して、ディレクトリのトラバースチェックのバイパスが禁止されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ------------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ------------------------
vs1       EXAMPLE\eng          -
```

関連情報

ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスの許可

ファイルセキュリティと監査ポリシーに関する情報を表示する

ファイルセキュリティと監査ポリシーに関する情報の概要を表示する

Storage Virtual Machine（SVM）のボリュームに格納されたファイルとディレクトリのファイルセキュリティに関する情報を表示できます。FlexVolの監査ポリシーに関する情報を表示できます。設定されている場合、FlexVolボリュームのストレージレベルのアクセス保護およびダイナミックアクセス制御セキュリティの設定に関する情報を表示できます。

ファイルセキュリティに関する情報の表示

次のセキュリティ形式のボリュームおよびqtree（FlexVolボリュームの場合）に格納されたデータに適用されているファイルセキュリティに関する情報を表示できます。

- NTFS
- UNIX
- mixed

監査ポリシーに関する情報の表示

次のNASプロトコルを介したFlexVolボリュームのアクセスイベントを監査する監査ポリシーに関する情報を表示できます。

- SMB（すべてのバージョン）
- NFSv4.x

ストレージレベルのアクセス保護（**SLAG**）セキュリティに関する情報の表示

ストレージレベルのアクセス保護セキュリティは、次のセキュリティ形式のFlexVolボリュームおよびqtreeオブジェクトに適用できます。

- NTFS
- mixed
- UNIX（ボリュームが格納されたSVMでCIFSサーバが設定されている場合）

ダイナミックアクセス制御（**DAC**）セキュリティに関する情報の表示

ダイナミックアクセス制御セキュリティは、次のセキュリティ形式のFlexVol volume内のオブジェクトに適用できます。

- NTFS
- mixed（オブジェクトにNTFS対応のセキュリティが設定されている場合）

関連情報

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

ストレージレベルのアクセス保護に関する情報の表示

NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、DOS属性に関する情報など、NTFSセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することも

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、ファイルアクセス権の決定時にNTFSファイル権限およびWindowsのユーザおよびグループのみが使用されるため、UNIX関連の出力フィールドには表示専用のUNIXファイル権限情報が表示されます。
- ACL出力は、NTFSセキュリティが適用されたファイルとフォルダについて表示されます。
- ストレージレベルのアクセス保護セキュリティはボリュームのルートまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルACLとストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- 指定したファイルまたはディレクトリパスにダイナミックアクセス制御が設定されている場合は、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細を表示	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1のパスに関するセキュリティ情報を表示し `/vol4`ます。

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

次の例では、マスクを展開して、SVM vs1のパスに関するセキュリティ情報を表示します `/data/engineering`。

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
```

```
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
```

```
                                .... .... .... .... .... ...1 .... .... =
Write Attributes
                                .... .... .... .... .... .... 1... .... =
Read Attributes
                                .... .... .... .... .... .... .1.. .... =
Delete Child
                                .... .... .... .... .... .... ..1. .... =
Execute
                                .... .... .... .... .... .... ...1 .... =
Write EA
                                .... .... .... .... .... .... .... 1... =
Read EA
                                .... .... .... .... .... .... .... .1.. =
Append
                                .... .... .... .... .... .... .... ..1. =
Write
                                .... .... .... .... .... .... .... ...1 =
Read

                              ALLOW-Everyone-0x10000000-OI|CI|IO
                                0... .... .... .... .... .... .... .... =
Generic Read
                                .0.. .... .... .... .... .... .... .... =
Generic Write
                                ..0. .... .... .... .... .... .... .... =
Generic Execute
                                ...1 .... .... .... .... .... .... .... =
Generic All
                                .... ...0 .... .... .... .... .... .... =
System Security
                                .... .... ...0 .... .... .... .... .... =
Synchronize
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
```

```
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

次の例では、SVM vs1のパスにあるボリュームの、ストレージレベルのアクセス保護セキュリティ情報を含むセキュリティ情報を表示します `/datavol1`。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

関連情報

mixedセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

UNIXセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、mixedセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびフォルダと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。
- mixedセキュリティ形式のボリュームの最上位では、UNIX対応またはNTFS対応のセキュリティを設定できます。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、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、mixedセキュリティ形式のボリュームまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、UNIXファイル権限とストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例では、マスクを展開した形式で、SVM vs1のパスに関するセキュリティ情報を表示します

/projects。このmixedセキュリティ形式のパスには、UNIX対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

次の例は、SVM vs1のパスに関するセキュリティ情報を表示します /data。このmixedセキュリティ形式のパスには、NTFS対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

次の例では、SVM vs1のパスにあるボリュームに関するセキュリティ情報を表示します `/datavol5`。このmixedセキュリティ形式のボリュームの最上位には、UNIX対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

関連情報

NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

UNIXセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

UNIX セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、UNIXセキュリティ形式のボリューム上にあるファイルやディ

レクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine（SVM）の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを指定する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- ファイルアクセス権の決定時に、UNIXセキュリティ形式のボリュームおよびqtreeでは、UNIXファイル権限（モードビットまたはNFSv4 ACL）のみが使用されます。
- ACL出力は、NFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NFSv4セキュリティ記述子の場合は適用されません。

  NTFSセキュリティ記述子でのみ意味があります。

- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、パラメータで指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります `-path`。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細を表示	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1のパスに関するセキュリティ情報を表示し `/home`ます。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

次の例では、マスクを展開した形式で、SVM vs1のパスに関するセキュリティ情報を表示します `/home`。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

関連情報

NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

mixedセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

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、適用されている権限、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。

タスクの内容

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、NTFSのシステムアクセス制御リスト（SACL）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やフォルダには、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ファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixedセキュリティ形式のボリュームの最上位には、UNIX対応またはNTFS対応のセキュリティを設定でき、NTFS SACLが格納されている場合と格納されていない場合があります。
- ストレージレベルのアクセス保護セキュリティは、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、mixedセキュリティ形式のボリュームまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常の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NTFS SACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御ACEに関する情報も出力に表示されます。
- 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を表示する場合、UNIX関連の出力フィールドに表示専用のUNIXファイル権限情報が表示されます。

  ファイルアクセス権の決定時に、NTFSセキュリティ形式のファイルおよびフォルダでは、NTFSファイル権限と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セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルやフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。

ステップ

1. ファイルおよびディレクトリ監査ポリシーの設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリスト	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/corp`。パスにはNTFS対応のセキュリティが設定されています。NTFSセキュリティ記述子には、SUCCESSおよびSUCCESS / FAIL SACLエントリの両方が含まれています。

```
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のパスの監査ポリシーの情報を表示します `/datavol1`。このパスには、通常のファイルとフォルダのSACLとストレージレベルのアクセス保護のSACLの両方が含まれています。

```
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
```

CLIを使用して**FlexVol**の**NFSv4**監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されている権限、システムアクセス制御リスト（ SACL ）に関する情報など、 ONTAP CLI を使用して FlexVol の NFSv4 監

査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

タスクの内容

Storage Virtual Machine （ SVM ）の名前、および監査情報を表示するファイルまたはディレクトリのパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- UNIX セキュリティ形式のボリュームおよび qtree では、監査ポリシーに NFSv4 SACL のみが使用されます。
- mixed セキュリティ形式のボリュームにある UNIX セキュリティ形式のファイルとディレクトリには、NFSv4 監査ポリシーを適用できます。

  mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モードビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixed セキュリティ形式のボリュームの最上位では、 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、 NFSv4 SACL が含まれる場合と含まれない場合があります。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルやフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、 mixed セキュリティ形式のボリュームまたは qtree で設定できるため、 ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、標準の NFSv4 ファイルおよびディレクトリの SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、パラメータで指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります `-path`。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスに関するセキュリティ情報を表示します `/lab`。この UNIX セキュリティ形式のパスには NFSv4 SACL が設定されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

ファイルセキュリティと監査ポリシーに関する情報を表示する方法

ワイルドカード文字（*）を使用すると、特定のパスまたはルートボリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関する情報を表示できます。

ワイルドカード文字（*）は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。「*」という名前の特定のファイルまたはディレクトリの情報を表示する場合は、二重引用符（「`」）で完全なパスを指定する必要があります。

例

次のコマンドでワイルドカード文字を使用すると、SVM vs1のパスの下にあるすべてのファイルとディレクトリに関する情報が表示され `/1/` ます。

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0x8514
                            Owner:BUILTIN\Administrators
                            Group:BUILTIN\Administrators
                            DACL - ACEs
                            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0x8404
                            Owner:BUILTIN\Administrators
                            Group:BUILTIN\Administrators
                            DACL - ACEs
                            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

次のコマンドは、SVM vs1のパスの下にある「*」という名前のファイルの情報を表示します `/vol1/a`。パスは二重引用符（ "" ）で囲まれます。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: "/vol1/a/*"
           Security Style: mixed
          Effective Style: unix
           DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
             Unix User Id: 1002
            Unix Group Id: 65533
           Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

CLIを使用して、**SVM**の**NTFS**ファイルセキュリティ、**NTFS**監査ポリシー、ストレージレベルのアクセス保護を管理します。

CLIの概要を使用して、**SVM**の**NTFS**ファイルセキュリティ、**NTFS**監査ポリシー、ストレージレベルのアクセス保護を管理します。

CLIを使用して、Storage Virtual Machine（SVM）のNTFSファイルセキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護を管理できます。

NTFSファイルセキュリティと監査ポリシーは、SMBクライアントから、またはCLIを使用して管理できます。ただし、CLIを使用してファイルセキュリティと監査ポリシーを設定すると、リモートクライアントを使用してファイルセキュリティを管理する必要がなくなります。CLIを使用すると、1つのコマンドで多数のファイルやフォルダにセキュリティを適用する時間を大幅に短縮できます。

ONTAPがSVMボリュームに適用するもう1つのセキュリティレイヤであるストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護は、すべてのNASプロトコルからストレージレベルのアクセス保護が適用されるストレージオブジェクトへのアクセスに適用されます。

ストレージレベルのアクセス保護は、ONTAP CLIからのみ設定および管理できます。ストレージレベルのアクセス保護設定をSMBクライアントから管理することはできません。さらに、NFS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セキュリティは表示されません。システム（WindowsまたはUNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が個別に設定および管理できる、データアクセスのセキュリティレイヤを強化します。

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ますが、ストレージレベルのアクセス保護が適用されているボリューム上のデータへのNFS経由のアクセスについては、そのボリュームを所有するSVM上のWindowsユーザにUNIXユーザがマッピングされている場合にONTAPでセキュリティチェックを実行できます。

NTFSセキュリティ形式のボリューム

NTFSセキュリティ形式のボリュームやqtreeに格納されているファイルやフォルダでは、すべてNTFS対応のセキュリティが有効になります。コマンドファミリーを使用すると、NTFSセキュリティ形式のボリュームに次の種類のセキュリティを実装でき `vserver security file-directory`ます。

- ボリュームに含まれるファイルとフォルダに対するファイル権限と監査ポリシー
- ボリュームに対するストレージレベルのアクセス保護セキュリティ

mixedセキュリティ形式のボリューム

mixedセキュリティ形式のボリュームやqtreeには、UNIX対応のセキュリティが有効で、UNIXファイル権限（モードビットまたはNFSv4.x ACL）とNFSv4.x監査ポリシーを使用するファイルやフォルダ、およびNTFS対応のセキュリティが有効でNTFSファイル権限と監査ポリシーを使用するファイルやフォルダを格納できます。コマンドファミリーを使用すると、mixedセキュリティ形式のデータに次の種類のセキュリティを適用でき `vserver security file-directory`ます。

- mixed形式のボリュームまたはqtreeにおけるNTFS対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- NTFS対応またはUNIX対応のセキュリティ形式のボリュームに対するストレージレベルのアクセス保護

UNIXセキュリティ形式のボリューム

UNIXセキュリティ形式のボリュームおよびqtreeには、UNIX対応のセキュリティ（モードビットまたはNFSv4.x ACL）が設定されたファイルおよびフォルダが格納されます。コマンドファミリーを使用してUNIXセキュリティ形式のボリュームにセキュリティを実装する場合は、次の点に注意する必要があり `vserver security file-directory`ます。

- UNIXセキュリティ形式のボリュームおよびqtreeでは、 `vserver security file-directory`コマンドファミリーを使用してUNIXファイルセキュリティおよび監査ポリシーを管理することはできません。
- ターゲットボリュームを含むSVMにCIFSサーバが含まれている場合は、コマンドファミリーを使用してUNIXセキュリティ形式のボリュームにストレージレベルのアクセス保護を設定できます `vserver security file-directory`。

関連情報

ファイルセキュリティと監査ポリシーに関する情報を表示する

CLIを使用したNTFSファイルおよびフォルダに対するファイルセキュリティの設定と適用

CLIを使用した監査ポリシーの設定とNTFSファイルおよびフォルダへの適用

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

CLIを使用したファイルおよびフォルダのセキュリティ設定のユースケース

ファイルおよびフォルダのセキュリティは、リモートクライアントを使用せずにローカルで適用および管理できるため、多数のファイルまたはフォルダに対して一括でセキュリティを設定する場合に比べて大幅に時間を短縮できます。

CLI を使用してファイルおよびフォルダのセキュリティを設定すると効果的な状況として、次のようなユースケースがあります。

- ホームディレクトリ内のファイルストレージなど、大規模なエンタープライズ環境のファイルの格納
- データの移行
- Windowsドメインの変更
- NTFS ファイルシステムのファイルセキュリティと監査ポリシーの標準化

CLIを使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項

CLIを使用してファイルおよびフォルダのセキュリティを設定する場合は、一定の制限事項に注意する必要があります。

- `vserver security file-directory`コマンドファミリーはNFSv4 ACLの設定をサポートしていません。

  NTFSセキュリティ記述子は、NTFSファイルおよびNTFSフォルダにのみ適用できます。

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

セキュリティ記述子には、ユーザがファイルやフォルダに対して実行できる操作、およびユーザがファイルやフォルダにアクセスするときに監査される内容を決定するアクセス制御リストが含まれます。

- * 権限 *

  権限はオブジェクトの所有者によって許可または拒否され、オブジェクト（ユーザ、グループ、またはコンピュータオブジェクト）が指定されたファイルまたはフォルダに対して実行できる操作を決定します。

- * セキュリティ記述子 *

  セキュリティ記述子は、ファイルまたはフォルダに関連付けられた権限を定義するセキュリティ情報を含むデータ構造です。

- * アクセス制御リスト (ACL) *

  アクセス制御リストは、セキュリティ記述子内に含まれるリストで、セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータオブジェクトが実行できる操作に関する情報が含まれます。セキュリティ記述子には、次の2種類のACLを含めることができます。

  - Discretionary Access Control List （ DACL ；随意アクセス制御リスト）
  - システムアクセスセイギョリスト SACL

- * 随意アクセス制御リスト（ DACL ） *

DACLには、ファイルまたはフォルダに対してアクションを実行するためのアクセスを許可または拒否するユーザ、グループ、およびコンピュータオブジェクトのSIDリストが含まれます。DACLには0個以上のAccess Control Entry（ACE；アクセス制御エントリ）が含まれます。

- * システム・アクセス・コントロール・リスト（ SACL ） *

  SACLには、成功または失敗した監査イベントがログに記録されるユーザ、グループ、およびコンピュータオブジェクトのSIDリストが含まれます。SACLには0個以上のAccess Control Entry（ACE；アクセス制御エントリ）が含まれます。

- * アクセス制御エントリ (ACE) *

  ACEは、DACLまたはSACLの個 々 のエントリです。

  - DACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトに対して許可または拒否されるアクセス権を指定します。
  - SACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトによって実行される指定された操作の監査時にログに記録される成功または失敗イベントを指定します。

- * 権限の継承 *

  権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトにパーミッションを設定する際に、「適用先」、 `sub-folders`「ファイル」でフォルダ、サブフォルダ、およびファイルを継承できるかどうかを指定できます `this-folder`。

関連情報

"SMBおよびNFSの監査とセキュリティトレース"

CLIを使用したNTFSファイルおよびフォルダへの監査ポリシーの設定および適用

SVM ディザスタリカバリデスティネーションでローカルユーザまたはグループを使用するファイルとディレクトリのポリシーを適用する際のガイドライン

ファイルとディレクトリのポリシー設定でセキュリティ記述子、DACL、SACLエントリのいずれかでローカルユーザまたはグループを使用する場合、ID破棄設定のStorage Virtual Machine（SVM）ディザスタリカバリデスティネーションでファイルとディレクトリのポリシーを適用する前に注意する必要がある一定のガイドラインがあります。

ソースクラスタのソース SVM が、ソース SVM からデスティネーションクラスタのデスティネーション SVM にデータと設定をレプリケートする SVM ディザスタリカバリ構成を設定できます。

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます

  この設定では、 SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

  この設定では、 SVM と CIFS サーバの ID が維持されません。このシナリオでは、デスティネーション

SVM の SVM と CIFS サーバの名前は、ソース SVM の SVM と CIFS サーバの名前と異なります。

ID 破棄設定に関するガイドライン

ID 破棄設定では、ローカルユーザ、グループ、権限設定を含む SVM ソースを SVM デスティネーションの CIFS サーバ名に一致するようにローカルドメインの名前（ローカル CIFS サーバ名）を変更する必要があります。たとえば、ソース SVM 名が「 vs1 」で CIFS サーバ名が「 CIFS1 」、デスティネーション SVM 名が「 vs1_dst 」で CIFS サーバ名が「 CIFS1_DST` 」の場合、ローカルユーザ「 CIFS1\user1 」のローカルドメイン名は「 CIFS1_DST` デスティネーション SVM 」で自動的に「 CIFS1_DST\user1 」に変更されます。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                 Full Name      Description
------------ ------------------------- -------------- -------------
vs1          CIFS1\Administrator                      Built-in
administrator account
vs1          CIFS1\user1               -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                 Full Name      Description
------------ ------------------------- -------------- -------------
vs1_dst      CIFS1_DST\Administrator                  Built-in
administrator account
vs1_dst      CIFS1_DST\user1           -              -
```

ローカルユーザおよびグループデータベースでローカルユーザおよびグループ名が自動的に変更されても、ファイルとディレクトリのポリシー設定（コマンドファミリーを使用してCLIで設定するポリシー）のローカルユーザまたはグループ名は自動的に変更されません `vserver security file-directory`。

たとえば、「vs1」について、パラメータが「`CIFS1\user1`」に設定されたDACLエントリを設定している場合 `-account`、デスティネーションSVMで設定がデスティネーションのCIFSサーバ名を反映するように自動的に変更されることはありません。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

CIFSサーバ名を手動でデスティネーションCIFSサーバ名に変更するには、コマンドを使用する必要があります `vserver security file-directory modify`。

アカウントパラメータを含むファイルとディレクトリのポリシー設定コンポーネント

ローカルユーザまたはグループを含むパラメータ設定を使用できるファイルとディレクトリのポリシー設定コンポーネントは 3 つあります。

- セキュリティ記述子

  必要に応じて、セキュリティ記述子の所有者とセキュリティ記述子の所有者のプライマリグループを指定できます。セキュリティ記述子で所有者とプライマリグループのエントリにローカルユーザまたはグループを使用する場合、デスティネーション SVM にアカウント名を使用するようにセキュリティ記述子を変更する必要があります。アカウント名に必要な変更を加えるには、コマンドを使用し `vserver security file-directory ntfs modify`ます。

- DACLエントリ

  各DACLエントリは、アカウントに関連付ける必要があります。ローカルユーザまたはグループアカウントを使用する DACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存のDACLエントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべてのDACLエントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しいDACLエントリを作成し、それらの新しいDACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

- SACLエントリ

  各SACLエントリは、アカウントに関連付ける必要があります。ローカルユーザまたはグループアカウン

トを使用する SACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存のSACLエントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべてのSACLエントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しいSACLエントリを作成し、それらの新しいSACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

ポリシーを適用する前に、ファイルとディレクトリのポリシー設定で使用されているローカルユーザまたはグループに必要な変更を行う必要があります。そうしないと、適用ジョブは失敗します。

CLIを使用したNTFSファイルおよびフォルダに対するファイルセキュリティの設定と適用

NTFSセキュリティ記述子を作成します。

NTFS セキュリティ記述子（ファイルセキュリティポリシー）の作成は、 Storage Virtual Machine （ SVM ）内のファイルやフォルダの NTFS Access Control List （ ACL ；アクセス制御リスト）を設定および適用するための最初のステップです。セキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けることができます。

タスクの内容

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4つのデフォルトACEは次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み\管理者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込み\ユーザ	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者所有者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュ

アルページを参照してください。

NTFSセキュリティ記述子への**NTFS DACL**アクセス制御エントリの追加

NTFS セキュリティ記述子への随意アクセス制御リスト（ DACL ）のアクセス制御エントリ（ ACE ）の追加は、ファイルまたはフォルダに対する NTFS ACL の設定および適用における 2 番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、 ACE で定義されているファイルまたはフォルダに対してオブジェクトが実行できる操作または実行できない操作が定義されます。

タスクの内容

セキュリティ記述子のDACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるDACLに既存のACEがある場合は、新しいACEがDACLに追加されます。セキュリティ記述子にDACLが含まれていない場合は、DACLが作成されて新しいACEが追加されます。

必要に応じて、パラメータで指定したアカウントに対して許可または拒否する権限を指定することで、DACLエントリをカスタマイズでき `-account`ます。権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権限
- 詳細な権限
- raw 権限（ advanced 権限）

DACLエントリの権限を指定しない場合、権限はデフォルトでに設定され `Full Control`ます。

必要に応じて、継承の適用方法を指定することで、 DACL エントリをカスタマイズできます。

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. セキュリティ記述子にDACLエントリを追加します。 `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. DACLエントリが正しいことを確認します。 `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
           Account Name or SID: DOMAIN\joe
                 Access Rights: full-control
        Advanced Access Rights: -
                     Apply To: this-folder
                 Access Rights: full-control
```

セキュリティポリシーを作成する

SVM のファイルセキュリティポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

タスクの内容

セキュリティポリシーに追加するタスクには、 NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFSセキュリティ形式またはmixedセキュリティ形式のボリュームを含む各SVMに関連付ける必要があります。

手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver vs1
   ```

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
 ------------      ---------------
     vs1               policy1
```

セキュリティポリシーにタスクを追加する

ACL を設定し、 SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、 1 つ以上のタスクエントリを追加できます。

タスクの内容

セキュリティポリシーはタスクのコンテナです。タスクとは、 NTFS または mixed セキュリティが設定され

たファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

  指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10 、 000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

  ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

セキュリティポリシーにタスクを追加する際には、次の 4 つの必須パラメータを指定する必要があります。

- SVM名
- ポリシー名
- パス
- パスに関連付けるセキュリティ記述子

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory`は、パラメータのデフォルト値 `-access-control`です。ファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

セキュリティポリシーを適用する

SVM へのファイルセキュリティポリシーの適用は、ファイルまたはフォルダに対して NTFS ACL を作成および適用する最後のステップです。

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在するNTFSファイルおよびフォルダに適用できます。

> 監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver`

```
vserver_name -policy-name policy_name

vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

セキュリティポリシージョブを監視する

Storage Virtual Machine （ SVM ）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

タスクの内容

セキュリティポリシージョブに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

適用したファイルセキュリティの確認

Storage Virtual Machine （ SVM ）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

タスクの内容

データが格納されている SVM の名前、およびセキュリティ設定を確認するファイルとフォルダのパスを指定する必要があります。オプションのパラメータを使用すると、セキュリティ設定に関する詳細情報を表示できます `-expand-mask`。

ステップ

1. ファイルとフォルダのセキュリティ設定を表示します。 `vserver security file-directory show`

```
-vserver vserver_name -path path [-expand-mask true]

vserver security file-directory show -vserver vs1 -path /data/engineering
-expand-mask true
```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
```

```
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
                             .... .... .... .... .... ...1 .... .... =
Write Attributes
                             .... .... .... .... .... .... 1... .... =
Read Attributes
                             .... .... .... .... .... .... .1.. .... =
Delete Child
                             .... .... .... .... .... .... ..1. .... =
Execute
                             .... .... .... .... .... .... ...1 .... =
Write EA
                             .... .... .... .... .... .... .... 1... =
Read EA
                             .... .... .... .... .... .... .... .1.. =
Append
                             .... .... .... .... .... .... .... ..1. =
Write
                             .... .... .... .... .... .... .... ...1 =
Read

                           ALLOW-Everyone-0x10000000-OI|CI|IO
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
```

```
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

CLIを使用した監査ポリシーの設定と**NTFS**ファイルおよびフォルダへの適用

CLIの概要を使用した**NTFS**ファイルおよびフォルダへの監査ポリシーの設定と適用

ONTAP CLIを使用してNTFSファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、NTFSセキュリティ記述子を作成し、そのセキュリティ記述子にSACLを追加します。次に、セキュリティポリシーを作成し、ポリシータスクを追加します。その後、そのセキュリティポリシーをStorage Virtual Machine（SVM）に適用します。

タスクの内容

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視し、適用した監査ポリシーの設定を確認できます。

監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

関連情報

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

CLIを使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

"SMBおよびNFSの監査とセキュリティトレース"

CLIを使用したNTFSファイルおよびフォルダに対するファイルセキュリティの設定と適用

NTFSセキュリティ記述子を作成します。

NTFS セキュリティ記述子監査ポリシーの作成は、 SVM 内のファイルやフォルダの NTFS Access Control List （ ACL ；アクセス制御リスト）を設定および適用するための最初のステップです。このセキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けます。

タスクの内容

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4つのデフォルトACEは次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み\管理者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込み\ユーザ	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者所有者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. advancedパラメータを使用する場合は、権限レベルをadvancedに設定します。 `set -privilege advanced`
2. セキュリティ記述子を作成します。 `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                  Owner of the Security Descriptor: DOMAIN\joe
   ```

4. advanced権限レベルの場合は、admin権限レベルに戻ります。 `set -privilege admin`

NTFSセキュリティ記述子への**NTFS SACL**アクセス制御エントリの追加

NTFS セキュリティ記述子への SACL （システムアクセス制御リスト）アクセス制御エントリ（ ACE ）の追加は、 SVM 内のファイルやフォルダに対する NTFS 監査ポリシーを作成する 2 番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。SACL エントリは、成功したアクセス試行と失敗したアクセス試行のどちらを監査するかを定義します。

タスクの内容

セキュリティ記述子のSACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるSACLに既存のACEがある場合は、新しいACEがSACLに追加されます。セキュリティ記述子にSACLが含まれていない場合は、SACLが作成されて新しいACEが追加されます。

SACLエントリを設定するには、パラメータで指定したアカウントの成功イベントまたは失敗イベントについて監査する権限を指定し `-account`ます。権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権限

- 詳細な権限
- raw 権限（ advanced 権限）

SACLエントリの権限を指定しない場合のデフォルト設定はです `Full Control`。

必要に応じて、パラメータで継承を適用する方法を指定して、SACLエントリをカスタマイズでき `apply to`ます。このパラメータを指定しない場合、デフォルトでは、この SACL エントリがこのフォルダ、サブフォルダ、およびファイルに適用されます。

手順

1. SACLエントリをセキュリティ記述子に追加します。 `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. SACLエントリが正しいことを確認します。 `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                    Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
   ```

セキュリティポリシーを作成する

Storage Virtual Machine （ SVM ）の監査ポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

タスクの内容

セキュリティポリシーに追加するタスクには、 NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFSセキュリティ形式のボリュームまたはmixedセキュリティ形式のボリュームを含むStorage Virtual Machine（SVM）ごとに関連付ける必要があります。

手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
 ------------      --------------
     vs1               policy1
```

セキュリティポリシーにタスクを追加する

ACL を設定し、 SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1 つ以上のタスクエントリを追加できます。

タスクの内容

セキュリティポリシーはタスクのコンテナです。タスクとは、 NTFS または mixed セキュリティが設定されたファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

  指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10 、 000 個です。

- ポリシーには 1 つ以上のタスクを含めることができます。

  ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory`は、パラメータのデフォルト値 `-access-control`です。ファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

セキュリティポリシーを適用する

SVMへの監査ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在するNTFSファイルおよびフォルダに適用できます。

> 監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

セキュリティポリシージョブを監視する

Storage Virtual Machine （ SVM ）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

タスクの内容

セキュリティポリシージョブに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

適用された監査ポリシーの確認

Storage Virtual Machine （ SVM ）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりになっているかを確認するには、監査ポリシーを確認します。

タスクの内容

監査ポリシーの情報を表示するには、コマンドを使用し `vserver security file-directory show`ます。データが格納されている SVM の名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

ステップ

1. 監査ポリシーの設定を表示します。 `vserver security file-directory show -vserver vserver_name -path path`

例

次のコマンドは、 SVM vs1 のパス「 `/corp` 」に適用されている監査ポリシーの情報を表示します。このパスには、 SUCCESS と SUCCESS/FAIL SACL の両方のエントリが適用されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-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
```

セキュリティポリシージョブを管理する際の考慮事項

セキュリティポリシージョブが存在する場合、特定の状況下では、そのセキュリティポリシーやポリシーに割り当てられたタスクを変更できません。セキュリティポリシーの変更が確実に成功するように、ポリシーを変更できる条件やできない条件を理解しておく必要があります。ポリシーの変更には、ポリシーに割り当てられたタスクの追加、削除、変更と、ポリシーの削除または変更が含まれます。

セキュリティポリシーにジョブが存在し、そのジョブが次の状態の場合、そのポリシーまたはポリシーに割り当てられたタスクは変更できません。

- ジョブが実行中または実行中です。
- ジョブが一時停止中の場合
- ジョブが再開され、実行中の状態になります。
- ジョブが別のノードへのフェイルオーバーを待機中の場合。

セキュリティポリシーにジョブが存在する場合、次の状況下では、そのセキュリティポリシーまたはポリシーに割り当てられたタスクを正常に変更できます。

- ポリシージョブが停止されました。
- ポリシージョブが正常に終了しました。

NTFSセキュリティ記述子の管理用コマンド

ONTAP には、セキュリティ記述子を管理するためのコマンドが用意されています。セキュリティ記述子を作成、変更、削除、および表示できます。

状況	使用するコマンド
NTFS セキュリティ記述子を作成します	`vserver security file-directory ntfs create`
既存の NTFS セキュリティ記述子を変更します	`vserver security file-directory ntfs modify`
既存の NTFS セキュリティ記述子に関する情報を表示します	`vserver security file-directory ntfs show`
NTFS セキュリティ記述子を削除します	`vserver security file-directory ntfs delete`

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 `vserver security file-directory ntfs`。

NTFS DACLアクセス制御エントリの管理用コマンド

ONTAPには、DACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS DACL に追加できます。また、DACLのACEを変更、削除、および情報表示することで、既存のNTFS DACLを管理することもできます。

状況	使用するコマンド
ACE を作成して NTFS DACL に追加します	`vserver security file-directory ntfs dacl add`
NTFS DACL の既存の ACE の変更	`vserver security file-directory ntfs dacl modify`
NTFS DACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs dacl show`
NTFS DACL から既存の ACE を削除します	`vserver security file-directory ntfs dacl remove`

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 `vserver security file-directory`

ntfs dacl。

NTFS SACLアクセス制御エントリの管理用コマンド

ONTAPには、SACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS SACL に追加できます。また、SACLのACEを変更、削除、および情報表示することで、既存のNTFS SACLを管理することもできます。

状況	使用するコマンド
ACE を作成して NTFS SACL に追加します	`vserver security file-directory ntfs sacl add`
NTFS SACL の既存の ACE の変更	`vserver security file-directory ntfs sacl modify`
NTFS SACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs sacl show`
NTFS SACL から既存の ACE を削除します	`vserver security file-directory ntfs sacl remove`

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 `vserver security file-directory ntfs sacl`。

セキュリティポリシーの管理用コマンド

ONTAP には、セキュリティポリシーを管理するためのコマンドが用意されています。ポリシーに関する情報を表示したり、ポリシーを削除したりできます。セキュリティポリシーは変更できません。

状況	使用するコマンド
セキュリティポリシーを作成する	`vserver security file-directory policy create`
セキュリティポリシーに関する情報を表示します	`vserver security file-directory policy show`
セキュリティポリシーを削除する	`vserver security file-directory policy delete`

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 `vserver security file-directory policy`。

セキュリティポリシータスクに関する情報を追加、変更、削除、および表示するためのONTAPコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシータスクを追加する	`vserver security file-directory policy task add`
セキュリティポリシータスクを変更する	`vserver security file-directory policy task modify`
セキュリティポリシータスクに関する情報を表示します	`vserver security file-directory policy task show`
セキュリティポリシータスクを削除する	`vserver security file-directory policy task remove`

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 `vserver security file-directory policy task`。

ONTAP には、セキュリティポリシージョブを一時停止、再開、停止、および関連する情報を表示するためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシージョブを一時停止します	`vserver security file-directory job pause -vserver vserver_name -id integer`
セキュリティポリシージョブを再開します	`vserver security file-directory job resume -vserver vserver_name -id integer`
セキュリティポリシージョブに関する情報を表示します	`vserver security file-directory job show -vserver vserver_name`このコマンドを使用して、ジョブのジョブIDを確認できます。
セキュリティポリシージョブを停止します	`vserver security file-directory job stop -vserver vserver_name -id integer`

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 `vserver security file-directory job`。

SMB共有のメタデータキャッシュの設定

SMBメタデータのキャッシングの仕組み

メタデータのキャッシングにより、 SMB 1.0 クライアントでファイル属性をキャッシュして、ファイル属性およびフォルダ属性にすばやくアクセスできるようになります。属性のキャッシュは、共有ごとに有効または無効にすることができます。メタデータのキャッシングが有効な場合は、キャッシュされたエントリの TTL を設定することもできます。クライアントが SMB 2.x または SMB 3.0 で共有に接続している場合は、メタデータキャッシュの設定は必要ありません。

SMB メタデータのキャッシングを有効にすると、パスとファイルの属性データが一定期間保存されます。これにより、一般的なワークロードでの SMB 1.0 クライアントの SMB パフォーマンスを向上させることができます。

特定のタスクでは、 SMB によって大量のトラフィックが作成され、そのトラフィックにはパスとファイルのメタデータに対する複数の同一クエリが含まれることがあります。代わりに、 SMB メタデータのキャッシングを使用してキャッシュから情報を読み込むことで、重複するクエリの数を減らし、 SMB 1.0 クライアントのパフォーマンスを向上させることができます。

メタデータのキャッシングを使用すると、ごくまれに、古い情報が SMB 1.0 クライアントに提供されることがあります。ご使用の環境でこのリスクを回避する必要がある場合は、この機能を有効にしないでください。

SMBメタデータのキャッシュを有効にする

SMBメタデータのキャッシュを有効にすることで、SMB 1.0クライアントのSMBパフォーマンスを向上させることができます。デフォルトでは、SMBメタデータのキャッシングは無効になっています。

ステップ

1. 必要な操作を実行します。

状況	入力するコマンド
共有の作成時にSMBメタデータのキャッシングを有効にする	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache`
既存の共有でSMBメタデータのキャッシングを有効にする	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

関連情報

SMBメタデータキャッシュエントリの有効期間の設定

SMBメタデータキャッシュエントリの有効期間の設定

SMB メタデータキャッシュエントリの有効期間を設定できます。これにより、環境内での SMB メタデータキャッシュのパフォーマンスを最適化できます。デフォルトは10秒です。

開始する前に

SMB メタデータキャッシュ機能を有効にしている必要があります。SMB メタデータのキャッシングが有効でない場合、 SMB キャッシュの TTL 設定は使用されません。

ステップ

1. 必要な操作を実行します。

SMB メタデータキャッシュエントリの有効期間を設定する際の方法	入力するコマンド
共有を作成する	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
既存の共有を変更する	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

共有を作成または変更するときに、追加の共有設定オプションおよび共有プロパティを指定できます。詳細については、マニュアルページを参照してください。

ファイルロックを管理します。

プロトコル間のファイルロックについて

ファイルロックは、別のユーザが以前に開いていたファイルにユーザがアクセスできないようにするためにクライアントアプリケーションで使用される方法です。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クライアントの場合はロックを推奨します。クライアントがSMBクライアントの場合はロックは必須です。

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以前に開いたファイルにNFSクライアントからアクセスすると失敗することがあります。

NFSクライアントがSMBアプリケーションでロックされているファイルにアクセスしようとすると、次の状況が発生します。

- mixed形式またはNTFS形式のボリュームでは、、 `rmdir`などのファイル操作を `rm`mv`行うと、NFSアプリケーションが失敗することがあります。
- NFSの読み取り処理と書き込み処理は、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。
- ファイルの書き込み範囲が排他的なSMBバイトロックでロックされている場合、NFSの書き込み処理が失敗します。
- リンク解除
  - NTFSファイルシステムでは、SMBとCIFSの削除処理がサポートされています。

    ファイルは最後に閉じたあとで削除されます。
  - NFSのリンク解除処理は、サポートされていません。

    サポートされていない理由は、NTFSとSMBのセマンティクスが必要であり、NFSではLast Delete-On-Close処理がサポートされていないためです。
  - UNIXファイルシステムでは、リンク解除操作がサポートされています。

    サポートされている理由は、NFSとUNIXのセマンティクスが必要だからです。
- 名前変更
  - NTFSファイルシステムでは、デスティネーション ファイルがSMBかCIFSから開かれている場合には、デスティネーション ファイルの名前を変更できます。
  - NFSの名前変更はサポートされていません。

    サポートされていない理由は、NTFSとSMBのセマンティクスが必要だからです。

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上の他のすべてのNFS処理では、SMBロック状態が維持されます。

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ます。

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。

ONTAP 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、 ONTAP は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。 ONTAP

- 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、 ONTAP はそのファイルの読み取り専用ビットを有効にします。
- 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、 ONTAP はそのファイルの読み取り専用ビットを無効にします。
- 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 ONTAP 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クライアントがその読み取り専用ビットを無効にすると、ONTAPはそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 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。

ファイル権限の変更は、 SMB クライアントではすぐに反映されますが、 NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理に関する**ONTAP**と**Windows**の違い

Windowsとは異なり、ONTAPはファイルが開いている間、開いているファイルへのパスの各コンポーネントをロックしません。この動作はSMB共有パスにも影響します。

ONTAPではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。その結果、共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、セキュリティ設定を適用して、ユーザやアプリケーションが重要なディレクトリの名前を変更できないようにします。

ロックに関する情報を表示する

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。

タスクの内容

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。

`vserver locks show`このコマンドは、次の4種類のロックに関する情報を表示します。

- 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、各ロックタイプ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。

ステップ

1. コマンドを使用して、ロックに関する情報を表示します `vserver locks show`。

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。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
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します `/data2/data2_2/intro.pptx`。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

ファイルロックによってクライアントがファイルにアクセスできない場合は、現在有効なロックに関する情報を表示して、特定のロックを解除できます。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。

タスクの内容

コマンドは `vserver locks break`、advanced権限レベル以上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、コマンドを使用し `vserver locks show`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`

4. admin権限レベルに戻ります。 `set -privilege admin`

SMBアクティビティの監視

SMBセッション情報を表示する

SMB接続、SMB Session ID、セッションを使用しているワークステーションのIPアドレスなど、確立されているSMBセッションに関する情報を表示できます。セッションのSMBプロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうかを確認するのに役立ちます。

タスクの内容

SVM上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのパラメータを使用すると、選択したフィールドに関する出力を表示できます `-fields`。

  と入力して、使用できるフィールドを指定できます `-fields ?`。

- パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます `-instance`。
- パラメータまたは `-instance`パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます `-fields`。

ステップ

1. 次のいずれかを実行します。

表示する **SMB** セッション情報	入力するコマンド
SVM上のすべてのセッション（要約形式）	`vserver cifs session show -vserver vserver_name`
指定した接続IDのファイル	`vserver cifs session show -vserver vserver_name -connection-id integer`
指定したワークステーションのIPアドレスから	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定したLIF IPアドレスのファイル	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
指定したノードのオブジェクト	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	指定したWindowsユーザからのセッション
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	指定した認証メカニズムを使用している場合
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
指定したプロトコルバージョンを使用している場合	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 継続的可用性を備えた保護とSMBマルチチャネルは、SMB 3.0以降のセッションでのみ使用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を以降に設定します。 `SMB3` ====
指定したレベルの継続的可用性を備えた保護を使用しているセッション	`vserver cifs session show -vserver vserver_name -continuously-available {No

表示する **SMB** セッション情報	入力するコマンド
Yes	Partial}`  [NOTE] ==== 継続的可用性のステータスがの場合は `Partial`、継続的可用性を備えた開いているファイルがセッションに少なくとも1つ含まれていますが、継続的可用性を備えた保護を使用して開かれていないファイルがセッションに含まれています。コマンドを使用すると、確立されたセッションのファイルのうち、継続的可用性を備えた保護を使用して開かれていないファイルを確認できます `vserver cifs sessions file show`。 ====
指定したSMB署名セッションステータスのセッション	`vserver cifs session show -vserver vserver_name -is-session-signed {true

例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。接続はドメインアカウントを使用して行われました。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

次のコマンドを実行すると、SVM vs1上のSMB 3.0とSMBマルチチャネルを使用しているセッションに関するセッション情報が表示されます。この例では、ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するには、Kerberos認証を使用して接続を確立する必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

関連情報

開いているSMBファイルに関する情報の表示

開いている**SMB**ファイルに関する情報を表示する

SMB接続とSession ID、ホスティングボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうかを確認するのに役立ちます。

タスクの内容

確立されたSMBセッションで開いているファイルに関する情報を表示できます。表示される情報は、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと継続的可用性を備えた保護を使用して開かれていないファイルがある場合（コマンド出力のフィールド `vserver cifs session show`の値 `-continuously-available`は `Partial`）、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

オプションのパラメータを何も指定せずにコマンドを実行することで、Storage Virtual Machine（SVM）上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show`。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションのパラメータを使用すると、選択したフィールドの出力を表示できます `-fields`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

- パラメータを使用すると、開いているSMBファイルに関する詳細情報を表示できます `-instance`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

ステップ

1. 次のいずれかを実行します。

表示する開いている **SMB** ファイル	入力するコマンド
SVM上のファイル（要約形式）	`vserver cifs session file show -vserver vserver_name`
指定したノードのオブジェクト	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	指定したファイルIDのファイル
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定したSMB接続IDのファイル
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定したSMB Session IDのファイル
`vserver cifs session file show -vserver vserver_name -session-id integer`	指定したホストアグリゲートのファイル
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	指定したボリュームのファイル
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定したSMB共有のファイル

表示する開いている **SMB** ファイル	入力するコマンド
`vserver cifs session file show -vserver vserver_name -share share_name`	指定したSMBパスのファイル
`vserver cifs session file show -vserver vserver_name -path path`	指定したレベルの継続的可用性を備えた保護を使用している
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 継続的可用性のステータスがの場合は `No`、開いているファイルがテイクオーバーやギブバックからの無停止でのリカバリに対応していません。また、ハイアベイラビリティ関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。 ====
指定した再接続状態のファイル	`vserver cifs session file show -vserver vserver_name -reconnected {No`

出力結果の絞り込みに使用できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

関連情報

SMBセッション情報の表示

使用可能な統計オブジェクトとカウンタの確認

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	`statistics catalog object show`
使用可能な特定のオブジェクト	`statistics catalog object show object object_name`
使用可能なカウンタ	`statistics catalog counter show object object_name`

使用可能なオブジェクトとカウンタの詳細については、マニュアルページを参照してください。

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次のコマンドを実行すると、advanced権限レベルで表示した場合の、クラスタ内のCIFSアクセスとSMBアクセスに関連する選択した統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

次のコマンドを実行すると、advanced権限レベルで表示したオブジェクトの一部のカウンタに関する情報が表示され `cifs`ます。

この例で表示されているのはオブジェクトの使用可能なカウンタの一部ではありませ `cifs`ん。出力は省略されています。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- ----------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

関連情報

統計の表示

統計を表示する

パフォーマンスの監視と問題の診断を行うために、CIFSとSMB、監査、BranchCacheハッシュに関する統計など、さまざまな統計を表示できます。

開始する前に

オブジェクトに関する情報を表示する前に、コマンドと `statistics stop`コマンドを使用してデータサンプルを収集しておく必要があり `statistics start`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。

統計を表示する対象	入力するコマンド
SMBのすべてのバージョン	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.xおよびSMB 3.0	`statistics show -object smb2`
ノードのCIFSサブシステム	`statistics show -object nblade_cifs`
マルチプロトコルの監査	`statistics show -object audit_ng`
BranchCacheハッシュサービス	`statistics show -object hashd`
動的DNS	`statistics show -object ddns_update`

詳細については、各コマンドのマニュアルページを参照してください。

3. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

使用可能な統計オブジェクトと統計カウンタの確認

SMB署名済みセッションの統計の監視

BranchCache統計の表示

統計を使用した自動ノードリファーラルアクティビティの監視

"Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"

"パフォーマンス監視のセットアップ"

SMBクライアントベースのサービスを導入する

オフラインファイルを使用してオフラインで使用するファイルをキャッシュできるようにする

オフラインファイルを使用してオフラインで使用するファイルのキャッシュを許可する概要

ONTAP では、 Microsoft のオフラインファイル機能（ _ クライアント側キャッシュ _ ）をサポートしています。これにより、オフラインで使用するファイルをローカルホストにキャッシュできます。オフラインファイル機能を使用すると、ネットワークから切断されていてもファイルの処理を継続できます。

Windowsのユーザドキュメントやプログラムを共有に自動的にキャッシュするかどうか、またはキャッシュするファイルを手動で選択する必要があるかどうかを指定できます。新しい共有では手動キャッシュがデフォルトで有効になります。オフラインで使用可能になったファイルは、Windowsクライアントのローカルディスクと同期されます。同期は、特定のストレージシステム共有へのネットワーク接続がリストアされたときに実行されます。

オフラインのファイルやフォルダへのアクセス権は、CIFSサーバに保存されているファイルやフォルダと同じになるため、オフラインのファイルやフォルダに対して操作を実行するには、CIFSサーバに保存されているファイルやフォルダに対する十分な権限がユーザに必要です。

ユーザーとネットワーク上の他のユーザーが同じファイルに変更を加えた場合、ユーザーはファイルのローカルバージョンをネットワークに保存するか、他のバージョンを保持するか、またはその両方を保存できます。ユーザが両方のバージョンを保持している場合、ローカルユーザの変更を含む新しいファイルがローカルに保存され、キャッシュされたファイルはCIFSサーバに保存されているバージョンの変更で上書きされます。

共有ごとにオフラインファイルを設定するには、共有設定を使用します。共有を作成または変更するときに、次の4つのオフラインフォルダ設定のいずれかを選択できます。

- キャッシュなし

  共有のクライアント側キャッシュを無効にします。クライアントのローカルにファイルやフォルダが自動的にキャッシュされず、ユーザがファイルやフォルダをローカルにキャッシュすることもできません。

- 手動キャッシュ

  共有にキャッシュするファイルを手動で選択できるようにします。これがデフォルト設定です。デフォルトでは、ファイルやフォルダはローカルクライアントにキャッシュされません。オフラインで使用するためにローカルにキャッシュするファイルやフォルダをユーザが選択できます。

- ドキュメントの自動キャッシュ

  ユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイルとフォルダだけです。

- プログラムの自動キャッシュ

  プログラムとユーザのドキュメントを共有に自動的にキャッシュできるようにします。ローカルにキャッシュされるのは、アクセスしたファイル、フォルダ、およびプログラムだけです。さらに、この設定により、クライアントはネットワークに接続されている場合でも、ローカルにキャッシュされた実行可能ファ

イルを実行できます。

Windowsサーバおよびクライアントでのオフラインファイルの設定の詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザプロファイルの一元的な格納

フォルダリダイレクトを使用したCIFSサーバへのデータの格納

BranchCacheを使用したブランチオフィスでのSMB共有のコンテンツのキャッシュ

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

オフラインファイルを使用するための要件

CIFS サーバで Microsoft のオフラインファイル機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAP の各リリースでオフラインファイルがサポートされます。

SMBプロトコルのバージョン

Storage Virtual Machine （ SVM ONTAP ）については、すべてのバージョンの SMB でオフラインファイルがサポートされます。

Windowsクライアントの要件

Windows クライアントでオフラインファイルがサポートされている必要があります。

オフラインファイル機能をサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

"mysupport.netapp.com/matrix"

オフラインファイルの導入に関するガイドライン

ホームディレクトリに共有プロパティが設定されているホームディレクトリ共有にオフラインファイルを導入する場合は、いくつかの重要なガイドラインについて理解しておく必要があり `showsnapshot`ます。

オフラインファイルが設定されているホームディレクトリ共有で共有プロパティが設定されている場合、`showsnapshot`Windowsクライアントはすべての`Snapshot`コピーをユーザのホームディレクトリ内のフォルダの下にキャッシュします `~snapshot`。

次のいずれかに該当する場合、 Windows クライアントでは、すべての Snapshot コピーがホームディレクトリの下にキャッシュされます。

- ユーザが、ホームディレクトリをクライアントからオフラインで利用できるようにしている。

  ホームディレクトリ内のフォルダの内容 `~snapshot`も含まれ、オフラインで使用できるようになります。

- ユーザが、などのフォルダをCIFSサーバ共有にあるホームディレクトリのルートにリダイレクトするようにフォルダリダイレクトを設定している `My Documents`。

  Windows クライアントによっては、リダイレクトされたフォルダが自動的にオフラインで利用できるようになる場合があります。フォルダがホームディレクトリのルートにリダイレクトされる場合、その `~snapshot`フォルダはキャッシュされたオフラインコンテンツに含まれます。

> フォルダがオフラインファイルに含まれているオフラインファイルの展開 `~snapshot`は避ける必要があります。フォルダ内の`Snapshot`コピー `~snapshot`には、`ONTAP`が`Snapshot`コピーを作成した時点のボリューム上のすべてのデータが含まれています。そのため、フォルダのオフラインコピーを作成すると `~snapshot`、クライアントのローカルストレージが大量に消費され、オフラインファイルの同期中にネットワーク帯域幅が消費され、オフラインファイルの同期にかかる時間が長くなります。

CLIを使用した**SMB**共有でのオフラインファイルサポートの設定

ONTAP CLIを使用してオフラインファイルのサポートを設定するには、SMB共有の作成時に、または既存のSMB共有の変更時にいつでも、4つのオフラインファイル設定のいずれかを指定します。デフォルトの設定は、オフラインファイルの手動サポートです。

タスクの内容

オフラインファイルのサポートを設定する場合は、次の4つのオフラインファイル設定のいずれかを選択できます。

設定	説明
`none`	Windowsクライアントがこの共有のファイルをキャッシュすることを禁止します。
`manual`	Windowsクライアントのユーザが、キャッシュするファイルを手動で選択できるようにします。
`documents`	Windowsクライアントがオフラインアクセスのために使用するユーザドキュメントをキャッシュすることを許可します。
`programs`	Windowsクライアントがオフラインアクセスのために使用するプログラムをキャッシュすることを許可します。クライアントは、共有が使用可能な場合でも、キャッシュされたプログラムファイルをオフラインモードで使用できます。

選択できるオフラインファイル設定は1つだけです。既存のSMB共有でオフラインファイル設定を変更すると、元の設定が新しいオフラインファイル設定に置き換えられます。その他の既存のSMB共有設定および共

有プロパティは削除も置き換えもされません。これらは、明示的に削除または変更されるまで有効です。

手順

1. 適切な操作を実行します。

オフラインファイルを設定する対象	入力するコマンド
新しいSMB共有	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	既存のSMB共有
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. SMB共有の設定が正しいことを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

例

次のコマンドは、オフラインファイルをに設定して「data1」という名前のSMB共有を作成します `documents`。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

次のコマンドは、オフラインファイルの設定をに変更し、ファイルモードおよびディレクトリモードの作成マスクの値を追加することで、「data1」という名前の既存のSMB共有を変更します。 `manual`

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

関連情報

既存のSMB共有に対する共有プロパティの追加または削除

コンピュータの管理**MMC**を使用した**SMB**共有でのオフラインファイルサポートの設定

オフラインで使用するためにファイルをローカルにキャッシュすることをユーザに許可する場合は、コンピュータの管理 MMC （ Microsoft 管理コンソール）を使用してオフラインファイルのサポートを設定できます。

手順

1. Windows サーバー上の MMC を開くには、 Windows エクスプローラで、ローカルコンピューターのアイコンを右クリックし、 * 管理 * を選択します。
2. 左側のパネルで、「 * コンピュータの管理 * 」を選択します。
3. 「 * アクション * > * 別のコンピューターに接続 * 」を選択します。

   [コンピュータの選択] ダイアログボックスが表示されます。

4. CIFS サーバの名前を入力するか、 * Browse * をクリックして CIFS サーバを指定します。

   CIFSサーバの名前がStorage Virtual Machine（SVM）ホスト名と同じ場合は、SVM名を入力しま

す。CIFS サーバの名前が SVM ホスト名と異なる場合は、 CIFS サーバの名前を入力します。

5. [OK]*をクリックします。
6. コンソールツリーで、 * システムツール * > * 共有フォルダー * をクリックします。
7. [* 共有] をクリックします。
8. 結果ペインで、共有を右クリックします。
9. * プロパティ * をクリックします。

   選択した共有のプロパティが表示されます。

10. [一般 *] タブで、 [* オフライン設定 *] をクリックします。

    [オフライン設定] ダイアログボックスが表示されます。

11. 必要に応じて、オフラインの可用性オプションを設定します。
12. [OK]*をクリックします。

移動プロファイルを使用して、**SVM**に関連付けられた**SMB**サーバにユーザプロファイルを一元的に格納する

移動プロファイルを使用して、**SVM**の概要に関連付けられた**SMB**サーバにユーザプロファイルを一元的に格納する

ONTAPでは、Windowsの移動プロファイルの格納をサポートしており、Storage Virtual Machine（SVM）に関連付けられたCIFSサーバに格納できます。ユーザ移動プロファイルを設定すると、ユーザはどこでログインしても自動でリソースを利用できるようになります。また、ユーザ プロファイルの管理が簡単になり、管理者にとってもメリットがあります。

移動ユーザプロファイルには、次の利点があります。

- 自動でリソースを利用できる

  ユーザーがWindows 8、Windows 7、Windows 2000、またはWindows XPを実行しているネットワーク上のコンピュータにログインすると、ユーザーの一意のプロファイルが自動的に使用可能になります。ユーザは、ネットワーク上で使用する各コンピュータでプロファイルを作成する必要はありません。

- コンピュータの交換が簡単

  ユーザのプロファイル情報はすべてネットワーク上で個別に管理されるため、ユーザのプロファイルは新しい交換用コンピュータに簡単にダウンロードできます。ユーザが新しいコンピュータに初めてログインしたときに、サーバに保存されているユーザのプロファイルが新しいコンピュータにコピーされます。

関連情報

オフラインファイルを使用したオフラインで使用するファイルのキャッシュ

フォルダリダイレクトを使用したCIFSサーバへのデータの格納

CIFSサーバでMicrosoftの移動プロファイルを使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAPでは、移動プロファイルがサポートされます。

SMBプロトコルのバージョン

Storage Virtual Machine（SVM）についてはONTAP、すべてのバージョンのSMBで移動プロファイルがサポートされます。

Windowsクライアントの要件

移動プロファイルを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。

移動プロファイルをサポートするWindowsクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ユーザがネットワーク上の任意のコンピュータにログオンしたときにそのユーザのプロファイルを自動的に使用可能にするには、[Active Directoryユーザーとコンピュータ]MMCスナップインで移動プロファイルを設定します。Windows Serverで移動プロファイルを設定する場合は、Active Directory管理センターを使用します。

手順

1. Windowsサーバーで、Active DirectoryユーザーとコンピュータMMC（またはWindowsサーバーのActive Directory管理センター）を開きます。
2. 移動プロファイルを設定するユーザを見つけます。
3. ユーザーを右クリックし、 * プロパティ * をクリックします。
4. [プロファイル]*タブで、ユーザの移動プロファイルを保存する共有のプロファイルパスを入力し、続けてを入力します `%username%`。

   たとえば、プロファイルパスは次のようになります `\\vs1.example.com\profiles\%username%`。ユーザが初めてログインすると、 `%username%`はそのユーザの名前に置き換えられます。

   > パスの `\\vs1.example.com\profiles\%username%` `profiles`は、すべてのメンバーにフルコントロール権限が割り当てられているStorage Virtual Machine（SVM）vs1上の共有の共有名です。

5. [OK]*をクリックします。

フォルダリダイレクトを使用して**SMB**サーバにデータを格納する

フォルダリダイレクトを使用した**SMB**サーバへのデータの格納の概要

ONTAPでは、Microsoftのフォルダリダイレクトがサポートされています。ユーザや管理者は、この機能を使用して、ローカルフォルダのパスをCIFSサーバ上の場所にリダイレクトできます。リダイレクトされたフォルダは、データがSMB共有に格納されていても、ローカルのWindowsクライアントに格納されているように見えます。

フォルダリダイレクトは、主に、ホームディレクトリをすでに導入していて、既存のホームディレクトリ環境との互換性を維持したい組織を対象としています。

- `Documents`、 `Desktop`、および `Start Menu`は、リダイレクト可能なフォルダの例です。
- ユーザはWindowsクライアントからフォルダをリダイレクトできます。
- 管理者は、Active DirectoryでGPOを設定することで、フォルダリダイレクトを一元的に設定および管理できます。
- 管理者が移動プロファイルを設定している場合、フォルダリダイレクトを使用すると、管理者はユーザデータをプロファイルデータから分割できます。
- フォルダリダイレクトとオフラインファイルを使用して、ユーザがコンテンツをローカルにキャッシュしながら、ローカルフォルダのデータストレージをCIFSサーバにリダイレクトできます。

関連情報

オフラインファイルを使用したオフラインで使用するファイルのキャッシュ

移動プロファイルを使用したSVMに関連付けられたCIFSサーバへのユーザプロファイルの一元的な格納

フォルダリダイレクトを使用するための要件

CIFS サーバで Microsoft のフォルダリダイレクトを使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAP は、 Microsoft のフォルダリダイレクトをサポートしています

SMBプロトコルのバージョン

Storage Virtual Machine （ SVM ）については、 ONTAP のすべてのバージョンの SMB で Microsoft のフォルダリダイレクトがサポートされます。

Windowsクライアントの要件

Microsoft のフォルダリダイレクトを使用するには、 Windows クライアントでこの機能がサポートされている必要があります。

フォルダリダイレクトをサポートする Windows クライアントに関する最新情報については、 Interoperability Matrix を参照してください。

"mysupport.netapp.com/matrix"

フォルダリダイレクトの設定

Windowsの[プロパティ]ウィンドウを使用して、フォルダリダイレクトを設定できます。この方法を使用する利点は、WindowsユーザがSVM管理者の支援なしでフォルダリダイレクトを設定できることです。

手順

1. エクスプローラで、ネットワーク共有にリダイレクトするフォルダを右クリックします。
2. * プロパティ * をクリックします。

   選択した共有のプロパティが表示されます。

3. [* ショートカット *] タブで、 [* ターゲット *] をクリックし、選択したフォルダーをリダイレクトするネットワーク上の場所へのパスを指定します。

   たとえば、にマッピングされているホームディレクトリ内のフォルダ `Q:\` にフォルダをリダイレクトする場合 `data` は、をターゲットとして指定します `Q:\data`。

4. [OK]*をクリックします。

   オフラインフォルダの設定の詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

SMB 2.xを使用して**Windows**クライアントから**~snapshot**ディレクトリにアクセスする

SMB 2.xを使用するWindowsクライアントからのディレクトリへのアクセスに使用する方法 `~snapshot`は、SMB 1.0の場合とは異なります。SMB 2.x接続を使用してSnapshotコピーに格納されたデータに正常にアクセスするためのディレクトリへのアクセス方法について理解しておく必要があり `~snapshot`ます。

SVM管理者は、vserver cifs share propertiesファミリーのコマンドを使用して共有プロパティを有効または無効にすることで、Windowsクライアントのユーザが共有のディレクトリを表示してアクセスできるかどうかを制御します `~snapshot`。 `showsnapshot`

共有プロパティが無効になっている場合、 `showsnapshot` `SMB 2.x` を使用する `Windows` クライアントのユーザは、ディレクトリのパスまたはディレクトリ内の特定の `Snapshot` コピーのパスを手動で入力しても、 `~snapshot` ディレクトリを表示できず、ディレクトリ内の `Snapshot` コピーにアクセスできませ `~snapshot` ん `~snapshot`。

共有プロパティが有効になっている場合 `showsnapshot` でも、 `SMB 2.x` を使用する `Windows` クライアントのユーザは、共有のルートにあるディレクトリ、または共有のルートより下のジャンクションまたはディレクトリ内のディレクトリを表示できません `~snapshot`。ただし、共有に接続したユーザは、共有パスの末尾にを手動で追加することで、非表示のディレクトリに `\~snapshot` アクセスできます `~snapshot`。非表示の `~snapshot` ディレクトリには、次の2つのエントリポイントからアクセスできます。

- 共有のルート
- 共有スペースのすべてのジャンクションポイント

非表示の `~snapshot`ディレクトリには、共有内のジャンクション以外のサブディレクトリからはアクセスできません。

例

次の例に示す設定では、「eng'」共有へのSMB 2.x接続を使用するWindowsクライアントのユーザが、共有パス（共有のルートおよびパス内のすべてのジャンクションポイント）に手動でを追加することで、ディレクトリにアクセスできます `~snapshot`。 `\~snapshot`非表示の `~snapshot`ディレクトリには、次の3つのパスからアクセスできます。

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

以前のバージョン機能を使用したファイルとフォルダのリカバリ

[以前のバージョン**]**機能を使用したファイルとフォルダのリカバリの概要

Microsoft の以前のバージョン機能は、 Snapshot コピーを何らかの形でサポートしているファイルシステムで、それらが有効になっている場合に使用できます。Snapshot テクノロジは ONTAP に不可欠なテクノロジの 1 つです。ユーザは、 Windows クライアントで Microsoft の以前のバージョン機能を使用して、 Snapshot コピーからファイルとフォルダをリカバリできます。

以前のバージョン機能を使用すると、ストレージ管理者の手を借りなくても、一連の Snapshot コピーを参照したり、 Snapshot コピーからデータをリストアしたりできます。以前のバージョン機能は設定できません。常に有効になります。ストレージ管理者が Snapshot コピーを共有で使用できるようにした場合、ユーザは以前のバージョン機能を使用して次の作業を実行できます。

- 誤って削除したファイルをリカバリする。
- 誤って上書きしたファイルをリカバリする。
- 作業中にファイルのバージョンを比較します。

Snapshot コピーに格納されているデータは読み取り専用です。ファイルに変更を加えるには、ファイルのコピーを別の場所に保存する必要があります。Snapshot コピーは定期的に削除されるため、以前のバージョンのファイルを残しておく場合は、以前のバージョン機能で格納されたファイルのコピーを作成しておく必要があります。

Microsoftの以前のバージョン機能を使用するための要件

CIFSサーバで[以前のバージョン]機能を使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとWindowsクライアントの種類について確認しておく必要があります。また、Snapshotコピー設定の要件についても理解しておく必要があります。

ONTAPのバージョンの要件

以前のバージョンをサポートします。

SMBプロトコルのバージョン

Storage Virtual Machine（SVM）についてはONTAP、すべてのバージョンのSMBで[以前のバージョン]機能がサポートされます。

Windowsクライアントの要件

[以前のバージョン]機能を使用してSnapshotコピーのデータにアクセスするには、Windowsクライアントでこの機能がサポートされている必要があります。

[以前のバージョン]機能をサポートするWindowsクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

Snapshotコピーの設定の要件

[以前のバージョン]機能を使用してSnapshotコピーのデータにアクセスするには、有効なSnapshotポリシーがデータを含むボリュームに関連付けられ、クライアントがSnapshotデータにアクセスできること、およびSnapshotコピーが存在していることが必要です。

[以前のバージョン**]**タブを使用して**Snapshot**コピーデータを表示および管理

Windowsクライアントマシンでは、Windowsの[プロパティ]ウィンドウの[以前のバージョン]タブを使用して、Storage Virtual Machine（SVM）管理者の手を借りなくても、Snapshotコピーに格納されたデータをユーザがリストアできます。

タスクの内容

SVMに格納されたSnapshotコピーのデータを[以前のバージョン]タブで表示および管理できるのは、管理者が共有を含むボリュームでSnapshotコピーを有効にし、Snapshotコピーを表示するように共有を設定している場合のみです。

手順

1. エクスプローラで、CIFSサーバに格納されているデータのマッピングされたドライブの内容を表示します。
2. Snapshotコピーを表示または管理するマッピングされたネットワークドライブ内のファイルまたはフォルダを右クリックします。
3. * プロパティ * をクリックします。

   選択したファイルまたはフォルダのプロパティが表示されます。

4. [以前のバージョン *] タブをクリックします。

   選択したファイルまたはフォルダの使用可能なSnapshotコピーのリストが、[Folder Versions]ボックスに表示されます。表示されたSnapshotコピーは、Snapshotコピー名のプレフィックスと作成時のタイムスタンプで識別されます。

5. [* フォルダーバージョン： *] ボックスで、管理するファイルまたはフォルダーのコピーを右クリックします。
6. 適切な操作を実行します。

状況	操作
Snapshotコピーのデータを表示する	• 開く * をクリックします。
そのSnapshotコピーのデータのコピーを作成する	[* コピー（ Copy ）] をクリックします

   Snapshotコピーのデータは読み取り専用です。[以前のバージョン]タブに表示されているファイルやフォルダに変更を加える場合は、変更するファイルやフォルダのコピーを書き込み可能な場所に保存し、コピーに変更を加える必要があります。

7. スナップショット・データの管理が終了したら **'OK** をクリックして * プロパティ * ダイアログ・ボックスを閉じます

   [以前のバージョン]タブを使用したSnapshotデータの表示と管理の詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

以前のバージョン機能で**Snapshot**コピーを使用できるかどうかの確認

[以前のバージョン]タブからSnapshotコピーを表示できるのは、共有を含むボリュームに有効なSnapshotポリシーが適用されていて、ボリューム設定でSnapshotコピーへのアクセスが許可されている場合のみです。Snapshotコピーを使用できるかどうかを確認すると、ユーザが[以前のバージョン]機能にアクセスできるかどうかを確認するときに役立ちます。

手順

1. 共有データが存在するボリュームで自動Snapshotコピーが有効になっているかどうか、およびクライアン

トがSnapshotディレクトリにアクセスできるかどうかを確認します。 `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

出力には、ボリュームに関連付けられているSnapshotポリシー、クライアントのSnapshotディレクトリアクセスが有効かどうか、および使用可能なSnapshotコピーの数が表示されます。

2. 関連付けられているSnapshotポリシーが有効になっているかどうかを確認します。 `volume snapshot policy show -policy policy-name`
3. 使用可能なSnapshotコピーの一覧を表示します。 `volume snapshot show -volume volume_name`

SnapshotポリシーとSnapshotスケジュールの設定と管理の詳細については、を参照してください"データ保護"。

例

次の例は、「 `data`」 上の共有データと使用可能な Snapshot コピーを含む「 `data`」 という名前のボリュームに関連付けられている Snapshot ポリシーに関する情報を表示します。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                     3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- ------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

関連情報

以前のバージョン機能のアクセスを有効にするSnapshot設定の作成

"データ保護"

Snapshot設定を作成して以前のバージョン機能のアクセスを有効にする

Snapshotコピーへのクライアントアクセスが有効で、Snapshotコピーが存在する場合は、[以前のバージョン]機能をいつでも使用できます。Snapshotコピーの設定がこれらの要件を満たしていない場合は、要件を満たすSnapshotコピーの設定を作成できます。

手順

1. 以前のバージョン機能からのアクセスを許可する共有が含まれているボリュームにSnapshotポリシーが関連付けられていない場合は、コマンドを使用して、Snapshotポリシーをボリュームに関連付けて有効にします `volume modify`。

   コマンドの使用の詳細については `volume modify`、マニュアルページを参照してください。

2. コマンドを使用してオプションをに `true`設定し、 `-snap-dir`Snapshotコピーへのアクセスを有効にし `volume modify`ます。

   コマンドの使用の詳細については `volume modify`、マニュアルページを参照してください。

3. コマンドと `volume snapshot policy show`コマンドを使用して、Snapshotポリシーが有効になっていること、およびSnapshotディレクトリへのアクセスが有効になっていることを確認します `volume show`。

   コマンドと `volume snapshot policy show`コマンドの使用の詳細については `volume show`、マニュアルページを参照してください。

   SnapshotポリシーとSnapshotスケジュールの設定と管理の詳細については、を参照してください"データ保護"。

関連情報

"データ保護"

ジャンクションを含むディレクトリのリストアに関するガイドライン

以前のバージョン機能を使用してジャンクションポイントを含むフォルダをリストアする場合は、一定のガイドラインに注意する必要があります。

以前のバージョンを使用して、ジャンクションポイントである子フォルダを含むフォルダをリストアすると、リストアがエラーで失敗することがあります `Access Denied`。

リストアしようとしているフォルダにジャンクションが含まれているかどうかを確認するには、 `vol show`コマンドでオプションを指定し `-parent`ます。コマンドを使用して、ファイルやフォルダのアクセスに関する問題に関する詳細なログを作成することもできます `vserver security trace`。

関連情報

NASネームスペースでのデータボリュームの作成と管理

SMBサーバベースのサービスの導入

ホームディレクトリを管理します。

ONTAPニオケルドウテキホームディレクトリノシクミ

ONTAP ホームディレクトリを使用すると、 SMB 共有を設定し、ユーザと一連の変数に基づいてさまざまなディレクトリにマッピングすることができます。ユーザごとに別個の共有を作成するのではなく、 1 つの共有を設定し、いくつかのホームディレクトリパ

ラメータを指定して、エントリポイント（共有）とホームディレクトリ（ SVM 上のディレクトリ）間の関係をユーザ単位で定義します。

ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。ユーザとディレクトリのマッピング方法を決定する 4 つの変数があります。

- * 共有名 *

  ユーザの接続先として作成する共有の名前です。この共有にはホームディレクトリのプロパティを設定する必要があります。

  共有名には、次の動的な名前を使用できます。

  - `%w`（ユーザのWindowsユーザ名）
  - `%d`（ユーザのWindowsドメイン名）
  - `%u`（ユーザのマッピングされたUNIXユーザ名）すべてのホームディレクトリ間で共有名を一意にするには、共有名にまたは `%u`変数を使用する必要があります/%w`。共有名には変数と/`%w`変数の両方を使用することも（など `%d/%w`）、静的な部分と変数の部分を使用することも（home_など/`%w`）できます `%d`。

- * 共有パス *

  共有によって定義される、つまり、共有名の 1 つに関連付けられる相対パスです。各検索パスに付加されて、 SVM のルートからのユーザのホームディレクトリの完全パスを生成します。静的（例：）、動的（例：）、または2つの組み合わせ（例： `%w`）を `eng/%w`指定できます `home`。

- * 検索パス *

  SVM のルートからの絶対パスのセットで、 ONTAP ではこのパスに基づいてホームディレクトリが検索されます。コマンドを使用すると、1つ以上の検索パスを指定できます `vserver cifs home-directory search-path add`。複数の検索パスを指定すると、ONTAPは有効なパスが見つかるまで、指定された順序で検索パスを試行します。

- * ディレクトリ *

  ユーザに対して作成する、そのユーザのホームディレクトリです。通常、ディレクトリ名はユーザの名前です。ホームディレクトリは、検索パスで定義されるいずれかのディレクトリに作成する必要があります。

たとえば、次のように設定します。

- ユーザ： John Smith
- ユーザのドメイン： acme
- ユーザ名： jsmith
- SVM 名： vs1
- ホームディレクトリ共有名#1：home_ `%w`-共有パス： `%w`
- ホームディレクトリ共有名#2： `%w`-共有パス： `%d/%w`

- 検索パス#1： `/vol0home/home`
- 検索パス#2： `/vol1home/home`
- 検索パス#3： `/vol2home/home`
- ホームディレクトリ： `/vol1home/home/jsmith`

シナリオ1：ユーザーがに接続し `\\vs1\home_jsmith`ます。これは最初のホームディレクトリ共有名に一致し、相対パスが生成され `jsmith`ます。ONTAPでは、各検索パスが順にチェックされ、という名前のディレクトリが検索されるようになりまし `jsmith`た。

- `/vol0home/home/jsmith`は存在しません。検索パス#2に進みます。
- `/vol1home/home/jsmith`は存在します。したがって、検索パス#3はチェックされません。これで、ユーザは自分のホームディレクトリに接続されました。

シナリオ2：ユーザーがに接続します `\\vs1\jsmith`。これは2番目のホームディレクトリ共有名に一致し、相対パスが生成され `acme/jsmith`ます。ONTAPでは、各検索パスが順にチェックされ、という名前のディレクトリが検索されるようになりまし `acme/jsmith`た。

- `/vol0home/home/acme/jsmith`は存在しません。検索パス#2に進みます。
- `/vol1home/home/acme/jsmith`は存在しません。検索パス#3に進みます。
- `/vol2home/home/acme/jsmith`は存在しません。ホームディレクトリが存在しないため、接続は失敗します。

ホームディレクトリ共有

ホームディレクトリ共有を追加する

SMBホームディレクトリ機能を使用する場合は、ホームディレクトリプロパティが設定された共有を少なくとも1つ追加する必要があります。

タスクの内容

ホームディレクトリ共有は、共有の作成時にコマンドを使用して作成できます `vserver cifs share create`。既存の共有をホームディレクトリ共有に変更するには、コマンドを使用します `vserver cifs share modify`。

ホームディレクトリ共有を作成するには、共有を作成または変更するときにオプションに値 `-share-properties`を指定する必要があります `homedirectory`。共有名と共有パスは変数を使用して指定できます。変数はユーザがホームディレクトリに接続するときに動的に拡張されます。パスに使用できる変数は、 `%w`、 `%d`、および `%u`です。それぞれ、Windowsユーザ名、ドメイン、およびマッピングされたUNIXユーザ名に対応します。

手順

1. ホームディレクトリ共有を追加します。+
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver` `vserver`検索パスを追加するCIFS対応のStorage Virtual Machine（SVM）を指定します。

   `-share-name` *`share-name`*ホームディレクトリ共有名を指定します。

必要な変数の1つに加えて、リテラル文字列 `%u`、、またはの `%d`いずれかが共有名に含まれている場合は `%w`、リテラル文字列の前に%（パーセント）文字を付けて、ONTAPがリテラル文字列を変数として処理しないようにする必要があります（例： `%%w`）。

- 共有名には変数またはの `%u`いずれかを使用する必要があります `%w`。
- 共有名には、さらに変数（など `%d`/`%w`）を含めることも、静的な部分（例：home1_/`%w`）を含めることもできます `%d`。
- 管理者が、他のユーザのホームディレクトリに接続するために、またはユーザが他のユーザのホームディレクトリに接続するのを許可するために共有を使用する場合は、動的な共有名のパターンの先頭にチルダ（ ~ ）を付ける必要があります。

> `vserver cifs home-directory modify`このアクセスを有効にするには、オプションを `true`に設定する `-is-home-dirs-access-for-admin-enabled`か、アドバンストオプションをに `true`設定します `-is-home-dirs-access-for-public-enabled`。

`-path` `path`ホームディレクトリの相対パスを指定します。

`-share-properties homedirectory[,…]`その共有の共有プロパティを指定します。値を指定する必要があり `homedirectory`ます。追加の共有プロパティをカンマで区切って指定できます。

1. コマンドを使用して、ホームディレクトリ共有が追加されたことを確認します `vserver cifs share show`。

例

次のコマンドは、という名前のホームディレクトリ共有を作成し `%w`ます。 `oplocks` `browsable`、、および `changenotify`共有プロパティは、共有プロパティに加えて設定され `homedirectory`ます。

> この例で表示されているのは、SVM上のすべての共有の出力ではありません。出力は省略されています。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path          Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

関連情報

ホームディレクトリ検索パスの追加

自動ノードリファーラルの使用に関する要件とガイドライン

ユーザのホームディレクトリへのアクセスの管理

ホームディレクトリ共有での一意なユーザ名の必要性

（Windowsユーザ名）変数または（UNIXユーザ名） `%u`変数を使用してホームディレクトリ共有を動的に生成する場合は、一意のユーザ名を割り当てるように注意してください `%w`。共有名はユーザ名にマッピングされます。

静的共有の名前とユーザの名前が同じ場合、次の 2 つの問題が発生する可能性があります。

- ユーザがコマンドを使用してクラスタ上の共有の一覧を表示する `net view`と、同じユーザ名の2つの共有が表示されます。
- ユーザがその共有名に接続すると、常に静的共有に接続され、同じ名前のホームディレクトリ共有にはアクセスできません。

たとえば、「 administrator 」という名前の共有があり、「 administrator 」という名前の Windows ユーザ名が割り当てられているとします。ホーム・ディレクトリ共有を作成し、その共有に接続すると、「管理者」のホーム・ディレクトリ共有ではなく、「管理者」の静的共有に接続されます。

共有名が重複している問題を解決するには、次のいずれかの手順を実行します。

- 静的共有の名前を変更し、ユーザのホームディレクトリ共有と競合しないようにします。
- ユーザに新しいユーザ名を割り当てて、静的共有名と競合しないようにします。
- パラメータを使用する代わりに、「home」などの静的な名前を使用してCIFSホームディレクトリ共有を作成し、`%w`共有名との競合を回避します。

アップグレード後に静的ホームディレクトリ共有名が受ける影響

ホームディレクトリ共有名には、または `%u`動的変数のいずれかが含まれている必要があります `%w`。新しい要件がある ONTAP のバージョンにアップグレードしたあとに、既存の静的ホームディレクトリ共有名が受ける影響について理解しておく必要があります。

ホームディレクトリの設定に静的共有名が含まれている場合に ONTAP にアップグレードしても、静的ホームディレクトリ共有名は変更されず、共有も有効なままです。ただし、変数または `%u`を含まない新しいホームディレクトリ共有は作成できません `%w`。

ユーザのホームディレクトリ共有名にどちらかの変数を含めるという必須条件によって、すべての共有名がホームディレクトリ設定全体で一意であることが保証されます。必要に応じて、静的ホームディレクトリ共有名を変数または `%u`を含む名前に変更できます `%w`。

ホームディレクトリ検索パスを追加する

ONTAP SMBホームディレクトリを使用する場合は、ホームディレクトリ検索パスを少なくとも1つ追加する必要があります。

タスクの内容

ホームディレクトリ検索パスを追加するには、コマンドを使用し `vserver cifs home-directory search-path add`ます。

コマンドは `vserver cifs home-directory search-path add`、コマンドの実行中にオプションで指定されたパスをチェックし `-path`ます。指定したパスが存在しない場合は、続行するかどうかを確認するメッセージが表示されます。または `n`を選択し `y`ます。続行する場合は `y`、ONTAPによって検索パスが作成されます。ただし、ホームディレクトリ設定で検索パスを使用するには、事前にディレクトリ構造を作成しておく必要があります。続行しない場合、コマンドは失敗し、検索パスは作成されません。その後、パスディレクトリ構造を作成してコマンドを再実行できます `vserver cifs home-directory search-path add`。

手順

1. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`
2. コマンドを使用して、検索パスが追加されたことを確認します `vserver cifs home-directory search-path show`。

例

次の例は、SVM vs1のホームディレクトリ設定にパスを追加します `/home1`。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

次の例は、SVM vs1のホームディレクトリ設定にパスを追加することを試みます `/home2`。パスが存在しません。続行しないことが選択されます。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

関連情報

ホームディレクトリ共有の追加

%w変数と**%d**変数を使用してホームディレクトリ設定を作成する

変数と `%d`変数を使用して、ホームディレクトリ設定を作成できます `%w`。ユーザは、動的に作成された共有を使用してホーム共有に接続できます。

手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 目的のセキュリティ形式がqtreeで使用されていない場合は、コマンドを使用してセキュリティ形式を変更し `volume qtree security`ます。
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver` `vserver`検索パスを追加するCIFS対応のStorage Virtual Machine（SVM）を指定します。

   `-share-name` `%w`ホームディレクトリ共有名を指定します。ONTAPでは、ユーザがホームディレクトリに接続するたびに、共有名が動的に作成されます。共有名の形式は _windows_user_name です。

   `-path` `%d/%w`ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _domain/windows_user_name の形式で相対パスが動的に作成されます。

   `-share-properties homedirectory[,…]+`その共有の共有プロパティを指定します。値を指定する必要があり `homedirectory`ます。追加の共有プロパティをカンマで区切って指定できます。

5. コマンドを使用して、共有が目的の設定になっていることを確認します `vserver cifs share show`。
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *vserver-name*`検索パスを追加するCIFS対応のSVMを指定します。

   `-path` *path*`検索パスの絶対ディレクトリパスを指定します。

7. コマンドを使用して、検索パスが追加されたことを確認します `vserver cifs home-directory search-path show`。
8. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定したqtreeまたはボリューム内に、対応するディレクトリを作成します。

   たとえば、というパスのqtreeを作成し、ディレクトリを作成するユーザ名がmydomain\user1である場合は `/vol/vol1/users`、というパスでディレクトリを作成します `/vol/vol1/users/mydomain/user1`。

   にマウントされる「home1」という名前のボリュームを作成した場合は、というパスでディレクトリを作成し `/home1`ます `/home1/mydomain/user1`。

9. ドライブをマッピングするか、UNCパスを使用して接続し、ユーザがホーム共有に正常に接続できることを確認します。

   たとえば、ユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順8で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1`。

例

次の例のコマンドは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は%wです。
- 相対ホームディレクトリパスは%d/%wです。
- ホームディレクトリを含むように指定した検索パス `/home1`は、NTFSセキュリティ形式が設定されたボリュームです。
- 設定はSVM vs1に作成されます。

ユーザがWindowsホストからホームディレクトリにアクセスする場合は、このようなホームディレクトリ設定を使用できます。また、ユーザがWindowsホストおよびUNIXホストからホームディレクトリにアクセスし、ファイルシステム管理者がWindowsベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合にも、このような設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

関連情報

%u変数を使用したホームディレクトリの設定

追加のホームディレクトリ設定

SMBユーザのホームディレクトリパスに関する情報の表示

%u変数を使用してホームディレクトリを設定する

ホームディレクトリ設定を作成し、変数を使用して共有名を指定し、変数を使用して `%u`ホームディレクトリ共有の相対パスを指定することができます `%w`。これにより、ユーザは、ホームディレクトリの実際の名前やパスを意識することなく、Windowsユーザ名を使用して動的に作成された共有を使用してホーム共有に接続できます。

手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 目的のセキュリティ形式がqtreeで使用されていない場合は、コマンドを使用してセキュリティ形式を変更し `volume qtree security`ます。
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver` `vserver`検索パスを追加するCIFS対応のStorage Virtual Machine（SVM）を指定します。

   `-share-name` `%w`ホームディレクトリ共有名を指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _windows_user_name の形式で共有名が動的に作成されます。

   > オプションに変数 `-share-name`を使用することもでき `%u`ます。これにより、マッピングされたUNIXユーザ名を使用する相対共有パスが作成されます。

   `-path` `%u`ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _mapped_UNIX_user_name の形式で共有名が動的に作成されます。

   > このオプションの値には、静的要素も含めることができます。たとえば、 `eng/%u`です。

   `-share-properties` `homedirectory\[,...\]`その共有の共有プロパティを指定します。値を指定する必要があり `homedirectory`ます。追加の共有プロパティをカンマで区切って指定できます。

5. コマンドを使用して、共有が目的の設定になっていることを確認します `vserver cifs share show`。
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` `vserver`検索パスを追加するCIFS対応のSVMを指定します。

   `-path` `path`検索パスの絶対ディレクトリパスを指定します。

7. コマンドを使用して、検索パスが追加されたことを確認します `vserver cifs home-directory search-path show`。
8. UNIXユーザが存在しない場合は、コマンドを使用してUNIXユーザを作成し `vserver services unix-user`

create`ます。

ユーザをマッピングする前に、Windowsユーザ名のマッピング先となるUNIXユーザ名が存在している必要があります。

9. 次のコマンドを使用して、UNIXユーザへのWindowsユーザのネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   WindowsユーザをUNIXユーザにマッピングするネームマッピングがすでに存在する場合は、マッピング手順を実行する必要はありません。

   Windowsユーザ名は対応するUNIXユーザ名にマッピングされます。Windowsユーザは、ホームディレクトリ共有に接続すると、Windowsユーザ名に対応する共有名を使用して動的に作成されたホームディレクトリに接続します。ディレクトリ名がUNIXユーザ名に対応していることは認識されません。

10. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定したqtreeまたはボリューム内に、対応するディレクトリを作成します。

    たとえば、というパスのqtreeを作成し、ディレクトリの作成対象となるユーザのマッピングされたUNIXユーザ名が「unixuser1」の場合、 `/vol/vol1/users`というパスでディレクトリを作成します `/vol/vol1/users/unixuser1`。

    にマウントされる「home1」という名前のボリュームを作成した場合は、というパスでディレクトリを作成し `/home1`ます `/home1/unixuser1`。

11. ドライブをマッピングするか、UNCパスを使用して接続し、ユーザがホーム共有に正常に接続できることを確認します。

    たとえば、UNIXユーザunixuser1にマッピングされるユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順10で作成）に接続する場合は、UNCパスを使用して接続し `\\vs1\user1`ます。

例

次の例のコマンドは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は%wです。
- 相対ホームディレクトリパスは%uです。
- ホームディレクトリを含むように指定した検索パス `/home1`は、UNIXセキュリティ形式が設定されたボリュームです。
- 設定はSVM vs1に作成されます。

ユーザがWindowsホスト、またはWindowsホストとUNIXホストの両方からホームディレクトリにアクセスし、ファイルシステム管理者がUNIXベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合は、このようなホームディレクトリ設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

関連情報

%w変数と%d変数を使用したホームディレクトリ設定の作成

追加のホームディレクトリ設定

追加のホームディレクトリ設定

、 %d`の `%u`各変数を使用して追加のホームディレクトリの設定を作成し、ニーズに合わせてホームディレクトリの設定をカスタマイズできます `%w。

共有名と検索パスで変数と静的文字列の組み合わせを使用して、多数のホームディレクトリの設定を作成できます。次の表に、さまざまなホームディレクトリ設定を作成する例を示します。

がホームディレクトリを含む場合に作成されるパス /vol1/user	**share** コマンド
ユーザをに転送する /vol1/user/win_username`共有パスを作成するには `\\vs1\~win_username	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
ユーザをに転送する /vol1/user/domain/win_username`共有パスを作成するには `\\vs1\win_username	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
ユーザをに転送する /vol1/user/unix_username`共有パスを作成するには `\\vs1\win_username	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
ユーザをに転送する /vol1/user/unix_username`共有パスを作成するには `\\vs1\unix_username	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

検索パスの管理用コマンド

ONTAPには、SMBホームディレクトリ設定の検索パスを管理するためのコマンドが用意されています。たとえば、検索パスを追加、削除、および情報を表示するためのコマンドが用意されています。また、検索パスの順序を変更するためのコマンドもあります。

状況	使用するコマンド
検索パスを追加する	`vserver cifs home-directory search-path add`
検索パスを表示します。	`vserver cifs home-directory search-path show`

状況	使用するコマンド
検索パスの順序を変更する	`vserver cifs home-directory search-path reorder`
検索パスを削除する	`vserver cifs home-directory search-path remove`

詳細については、各コマンドのマニュアルページを参照してください。

SMB ユーザのホームディレクトリパスに関する情報を表示します

Storage Virtual Machine（SVM）上のSMBユーザのホームディレクトリパスを表示できます。このパスは、複数のCIFSホームディレクトリパスが設定されていて、ユーザのホームディレクトリがあるパスを確認する場合に使用できます。

ステップ

1. コマンドを使用して、ホームディレクトリパスを表示します `vserver cifs home-directory show-user`。

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  ----------------------
   vs1          user1                /home/user1
   ```

関連情報

ユーザのホームディレクトリへのアクセスの管理

ユーザのホームディレクトリへのアクセスを管理します。

デフォルトでは、ユーザのホームディレクトリにアクセスできるのはそのユーザだけです。動的な共有名の前にチルダ（ ｛チルダ｝ ）が付いている共有の場合、 Windows 管理者や他のユーザ（パブリックアクセス）によるユーザのホームディレクトリへのアクセスを有効または無効にできます。

開始する前に

Storage Virtual Machine （ SVM ）のホームディレクトリ共有に、動的な共有名の前にチルダ（ ｛チルダ｝ ）を追加した共有名を設定する必要があります。共有の命名要件を次に示します。

ホームディレクトリ共有名	共有に接続するコマンドの例
｛チルダ｝ %d ｛チルダ｝ %w	`net use * \\IPaddress\~domain~user/u:credentials`

ホームディレクトリ共有名	共有に接続するコマンドの例
｛チルダ｝ %w	`net use * \\IPaddress\~user/u:credentials`
｛チルダ｝ abc ｛チルダ｝ %w	`net use * \\IPaddress\abc~user/u:credentials`

ステップ

1. 適切な操作を実行します。

ユーザのホームディレクトリへのアクセスを有効または無効にする対象	入力するコマンド
Windows管理者	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}`デフォルトはです `true。
任意のユーザ（パブリックアクセス）	a. 権限レベルをadvancedに設定します。+ `set -privilege advanced` b. アクセスを有効または無効にします。`vserver cifs home-directory modify -vserver *vserver_name* -is-home-dirs-access-for-public -enabled {true

次の例は、ユーザのホームディレクトリへのパブリックアクセスを有効にします。

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true++
set -privilege admin
```

関連情報

SMBユーザのホームディレクトリパスに関する情報の表示

UNIXシンボリックリンクへのSMBクライアントアクセスの設定

ONTAPを使用してUNIXシンボリックリンクへのSMBクライアントアクセスを提供する方法

シンボリックリンクは UNIX 環境で作成されるファイルで、別のファイルまたはディレクトリへの参照が含まれます。シンボリックリンクにアクセスしたクライアントは、シンボリックリンクが参照するターゲットファイルまたはディレクトリにリダイレクトされます。ONTAPは、ワイドリンク（ローカルファイルシステムの外部にあるターゲットとの絶対リンク）を含む相対シンボリックリンクと絶対シンボリックリンクをサポートします。

ONTAP には、 SMB クライアントが SVM で設定されている UNIX のシンボリックリンクをたどるための機能が用意されています。この機能はオプションであり、次のいずれかの設定を指定してコマンドのオプションを

`vserver cifs share create`使用すると、共有ごとに設定でき `-symlink-properties`ます。

- 読み取り / 書き込みアクセスで有効化
- 読み取り専用アクセスで有効化
- SMB クライアントに対してシンボリックリンクを非表示にして無効にしました
- SMB クライアントからシンボリックリンクへのアクセス権なしで無効になりました

共有でシンボリックリンクを有効にした場合、相対シンボリックリンクは追加の設定なしで機能します。

共有でシンボリックリンクを有効にしただけでは、絶対シンボリックリンクは機能しません。最初に、シンボリックリンクの UNIX パスからデスティネーション SMB パスへのマッピングを作成する必要があります。絶対シンボリックリンクのマッピングを作成する場合、ローカルリンクか a_widelink ；ワイドリンクを他のストレージデバイス上のファイルシステムにリンクするか、同じ ONTAP システム上の別々の SVM でホストされているファイルシステムにリンクするかを指定できます。ワイドリンクを作成するときは、クライアントがたどる情報を含める必要があります。つまり、クライアントがディレクトリジャンクションポイントを検出するためのリパースポイントを作成します。ローカル共有外のファイルまたはディレクトリへの絶対シンボリックリンクを作成しても、局所性をローカルに設定すると、 ONTAP はターゲットへのアクセスを許可しません。

> クライアントがローカルシンボリックリンク（絶対または相対）を削除しようとすると、シンボリックリンクのみが削除され、ターゲットファイルやターゲットディレクトリは削除されません。ただし、クライアントがワイドリンクを削除しようとすると、ワイドリンクが参照する実際のターゲットファイルやターゲットディレクトリが削除される可能性があります。クライアントは SVM 外のターゲットファイルまたはディレクトリを明示的に開いて削除できるため、 ONTAP ではこの操作を制御できません。

- * リパースポイントと ONTAP ファイルシステムサービス *

  a_reparse point_ は、オプションでファイルとともにボリュームに格納できる NTFS ファイルシステムオブジェクトです。リパースポイントを使用すると、SMBクライアントは、NTFS形式のボリュームを使用する際に拡張ファイルシステムサービスを利用できます。リパースポイントは、リパースポイントのタイプを識別する標準のタグと、SMBクライアントが取得して以降の処理を実行できるリパースポイントの内容で構成されます。ファイルシステムの拡張機能で使用できるオブジェクトタイプのうち、ONTAPでは、リパースポイントタグを使用したNTFSシンボリックリンクとディレクトリジャンクションポイントのサポートが実装されています。リパースポイントの内容を理解できないSMBクライアントは、リパースポイントを無視し、リパースポイントで有効になる可能性のある拡張ファイルシステムサービスを提供しません。

- * ディレクトリジャンクションポイントおよびシンボリックリンクの ONTAP サポート *

  ディレクトリジャンクションポイントはファイルシステムディレクトリ構造内の場所で、別のパス（シンボリックリンク）または別のストレージデバイス（ワイドリンク）上のファイルが格納されている別の場所を参照できます。ONTAP SMBサーバはディレクトリジャンクションポイントをリパースポイントとしてWindowsクライアントに公開するため、対応するクライアントは、ディレクトリジャンクションポイントがトラバースされたときにONTAPからリパースポイントのコンテンツを取得できます。これにより、同じファイルシステムの一部であるかのように、異なるパスやストレージデバイスに移動して接続できます。

- * リパースポイントオプションを使用したワイドリンクサポートの有効化 *

  ONTAP 9では、この `-is-use-junctions-as-reparse-points-enabled`オプションはデフォルトで有効になっています。すべてのSMBクライアントがワイドリンクをサポートしているわけではないため、この情報を

有効にするオプションはプロトコルバージョンごとに設定できます。そのため、管理者はサポート対象のSMBクライアントとサポート対象外のSMBクライアントの両方に対応できます。ONTAP 9 .2以降のリリースでは、ワイドリンクを使用して共有にアクセスするクライアントプロトコルごとに、このオプションを有効にする必要があり `-widelink-as-reparse-point-versions`ます。デフォルトはsmb1です。以前のリリースでは、デフォルトのSMB1を使用してアクセスされるワイドリンクのみが報告され、SMB2またはSMB3を使用するシステムはワイドリンクにアクセスできませんでした。

関連情報

- "WindowsバックアップアプリケーションとUNIX形式のシンボリックリンク"
- "Microsoft のドキュメント：「 Reparse Points"

SMBアクセス用に**UNIX**シンボリックリンクを設定する場合の制限

SMBアクセス用にUNIXシンボリックリンクを設定する場合は、一定の制限事項に注意する必要があります。

制限	説明
45	CIFSサーバ名のFQDNを使用して指定できるCIFSサーバ名の最大長。 代わりに、CIFSサーバ名を15文字以内のNetBIOS名として指定することもできます。
80	共有名の最大文字数。
256	シンボリックリンクを作成するとき、または既存のシンボリックリンクのUNIXパスを変更するときに指定できるUNIXパスの最大長。UNIXパスは「/」で始まる必要があります。/`" (slash) and end with a "`先頭と末尾のスラッシュは、256文字の制限の一部としてカウントされます。
256	シンボリックリンクの作成時、または既存のシンボリックリンクのCIFSパスの変更時に指定できるCIFSパスの最大長。CIFSパスはで始まる必要があります。/`" (slash) and end with a "`先頭と末尾のスラッシュは、256文字の制限の一部としてカウントされます。

関連情報

SMB共有のシンボリックリンクマッピングの作成

ONTAPで**CIFS**サーバオプションを使用して**DFS**の自動通知を制御する

共有に接続する SMB クライアントに DFS 対応を通知する方法は、 CIFS サーバオプションで制御されます。ONTAP では、クライアントが SMB 経由でシンボリックリンクに

アクセスするときに DFS リファーラルを使用するため、このオプションを無効または有効にしたときの影響を理解しておく必要があります。

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

このオプションを無効にすると次のような影響があることに注意してください。

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

  シンボリックリンクへのクライアントの接続とアクセスは中断されることなく続行されます。

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

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

これらの変更は SMB 1.0 の接続には適用されません。

SMB共有でのUNIXシンボリックリンクサポートの設定

SMB共有の作成時に、または既存のSMB共有の変更によっていつでも、シンボリックリンクの共有プロパティ設定を指定することで、SMB共有でUNIXシンボリックリンクのサポートを設定できます。UNIXシンボリックリンクのサポートはデフォルトで有効になっています。共有でUNIXシンボリックリンクのサポートを無効にすることもできます。

タスクの内容

SMB共有に対してUNIXシンボリックリンクのサポートを設定する場合は、次のいずれかの設定を選択できます。

設定	説明
`enable`（廃止予定*）	読み取り/書き込みアクセスに対してシンボリックリンクを有効にします。

設定	説明
`read_only`（廃止予定*）	読み取り専用アクセスに対してシンボリックリンクを有効にします。この設定はワイドリンクには適用されません。Widelinkアクセスは常に読み取り/書き込みです。
`hide`（廃止予定*）	SMBクライアントにシンボリックリンクが表示されないように指定します。
`no-strict-security`	クライアントが共有の範囲外でシンボリックリンクを参照するように指定します。
`symlinks`	読み取り/書き込みアクセスに対してローカルシンボリックリンクを有効にします。CIFSオプションがに設定されて `true`いても、`DFS`通知は生成されません `is-advertise-dfs-enabled`。これがデフォルト設定です。
`symlinks-and-widelinks`	読み取り/書き込みアクセスに対してローカルシンボリックリンクとワイドリンクの両方を指定します。CIFSオプションがに設定されて `false`いる場合でも、DFS通知はローカルシンボリックリンクとワイドリンクの両方に対して生成され `is-advertise-dfs-enabled`ます。
`disable`	シンボリックリンクとワイドリンクを無効にします。CIFSオプションがに設定されて `true`いても、`DFS`通知は生成されません `is-advertise-dfs-enabled`。
""（null、未設定）	シンボリックリンクを共有で無効にします。
-（未設定）	シンボリックリンクを共有で無効にします。

- ONTAP の今後のリリースでは、 *enable*,*hide*,_read-only パラメータは廃止されており、削除される可能性があります。

手順

1. シンボリックリンクのサポートを設定または無効にします。

条件	入力するコマンド
新しいSMB共有	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only

条件	入力するコマンド
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	既存のSMB共有
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. SMB共有の設定が正しいことを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

例

次のコマンドでは、UNIXシンボリックリンク設定をに設定して、「data1」という名前のSMB共有を作成し`enable`ます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

関連情報

SMB共有のシンボリックリンクマッピングの作成

SMB共有のシンボリックリンクマッピングを作成する

SMB共有に対するUNIXシンボリックリンクのマッピングを作成できます。親フォルダを基準としたファイルまたはフォルダを参照する相対シンボリックリンクを作成することも、絶対パスを使用してファイルまたはフォルダを参照する絶対シンボリックリンクを作成することもできます。

タスクの内容

SMB 2.xを使用している場合、Mac OS Xクライアントからワイドリンクにアクセスすることはできません。ユーザがMac OS Xクライアントからワイドリンクを使用して共有に接続しようとすると、接続は失敗します。ただし、SMB 1を使用している場合は、Mac OS Xクライアントでワイドリンクを使用できます。

手順

1. SMB共有のシンボリックリンクマッピングを作成するには： `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver` `virtual_server_name`Storage Virtual Machine（SVM）名を示します。

   `-unix-path path`UNIXパスを指定します。UNIXパスはスラッシュ(/で始まる必要があります）、およびスラッシュで終わる必要があり(/ます。

   `-share-name` `share_name`マッピングするSMB共有の名前を指定します。

   `-cifs-path path`CIFSパスを指定します。CIFSパスはスラッシュ(/で始まる必要があります）、およびスラッシュで終わる必要が(/あります。

   `-cifs-server server_name`CIFSサーバ名を指定します。CIFSサーバ名は、DNS名（mynetwork.cifs.server.comなど）、IPアドレス、またはNetBIOS名で指定できます。NetBIOS名は、コマンドを使用して確認できます `vserver cifs show`。（オプション）このパラメータを指定しない場合、デフォルト値はローカルCIFSサーバのNetBIOS名です。

   `-locality local|free|widelink`}は、ローカルリンク、フリーリンク、ワイドシンボリックリンクのいずれを作成するかを指定します。ローカルシンボリックリンクはローカルSMB共有にマッピングされます。フリーシンボリックリンクは、ローカルSMBサーバ上の任意の場所にマッピングできます。ワイドシンボリックリンクは、ネットワーク上の任意のSMB共有にマッピングされます。このオプションパラメータを指定しない場合、デフォルト値はです `local`。

   `-home-directory true false`｝ターゲットの共有がホームディレクトリかどうかを指定します。このパラメータはオプションですが、ターゲットの共有をホームディレクトリとして設定する場合は、このパラメータをに設定する必要があります `true`。デフォルトはです `false`。

例

次のコマンドは、vs1という名前のSVM上にシンボリックリンクマッピングを作成します。このマッピングは、UNIXパス `/src/`、SMB共有名「ソース」、CIFSパス、CIFS `/mycompany/source/`サーバのIPアドレスが123.123.123.123で、ワイドリンクです。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

関連情報

SMB共有でのUNIXシンボリックリンクサポートの設定

シンボリックリンクのマッピングの管理用コマンド

ONTAP には、シンボリックリンクのマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
シンボリックリンクのマッピングを作成します	`vserver cifs symlink create`
シンボリックリンクのマッピングに関する情報を表示する	`vserver cifs symlink show`
シンボリックリンクのマッピングを変更する	`vserver cifs symlink modify`
シンボリックリンクのマッピングを削除する	`vserver cifs symlink delete`

詳細については、各コマンドのマニュアルページを参照してください。

Windowsバックアップアプリケーションと**UNIX**形式のシンボリックリンク

Windowsで実行されているバックアップアプリケーションでUNIX形式のシンボリックリンク（symlink）が検出されると、リンクに従ってデータがバックアップされます。ONTAP 9.15.1以降では、データの代わりにシンボリックリンクをバックアップするオプションが用意されています。この機能は、ONTAPのFlexGroupとFlexVolで完全にサポートされます。

概要

Windowsバックアップ処理中のシンボリックリンクの処理方法を変更する前に、ONTAP利点、主要な概念、および設定オプションについて理解しておく必要があります。

メリット

この機能を無効にするか使用できない場合、各シンボリックリンクがトラバースされ、リンク先のデータがバックアップされます。このため、不要なデータがバックアップされることがあり、特定の状況ではアプリケーションがループに陥る可能性があります。代わりに、シンボリックリンクをバックアップすることでこれらの問題を回避できます。また、ほとんどの場合、シンボリックリンクファイルはデータに比べて非常に小さいため、バックアップにかかる時間が短縮されます。IO処理が減少するため、クラスタの全体的なパフォーマンスも向上します。

Windowsサーバ環境

この機能は、Windowsで実行されているバックアップアプリケーションでサポートされています。環境を使用する前に、環境の関連する技術的側面を理解しておく必要があります。

拡張属性

Windowsでは、拡張属性（EA）がサポートされています。この拡張属性は、オプションでファイルに関連付けられた追加のメタデータをまとめて形成します。これらの属性は、Windows Subsystem for Linuxなどのさまざまなアプリケーションで使用されます（を参照） "WSLのファイル権限"。アプリケーションは、ONTAPからデータを読み取るときに、各ファイルの拡張属性を要求できます。

シンボリックリンクは、この機能が有効になっている場合に拡張属性で返されます。したがって、バックアップアプリケーションは、メタデータの格納に使用される標準のEAサポートを提供する必要があります。一部のWindowsユーティリティでは、拡張属性がサポートされ、保持されます。ただし、バックアップソフトウェアで拡張属性のバックアップとリストアがサポートされていない場合は、各ファイルに関連付けられているメタデータが保持されず、シンボリックリンクの適切な処理が失敗します。

Windowsコウセイ

Microsoft Windowsサーバ上で実行されているバックアップアプリケーションには、通常のファイルセキュリティをバイパスできる特別な権限を付与できます。これは通常、アプリケーションをBackup Operatorsグループに追加することによって行われます。アプリケーションは、必要に応じてファイルをバックアップおよび復元したり、その他の関連システム操作を実行したりできます。バックアップアプリケーションで使用されるSMBプロトコルにはわずかな変更が加えられていますが、データの読み取りと書き込みの際にONTAPで検出される可能性があります。

要件

シンボリックリンクバックアップ機能には、次のようないくつかの要件があります。

- クラスタでONTAP 9.15.1以降が実行されている。
- 特別なバックアップ権限が付与されたWindowsバックアップアプリケーション。
- バックアップアプリケーションでは、拡張属性もサポートし、バックアップ処理中に要求する必要があります。
- 該当するデータSVMに対してONTAPシンボリックリンクバックアップ機能が有効になっている。

設定オプション

ONTAP CLIに加えて、REST APIを使用してこの機能を管理することもできます。詳細については、を参照してください "ONTAP REST APIと自動化の新機能" 。ONTAPでのUNIX形式のシンボリックリンクの処理方法を決定する設定は、SVMごとに個別に実行する必要があります。

ONTAPでシンボリックリンクバックアップ機能を有効にする

ONTAP 9.15.1では、既存のCLIコマンドに設定オプションが導入されています。このオプションを使用すると、UNIX形式のシンボリックリンク処理を有効または無効にできます。

開始する前に

基本を確認します [要件]。その他：

- CLI権限をadvancedレベルに昇格できるようにします。

- 変更するデータSVMを決定します。このコマンド例ではSVMを `vs1` 使用しています。

手順

1. advanced権限レベルを設定します。

```
set privilege advanced
```

2. シンボリックリンクファイルのバックアップを有効にします。

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

BranchCacheを使用してブランチオフィスで**SMB**共有のコンテンツをキャッシュする

BranchCacheを使用してブランチオフィスで**SMB**共有のコンテンツをキャッシュする概要

BranchCacheは、要求元のクライアントのローカルコンピュータにコンテンツをキャッシュできるようにするためにMicrosoftが開発したものです。ONTAPにBranchCacheを実装すると、Storage Virtual Machine（SVM）に格納されたコンテンツにSMBを使用してブランチオフィスのユーザがアクセスする際に、広域ネットワーク（WAN）の使用量を抑え、アクセス応答時間を短縮できます。

BranchCacheを設定すると、Windows BranchCacheクライアントはまずSVMのコンテンツを取得し、次にそのコンテンツをブランチオフィスのコンピュータにキャッシュします。ブランチオフィスの別のBranchCache対応クライアントが同じコンテンツを要求すると、SVMは最初に要求元ユーザの認証と許可を行います。次にSVMは、キャッシュされたコンテンツが最新のものであるかどうかを確認し、最新のものである場合はそのコンテンツに関するメタデータをクライアントに送信します。クライアントは、そのメタデータを使用して、ローカルのキャッシュから直接コンテンツを取得します。

関連情報

オフラインファイルを使用したオフラインで使用するファイルのキャッシュ

要件とガイドライン

BranchCacheのバージョンのサポート

ONTAPでサポートされるBranchCacheのバージョンを確認しておく必要があります。

ONTAPでは、BranchCache 1と強化されたBranchCache 2がサポートされています。

- Storage Virtual Machine（SVM）のSMBサーバでBranchCacheを設定するときに、BranchCache 1、BranchCache 2、またはすべてのバージョンを有効にすることができます。

  デフォルトでは、すべてのバージョンが有効になっています。

- BranchCache 2のみを有効にする場合は、リモートオフィスのWindowsクライアントマシンでBranchCache 2がサポートされている必要があります。

BranchCache 2をサポートするのはSMB 3.0以降のクライアントだけです。

BranchCacheのバージョンの詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

ネットワークプロトコルのサポート要件

ONTAP BranchCache を実装するときは、ネットワークプロトコルの要件を考慮する必要があります。

ONTAP BranchCache 機能は、 SMB 2.1 以降を使用して、 IPv4 および IPv6 のネットワークに実装できます。

BranchCache の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、 SMB 2.1 以降のプロトコルを有効にする必要があります。SMB 2.1 では、プロトコルの機能拡張により、クライアントを BranchCache 環境に含めることができます。SMB プロトコルとして BranchCache をサポートするために必要な最小バージョンを指定してください。SMB 2.1 は、 BranchCache バージョン 1 をサポートします。

BranchCache バージョン 2 を使用する場合は、サポートする SMB の最小バージョンは SMB 3.0 になります。BranchCache 2 の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、 SMB 3.0 以降を有効にする必要があります。

リモートオフィスでSMB 2.1のみをサポートするクライアントとSMB 3.0をサポートするクライアントがある場合は、BranchCache 1とBranchCache 2の両方でキャッシュをサポートするCIFSサーバにBranchCache設定を実装できます。

Microsoft BranchCache 機能ではファイルアクセスプロトコルとして HTTP / HTTPS と SMB プロトコルの両方がサポートされますが、 ONTAP BranchCache でサポートされるのは SMB のみです。

ONTAPおよび**Windows**ホストのバージョン要件

BranchCacheを設定するには、ONTAPやブランチオフィスのWindowsホストが特定のバージョン要件を満たしている必要があります。

BranchCacheを設定するには、クラスタのONTAPのバージョンや対象となるブランチオフィスのクライアントで、SMB 2.1以降とBranchCacheの機能をサポートしている必要があります。ホスト型キャッシュモードを設定する場合は、サポートされているホストをキャッシュサーバに使用する必要もあります。

BranchCache 1は、次のONTAPバージョンおよびWindowsホストでサポートされています。

- コンテンツサーバ：ONTAPを備えたStorage Virtual Machine（SVM）
- キャッシュサーバ： Windows Server 2008 R2 または Windows Server 2012 以降
- ピアまたはクライアント： Windows 7 Enterprise 、 Windows 7 Ultimate 、 Windows 8 、 Windows Server 2008 R2 、または Windows Server 2012 以降

BranchCache 2は、次のONTAPバージョンおよびWindowsホストでサポートされています。

- コンテンツサーバ： ONTAP を備えた SVM
- キャッシュサーバ： Windows Server 2012 以降
- ピアまたはクライアント： Windows 8 または Windows Server 2012 以降

ONTAPで**BranchCache**ハッシュが無効になる理由

ONTAP でどのような場合にハッシュが無効になるかを理解すると、 BranchCache の設定を計画するときに役立ちます。この情報に基づいて、設定する必要がある動作モードの決定と、 BranchCache を有効にする共有を選択するかどうかの検討の助けになります。

ONTAP は、 BranchCache ハッシュが有効なものであるかを管理しています。ハッシュが無効な場合、 ONTAP は次にコンテンツが要求されたときにハッシュを無効にして新しいハッシュを計算します。これは、 BranchCache が有効なままであることを前提としています。

ONTAP は、以下の場合にハッシュを無効にします。

- サーバキーが変更された場合。

  サーバキーが変更された場合は、 ONTAP によってハッシュストア内のすべてのハッシュが無効になります。

- BranchCache のハッシュストアの最大サイズに達したために、ハッシュがキャッシュからフラッシュされた場合。

  このパラメータは調整可能で、ビジネス要件に合わせて変更することができます。

- SMB または NFS 経由のアクセスでファイルが変更された場合。
- 有効なハッシュが含まれているファイルがコマンドを使用してリストアされた `snap restore`場合。
- BranchCache対応のSMB共有を含むボリュームがコマンドを使用してリストアされた場合 `snap restore`。

ハッシュストアの場所の選択に関するガイドライン

BranchCacheを設定する場合は、ハッシュを格納する場所とハッシュストアのサイズを選択します。ハッシュストアの場所とサイズの選択に関するガイドラインについて理解しておくと、CIFS対応のSVMでBranchCacheの設定を計画するのに役立ちます。

- ハッシュストアは、atime更新が許可されているボリュームに配置する必要があります。

  ハッシュファイルへのアクセス時間は、アクセス頻度の高いファイルをハッシュストア内に保持するために使用されます。atime更新が無効になっている場合は、作成時間がこの目的に使用されます。頻繁に使用するファイルを追跡するには、atimeを使用することを推奨します。

- SnapMirrorデスティネーションやSnapLockボリュームなどの読み取り専用のファイルシステムにはハッシュを保存できません。
- ハッシュストアの最大サイズに達すると、古いハッシュがフラッシュされて新しいハッシュ用のスペースが確保されます。

ハッシュストアの最大サイズを拡張して、キャッシュからフラッシュされるハッシュの量を減らすことができます。

- ハッシュを格納するボリュームが使用できないかいっぱいである場合、またはクラスタ内通信に問題があり、BranchCacheサービスがハッシュ情報を取得できない場合は、BranchCacheサービスを使用できません。

  ボリュームがオフラインであるか、ストレージ管理者がハッシュストアの新しい場所を指定したために、ボリュームを使用できない可能性があります。

  これにより、ファイルアクセスで問題が発生することはありません。ハッシュストアに正常にアクセスできない場合、ONTAPはMicrosoft定義のエラーをクライアントに返します。これにより、クライアントは通常のSMB読み取り要求を使用してファイルを要求します。

関連情報

SMBサーバでのBranchCacheの設定

BranchCache設定を変更します。

BranchCacheの推奨事項

BranchCache を設定する前に、 BranchCache キャッシュを有効にする SMB 共有の決定時に考慮する必要がある推奨事項がいくつかあります。

使用する動作モードと BranchCache を有効にする SMB 共有の決定時には、次の推奨事項を考慮してください。

- リモートからキャッシュするデータが頻繁に変更されると、 BranchCache の利点が十分には生かされません。
- BranchCacheサービスは、複数のリモートオフィスクライアントで再利用されるファイルコンテンツや、1人のリモートユーザが繰り返しアクセスするファイルコンテンツを含む共有の場合に便利です。
- SnapshotコピーのデータやSnapMirrorデスティネーションのデータなど、読み取り専用コンテンツのキャッシュを有効にすることを検討してください。

BranchCacheの設定

BranchCacheの設定の概要

SMBサーバでBranchCacheを設定するには、ONTAPコマンドを使用します。BranchCache を実装するには、クライアント、および必要に応じてコンテンツをキャッシュするブランチオフィスにホストされるキャッシュサーバも設定する必要があります。

共有ごとにキャッシュを有効にするように BranchCache を設定する場合は、 BranchCache キャッシュサービスの対象となる SMB 共有で BranchCache を有効にする必要があります。

BranchCacheの設定要件

BranchCacheをセットアップするには、いくつかの前提条件を満たしている必要があり

ます。

SVMのCIFSサーバでBranchCacheを設定するには、次の要件を満たしている必要があります。

- クラスタ内のすべてのノードにONTAPがインストールされている必要があります。
- CIFSのライセンスが有効になっていて、SMBサーバが設定されている必要があります。SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- IPv4またはIPv6のネットワーク接続が設定されている必要があります。
- BranchCache 1の場合、SMB 2.1以降が有効になっている必要があります。
- BranchCache 2の場合、SMB 3.0が有効になっていて、リモートのWindowsクライアントでBranchCache 2がサポートされている必要があります。

SMBサーバでの**BranchCache**の設定

BranchCacheサービスを共有ごとに提供するようにBranchCacheを設定できます。また、すべてのSMB共有でキャッシュを自動的に有効にするようにBranchCacheを設定することもできます。

タスクの内容

BranchCacheはSVMで設定できます。

- CIFSサーバ上のすべてのSMB共有に格納されたすべてのコンテンツに対してキャッシュサービスを提供する場合は、すべての共有のBranchCache設定を作成できます。
- CIFSサーバ上の選択したSMB共有に格納されたコンテンツに対してキャッシュサービスを提供する場合は、共有ごとのBranchCache設定を作成できます。

BranchCacheの設定時には、次のパラメータを指定する必要があります。

必須パラメータ	説明
SVM 名 _	BranchCacheはSVM単位で設定します。BranchCacheサービスを設定するCIFS対応SVMを指定する必要があります。

必須パラメータ	説明
ハッシュストアへのパス _	BranchCacheハッシュは、SVMボリューム上の通常のファイルに格納されます。ONTAPにハッシュデータを格納する既存のディレクトリのパスを指定する必要があります。BranchCacheハッシュパスは読み取り/書き込み可能である必要があります。Snapshotディレクトリなどの読み取り専用パスは指定できません。他のデータを含むボリュームにハッシュデータを格納することも、ハッシュデータを格納するための別のボリュームを作成することもできます。 SVMがSVMディザスタリカバリソースの場合、ハッシュパスをルートボリュームに配置することはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。 ハッシュパスには、空白とファイル名の有効な文字を含めることができます。

必要に応じて、次のパラメータを指定できます。

オプションのパラメータ	説明
サポートされているバージョン _	ONTAPでは、BranchCache 1および2がサポートされます。バージョン1、バージョン2、またはその両方を有効にできます。デフォルトでは、両方のバージョンが有効になります。
_ ハッシュストアの最大サイズ _	ハッシュデータストアに使用するサイズを指定できます。ハッシュデータがこの値を超えると、ONTAPは古いハッシュを削除して新しいハッシュ用のスペースを確保します。ハッシュストアのデフォルトサイズは1GBです。ハッシュが過度に破棄されない場合、BranchCacheのパフォーマンスは向上します。ハッシュストアがいっぱいになったためにハッシュが頻繁に破棄されると判断した場合は、BranchCacheの設定を変更してハッシュストアのサイズを大きくすることができます。

オプションのパラメータ	説明
_ サーバキー _	クライアントがBranchCacheサーバを偽装できないようにするためにBranchCacheサービスで使用されるサーバキーを指定できます。指定しない場合、BranchCacheの設定の作成時にサーバキーがランダムに生成されます。サーバキーを特定の値に設定すると、複数のサーバが同じファイルのBranchCacheデータを提供している場合に、クライアントが同じサーバキーを使用して任意のサーバのハッシュを使用できるようになります。サーバキーにスペースを含める場合は、サーバキーを引用符で囲む必要があります。
オペレーティングモード _	デフォルトでは、BranchCacheは共有ごとに有効になります。 • BranchCacheを共有ごとに有効にするBranchCacheの設定を作成するには、このオプションパラメータを指定しないか、を指定します `per-share`。 • すべての共有でBranchCacheを自動的に有効にするには、動作モードをに設定する必要があります `all-shares`。

手順

1. 必要に応じてSMB 2.1および3.0を有効にします。
   a. 権限レベルをadvancedに設定します。 `set -privilege advanced`
   b. SVMのSMB設定を確認して、必要なすべてのバージョンのSMBが有効になっているかどうかを確認します。 `vserver cifs options show -vserver vserver_name`
   c. 必要に応じて、SMB 2.1を有効にします。 `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      コマンドは、SMB 2.0とSMB 2.1の両方を有効にします。
   d. 必要に応じて、SMB 3.0を有効にします。 `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
   e. admin権限レベルに戻ります。 `set -privilege admin`
2. BranchCacheを設定します。 `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   指定したハッシュストレージのパスが存在し、SVMによって管理されているボリューム上にある必要があります。また、パスは読み取り / 書き込み可能なボリュームにある必要があります。パスが読み取り専用であるか、または存在しない場合、コマンドは失敗します。

   SVM BranchCacheの追加設定で同じサーバキーを使用する場合は、サーバキーとして入力した値を記録

しておきます。BranchCacheの設定に関する情報を表示しても、サーバキーは表示されません。

3. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver` *`vserver_name`*

例

次のコマンドは、SMB 2.1と3.0の両方が有効になっていることを確認し、SVM vs1のすべてのSMB共有でキャッシュを自動的に有効にするようにBranchCacheを設定します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

次のコマンドは、SMB 2.1と3.0の両方が有効になっていることを確認し、SVM vs1の共有ごとにキャッシュを有効にするようにBranchCacheを設定し、BranchCacheの設定を確認します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

関連情報

要件とガイドライン： BranchCache バージョンのサポート

リモートオフィスでのBranchCacheの設定に関する情報の参照先

BranchCacheが有効なSMB共有を作成する

既存のSMB共有でBranchCacheを有効にする

BranchCache設定を変更します。

SMBキョウユウデノBranchCacheノムコウカノガイヨウ

SVMのBranchCache設定を削除する

リモートオフィスでの**BranchCache**の設定に関する情報の参照先

SMBサーバでBranchCacheを設定したら、リモートオフィスのクライアントコンピュータおよびキャッシュサーバ（オプション）にBranchCacheをインストールして設定する必要があります。リモートオフィスでBranchCacheを設定する手順について

は、Microsoftから説明されています。

BranchCacheを使用するようにブランチオフィスのクライアントおよびキャッシュサーバ（オプション）を設定する手順については、MicrosoftのBranchCacheのWebサイトを参照してください。

"Microsoft BranchCache のドキュメント：「 What's New"

BranchCacheが有効な**SMB**共有の設定

BranchCache対応の**SMB**共有の設定の概要

SMBサーバとブランチオフィスでBranchCacheを設定したら、ブランチオフィスのクライアントによるコンテンツのキャッシュを許可するSMB共有でBranchCacheを有効にすることができます。

BranchCacheキャッシュは、SMBサーバ上のすべてのSMB共有で有効にすることも、共有ごとに有効にすることもできます。

- BranchCache を共有ごとに有効にする場合、 BranchCache は共有の作成時に有効にするか、既存の共有を変更して有効にすることができます。

  既存の SMB 共有でキャッシュを有効にすると、その共有で BranchCache を有効にした時点で、 ONTAP によるハッシュの計算と要求元クライアントへのメタデータの送信が開始されます。

- 共有への SMB 接続をすでに確立しているクライアントは、それ以降にその共有で BranchCache が有効になった場合、 BranchCache のサポートを得ることができません。

  ONTAP は、 SMB セッションがセットアップされたときに共有の BranchCache のサポートを通知します。BranchCacheを有効にしたときにすでにセッションを確立していたクライアントは、キャッシュされたコンテンツをこの共有で使用するために、いったん切断してから再接続する必要があります。

その後 SMB 共有に対する BranchCache を無効にすると、 ONTAP による要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ（SMBサーバ）から直接データを取得します。

BranchCacheが有効な**SMB**共有を作成する

SMB共有の作成時に共有プロパティを設定して、共有でBranchCacheを有効にすることができます `branchcache`。

タスクの内容

- SMB共有でBranchCacheが有効になっている場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

  これは、共有を作成するときのデフォルト設定です。

- BranchCacheが有効な共有を作成するときに、オプションの共有パラメータを追加で指定することもできます。
- Storage Virtual Machine（SVM）でBranchCacheが設定されておらず、有効になっていない場合でも、共有のプロパティを設定でき `branchcache`ます。

ただし、共有でキャッシュされたコンテンツを提供するには、SVMでBranchCacheを設定して有効にする必要があります。

- パラメータを使用する場合、共有に適用されるデフォルトの共有プロパティはないため、 `-share -properties`共有プロパティに加えて、共有に適用する他のすべての共有プロパティをカンマで区切って指定する必要があります `branchcache`。
- 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 `vserver cifs share create`ください。

ステップ

1. BranchCacheが有効なSMB共有を作成します。+
`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,…]`
2. コマンドを使用して、SMB共有に対してBranchCache共有プロパティが設定されていることを確認します `vserver cifs share show`。

例

次のコマンドは、SVM vs1上でパスを使用して、「data」という名前のBranchCacheが有効なSMB共有を作成します `/data`。デフォルトでは、オフラインファイルの設定は次のように設定されてい `manual`ます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
            Share Properties: branchcache
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

関連情報

単一のSMB共有でのBranchCacheの無効化

既存のSMB共有でBranchCacheを有効にするには、共有プロパティの既存のリストに共有プロパティを追加し `branchcache`ます。

タスクの内容

- SMB共有でBranchCacheが有効になっている場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

  既存の共有のオフラインファイル設定が手動キャッシュに設定されていない場合は、共有を変更して設定する必要があります。

- Storage Virtual Machine（SVM）でBranchCacheが設定されておらず、有効になっていない場合でも、共有のプロパティを設定でき `branchcache`ます。

  ただし、共有でキャッシュされたコンテンツを提供するには、SVMでBranchCacheを設定して有効にする必要があります。

- 共有に共有プロパティを追加しても `branchcache`、既存の共有設定と共有プロパティは維持されます。

  branchcache共有プロパティは既存の共有プロパティリストに追加されます。コマンドの使用の詳細については `vserver cifs share properties add`、マニュアルページを参照してください。

手順

1. 必要に応じて、オフラインファイルの共有設定を手動キャッシュ用に設定します。
   a. コマンドを使用して、オフラインファイルの共有設定を確認します `vserver cifs share show`。
   b. オフラインファイルの共有設定がmanualに設定されていない場合は、必要な値に変更します。 `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. 既存のSMB共有でBranchCacheを有効にします。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. SMB共有でBranchCache共有プロパティが設定されていることを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドは、SVM vs1上のパスにある「data2」という名前の既存のSMB共有でBranchCacheを有効にします `/data2`。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

関連情報

既存のSMB共有に対する共有プロパティの追加または削除

単一のSMB共有でのBranchCacheの無効化

BranchCache設定を管理および監視する

BranchCache設定を変更します。

SVM上のBranchCacheサービスの設定では、ハッシュストアディレクトリのパス、最大サイズ、動作モード、サポートするBranchCacheのバージョンなどの設定を変更できます。ハッシュストアを含むボリュームのサイズを拡張することもできます。

手順

1. 適切な操作を実行します。

状況	入力するコマンド
ハッシュストアディレクトリのサイズ変更	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
ハッシュストアを含むボリュームのサイズを拡張する	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]`ハッシュストアを含むボリュームがいっぱいになった場合は、ボリュームのサイズを拡張できることがあります。新しいボリュームサイズは、数字と単位で指定できます。 詳細はこちら"FlexVol ボリュームの管理"	ハッシュストアディレクトリのパス変更

状況	入力するコマンド
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}`SVMがSVMディザスタリカバリソースの場合、ハッシュパスをルートボリュームに配置することはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。  BranchCacheハッシュパスには、空白とファイル名の有効な文字を含めることができます。  ハッシュパスを変更する場合、 `-flush-hashes`ONTAPで元のハッシュストアの場所からハッシュをフラッシュするかどうかを指定するには、が必須パラメータです。パラメータには次の値を設定でき `-flush-hashes`ます。  を指定する **`true`**と、**ONTAP**は元の場所にあるハッシュを削除し、**BranchCache**対応クライアントが新しい要求を行うたびに新しい場所に新しいハッシュを作成します。 を指定した場合 `false`、ハッシュはフラッシュされません。 + この場合、ハッシュストアパスを元の場所に戻すことで、既存のハッシュをあとから再利用できます。
動作モードの変更	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share	all-shares	disable}` 動作モードを変更する場合は、次の点に注意してください。 **ONTAP**では、**SMB**セッションのセットアップ時に、**BranchCache**による共有のサポートが通知されます。 BranchCacheを有効にしたときにすでにセッションを確立していたクライアントは、キャッシュされたコンテンツをこの共有で使用するために、いったん切断してから再接続する必要があります。
サポートするBranchCacheバージョンの変更	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable	v2-enable	enable-all}`

2. コマンドを使用して、設定の変更を確認します `vserver cifs branchcache show`。

BranchCache設定に関する情報を表示する

Storage Virtual Machine （ SVM ）の BranchCache 設定に関する情報を表示できます。

この情報は、設定を検証する場合や、設定を変更する前に現在の設定を確認する場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する項目	入力するコマンド
すべての SVM の BranchCache 設定に関する概要情報	`vserver cifs branchcache show`
特定の SVM の設定に関する詳細情報	`vserver cifs branchcache show -vserver` *`vserver_name`*

例

次の例では、SVM vs1のBranchCache設定に関する情報を表示します。

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

                                    Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

BranchCacheサーバキーを変更する

BranchCacheサーバキーを変更するには、Storage Virtual Machine（SVM）でBranchCacheの設定を変更し、別のサーバキーを指定します。

タスクの内容

サーバキーを特定の値に設定すると、複数のサーバが同じファイルのBranchCacheデータを提供している場合に、クライアントが同じサーバキーを使用して任意のサーバのハッシュを使用できるようになります。

サーバキーを変更する場合は、ハッシュキャッシュもフラッシュする必要があります。ハッシュのフラッシュ後、BranchCache対応クライアントによって新しい要求が行われると、ONTAPによって新しいハッシュが作成されます。

手順

1. 次のコマンドを使用して、サーバキーを変更します。 `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   新しいサーバキーを設定する場合は、も指定して値をに設定する `true`必要があります `-flush-hashes`。

2. コマンドを使用して、BranchCacheの設定が正しいことを確認し `vserver cifs branchcache show`ます。

例

次の例では、SVM vs1でスペースを含む新しいサーバキーを設定し、ハッシュキャッシュをフラッシュします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

関連情報

ONTAPでBranchCacheハッシュが無効になる理由

指定したパスのBranchCacheハッシュを事前に計算

単一のファイル、ディレクトリ、またはディレクトリ構造内のすべてのファイルについて、ハッシュを事前に計算するようにBranchCacheサービスを設定できます。これは、BranchCacheが有効な共有内のデータのハッシュをピーク以外の時間帯に計算する場合に役立ちます。

タスクの内容

ハッシュの統計を表示する前にデータサンプルを収集する場合は、コマンドとオプションの `statistics stop`コマンドを使用する必要があり `statistics start`ます。

- ハッシュを事前に計算するStorage Virtual Machine（SVM）とパスを指定する必要があります。
- また、ハッシュを再帰的に計算するかどうかも指定する必要があります。
- ハッシュを再帰的に計算する場合、BranchCacheサービスは指定されたパスの下のディレクトリツリー全体をトラバースし、対象となるオブジェクトごとにハッシュを計算します。

手順

1. 必要に応じてハッシュを事前に計算します。

ハッシュを事前に計算する対象	入力するコマンド
単一のファイルまたはディレクトリ	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`

ハッシュを事前に計算する対象	入力するコマンド
ディレクトリ構造内のすべてのファイルに対して再帰的に実行	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. コマンドを使用して、ハッシュが計算されていることを確認し `statistics`ます。
   a. 目的のSVMインスタンス上のオブジェクトの統計を表示します `hashd。 statistics show -object hashd -instance vserver_name`
   b. コマンドを繰り返し実行して、作成済みのハッシュの数が増加していることを確認します。

例

次の例では、パスおよびSVM vs1に格納されているすべてのファイルとサブディレクトリを対象にハッシュを作成します `/data`。

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

関連情報

"パフォーマンス監視のセットアップ"

SVM BranchCacheハッシュストアからハッシュをフラッシュする

Storage Virtual Machine （ SVM ）上の BranchCache ハッシュストアから、キャッシュされたハッシュをすべてフラッシュできます。これは、ブランチオフィスの BranchCache の設定を変更した場合に役立ちます。たとえば、最近キャッシュモードを分散キャッシュからホスト型キャッシュモードに再設定した場合は、ハッシュストアをフラッシュする必要があります。

タスクの内容

ハッシュのフラッシュ後、BranchCache対応クライアントによって新しい要求が行われると、ONTAPによって新しいハッシュが作成されます。

ステップ

1. BranchCacheハッシュストアからハッシュをフラッシュします。 `vserver cifs branchcache hash-flush -vserver vserver_name`

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

BranchCache統計を表示します。

BranchCache統計を表示すると、キャッシュが適切に実行されているかどうか、キャッシュされたコンテンツをクライアントに提供しているかどうか、新しいハッシュデータ用のスペースを確保するためにハッシュファイルが削除されたかどうかなどの情報を確認できます。

タスクの内容

`hashd`statisticオブジェクトには、BranchCacheハッシュに関する統計情報を提供するカウンタが含まれます。 `cifs`statisticオブジェクトには、BranchCache関連のアクティビティに関する統計情報を提供するカウンタが含まれます。これらのオブジェクトに関する情報は、advanced権限レベルで収集および表示できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

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

2. コマンドを使用して、BranchCache関連のカウンタを表示します `statistics catalog counter show`。

   統計カウンタの詳細については、このコマンドのマニュアルページを参照してください。

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    --------------------------
-------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
```

```
                                   and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                   data failed. These are failures when
                                   attempting to read existing hash data.
It
                                   does not include attempts to fetch hash
data
                                   that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                   data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                   requesting hashes.
    branchcache_missing_hash_bytes
                                   Total number of bytes of data that had
to be
                                   read by the client because the hash for
that
                                   content was not available on the server.
    ....Output truncated....
```

3. コマンドと `statistics stop`コマンドを使用して、BranchCache関連の統計を収集し `statistics start`ます。

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. コマンドを使用して、収集したBranchCache統計を表示します `statistics show`。

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

5. admin権限レベルに戻ります。 `set -privilege admin`

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

関連情報

統計の表示

"パフォーマンス監視のセットアップ"

BranchCacheグループポリシーオブジェクトのサポート

ONTAP BranchCacheでは、BranchCacheのグループポリシーオブジェクト（GPO）を

サポートしており、特定のBranchCacheの設定パラメータを一元管理できます。BranchCacheには、BranchCacheのハッシュの発行GPOとBranchCacheのハッシュバージョンサポートGPOの2つのGPOが使用されます。

- * BranchCache のハッシュの発行 GPO *

  BranchCacheのハッシュの発行GPOは、パラメータに対応し `-operating-mode`ます。GPOが更新されると、グループポリシーが適用される組織単位（OU）に含まれるStorage Virtual Machine（SVM）オブジェクトにこの値が適用されます。

- * BranchCache のハッシュバージョンサポート *

  BranchCacheのハッシュバージョンサポートGPOは、パラメータに対応し `-versions`ます。GPOが更新されると、グループポリシーが適用される組織単位に含まれるSVMオブジェクトにこの値が適用されます。

関連情報

CIFSサーバへのグループ ポリシー オブジェクトの適用

BranchCacheグループポリシーオブジェクトに関する情報を表示する

CIFSサーバのグループポリシーオブジェクト（GPO）の設定に関する情報を表示して、CIFSサーバが属しているドメインに対してBranchCache GPOが定義されているかどうか、定義されている場合は許可されている設定を確認できます。また、BranchCache GPO設定がCIFSサーバに適用されているかどうかを確認することもできます。

タスクの内容

CIFSサーバが属しているドメイン内でGPO設定が定義されていても、CIFS対応のStorage Virtual Machine（SVM）が含まれるOrganizational Unit（OU；組織単位）に適用されているとは限りません。適用されるGPO設定は、CIFS対応のSVMに適用されているすべての定義済みGPOの一部です。GPOを使用して適用されたBranchCache設定は、CLIを使用した設定よりも優先されます。

手順

1. コマンドを使用して、Active Directoryドメインに対して定義されているBranchCache GPO設定を表示します `vserver cifs group-policy show-defined`。

   この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. コマンドを使用して、CIFSサーバに適用されているBranchCache GPO設定を表示します `vserver cifs group-policy show-applied`。``

この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

関連情報

CIFSサーバでのGPOサポートの有効化と無効化

SMB共有でのBranchCacheの無効化

SMBキョウユウデノ**BranchCache**ノムコウカノガイヨウ

特定のSMB共有でBranchCacheキャッシュサービスを提供せずに、あとからそれらの共有でキャッシュサービスを提供する場合は、BranchCacheを共有ごとに無効にすることができます。すべての共有でキャッシュを提供するようにBranchCacheを設定していて、一時的にすべてのキャッシュサービスを無効にする場合は、BranchCache設定を変更してすべての共有で自動キャッシュを停止できます。

SMB共有で有効になっていたBranchCacheをあとから無効にすると、ONTAPによる要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ（ Storage Virtual Machine （ SVM ）上の CIFS サーバ）から直接データを取得します。

関連情報

BranchCache対応のSMB共有の設定

単一のSMB共有でBranchCacheを無効にする

キャッシュコンテンツを使用できるようにしていた特定の共有でキャッシュサービスを提供する必要がなくなった場合は、既存の SMB 共有で BranchCache を無効にすることができます。

ステップ

1. 次のコマンドを入力します。 `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   BranchCache 共有プロパティが削除されます。適用されているその他の共有プロパティは有効なままです。

例

次のコマンドは、「 `d ata2` 」という名前の既存の SMB 共有で BranchCache を無効にします。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

すべての**SMB**共有で自動キャッシュを停止する

Storage Virtual Machine（SVM）のすべてのSMB共有に対してBranchCacheキャッシュを自動的に有効にするように設定している場合、BranchCacheの設定を変更して、すべてのSMB共有に対するコンテンツの自動キャッシュを停止することができます。

タスクの内容

すべての SMB 共有に対する自動キャッシュを停止するには、 BranchCache の動作モードを共有ごとのキャッシュに変更します。

手順

1. すべてのSMB共有で自動キャッシュを停止するようにBranchCacheを設定します。 `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドを実行すると、Storage Virtual Machine（SVM、旧Vserver）vs1のBranchCache設定が変更され、すべてのSMB共有に対する自動キャッシュが停止します。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

SVMで**BranchCache**を無効または有効にする

CIFSサーバで**BranchCache**を無効または再度有効にした場合の動作

BranchCache を設定したあとに、ブランチオフィスのクライアントがキャッシュされたコンテンツを使用できないようにするには、 CIFS サーバでキャッシュを無効にします。BranchCache を無効にするときは、それを実行した場合の動作について理解しておく必要があります

BranchCache を無効にすると、 ONTAP によるハッシュの計算や要求元クライアントへのメタデータの送信が行われなくなります。ただし、ファイルアクセスは中断されません。以降に、 BranchCache 対応クライアント ONTAP からアクセスするコンテンツのメタデータ情報を要求すると、 Microsoft のエラーが返されます。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、CIFSサーバからStorage Virtual Machine（SVM）に格納されている実際のコンテンツが送信されます。

CIFS サーバで BranchCache を無効にしたあとは、 SMB 共有で BranchCache の機能がアドバタイズされなくなります。新しい SMB 接続でデータにアクセスするには、通常の SMB 読み取り要求を行います。

BranchCache は、 CIFS サーバでいつでも再度有効にすることができます。

- BranchCache ONTAP を無効にしてもハッシュストアは削除されないため、要求されたハッシュがまだ有効であれば、 BranchCache を再度有効にしたあとに、格納されたハッシュを使用してハッシュの要求に応答することができます。
- BranchCache 対応の共有に対する SMB 接続を確立したクライアントで接続を確立したときに BranchCache が無効になっていたクライアントの場合には、以降に BranchCache を再度有効にしても、BranchCache のサポートは有効になりません。

  これは、 SMB セッションのセットアップ時に共有に対する BranchCache のサポートが通知されるから ONTAP です。BranchCache を無効にしたときに BranchCache 対応の共有に対するセッションを確立していた場合、その共有のキャッシュされたコンテンツを使用するには、いったん切断してから再接続する必要があります。

CIFS サーバで BranchCache を無効にしたあとにハッシュストアを保存しておく必要がない場合は、手動で削除することができます。BranchCache を再度有効にするときは、ハッシュストアのディレクトリが存在することを確認する必要があります。BranchCache を再度有効にすると、 BranchCache 対応の共有で BranchCache の機能がアドバタイズされるようになります。BranchCache 対応クライアントから新しい要求が行われると、 ONTAP によって新しいハッシュが作成されます。

BranchCacheを無効または有効にする

Storage Virtual Machine（SVM）でBranchCacheを無効にするには、BranchCacheの動作モードをに変更します。`disabled`BranchCache サービスを共有単位で提供するか、すべての共有で自動的に提供するように動作モードを変更すると、いつでも BranchCache を有効にすることができます。

手順

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCacheを無効にする	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
共有ごとに BranchCache を有効にします	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
すべての共有で BranchCache を有効にします	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. BranchCacheの動作モードが目的の設定になっていることを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次の例では、SVM vs1でBranchCacheを無効にします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

SVMのBranchCache設定を削除する

BranchCache設定を削除した場合の動作

BranchCache を設定したあとに、 Storage Virtual Machine （ SVM ）からのキャッシュされたコンテンツの提供を中止する場合は、 CIFS サーバで BranchCache 設定を削除します。設定を削除するときは、それを実行した場合の動作について理解しておく必要があります。

設定を削除すると、 ONTAP によってその SVM の設定情報がクラスタから削除され、 BranchCache サービスが停止します。SVM のハッシュストアについては、 ONTAP で削除するかどうかを選択することができます。

BranchCache 設定を削除しても、 BranchCache 対応クライアントによるアクセスは中断されません。以降に、 BranchCache 対応クライアントから既存の SMB 接続でキャッシュ済みのコンテンツのメタデータ情報を要求すると、 ONTAP は Microsoft のエラーを返します。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、 CIFS サーバから SVM に格納されている実際のコンテンツが送信されます

BranchCache 設定を削除すると、 SMB 共有で BranchCache の機能がアドバタイズされなくなります。キャッシュされていないコンテンツに新しい SMB 接続でアクセスするには、通常の SMB 読み取り要求を行います。

BranchCache設定を削除します。

Storage Virtual Machine（SVM）でBranchCacheサービスの削除に使用するコマンドは、既存のハッシュを削除するか保持するかによって異なります。

ステップ

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCache設定を削除して既存のハッシュを削除する	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
BranchCache設定を削除しますが、既存のハッシュは保持します	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

例

次の例は、SVM vs1でBranchCache設定を削除し、既存のハッシュをすべて削除します。

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

リバート時の**BranchCache**の動作

ONTAPをBranchCacheがサポートされないリリースにリバートする場合の動作について理解しておくことが重要です。

- ONTAPをBranchCacheがサポートされないバージョンにリバートすると、BranchCache対応クライアントに対してSMB共有でBranchCacheの機能がアドバタイズされなくなります。そのため、クライアントからハッシュ情報が要求されることはありません。

  代わりに、通常のSMB読み取り要求を使用して実際のコンテンツを要求します。これに対する応答として、SMBサーバからStorage Virtual Machine（SVM）に格納されている実際のコンテンツが送信されます。

- ハッシュストアをホストするノードをBranchCacheがサポートされないリリースにリバートする場合、リバート時に出力されるコマンドを使用して、ストレージ管理者がBranchCacheの設定を手動でリバートする必要があります。

  このコマンドは、BranchCacheの設定とハッシュを削除します。

  リバートの完了後、必要に応じて、ハッシュストアが格納されていたディレクトリを手動で削除できます。

関連情報

SVMのBranchCache設定の削除

Microsoftリモートコピーのパフォーマンスを向上

Microsoftリモートコピーのパフォーマンスの向上の概要

Microsoft Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _ コピーオフロード _ とも呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やスト

レージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。ソースとデスティネーションにはCIFSサーバまたはLUNのどちらかを指定できます。

ODX以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションに転送します。要約すると、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODXファイル転送では、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現されるパフォーマンス上のメリットには、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用率（CPU、メモリ）の削減、ネットワークI/O帯域幅の使用量の削減などがあります。

SMB環境では、この機能は、クライアントとストレージサーバの両方でSMB 3.0およびODX機能がサポートされている場合にのみ使用できます。SAN環境では、この機能は、クライアントとストレージサーバの両方でODX機能がサポートされている場合にのみ使用できます。ODXをサポートしていてODXが有効になっているクライアントコンピュータでは、ファイルの移動またはコピー時にオフロードされたファイル転送が自動的かつ透過的に使用されます。ODXは、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

関連情報

Auto Locationを使用したSMB自動ノードリファーラルによるクライアント応答時間の短縮

"Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"

ODXの仕組み

ODX コピーオフロードでは、トークンベースのメカニズムを使用して、 ODX 対応の CIFS サーバ内または CIFS サーバ間でデータの読み取りおよび書き込みを行います。CIFS サーバは、ホストを介してデータをルーティングするのではなく、データを表す小さなトークンをクライアントに送信します。ODX クライアントがそのトークンをデスティネーションサーバに提示すると、サーバはそのトークンで表されるデータをソースからデスティネーションに転送できます。

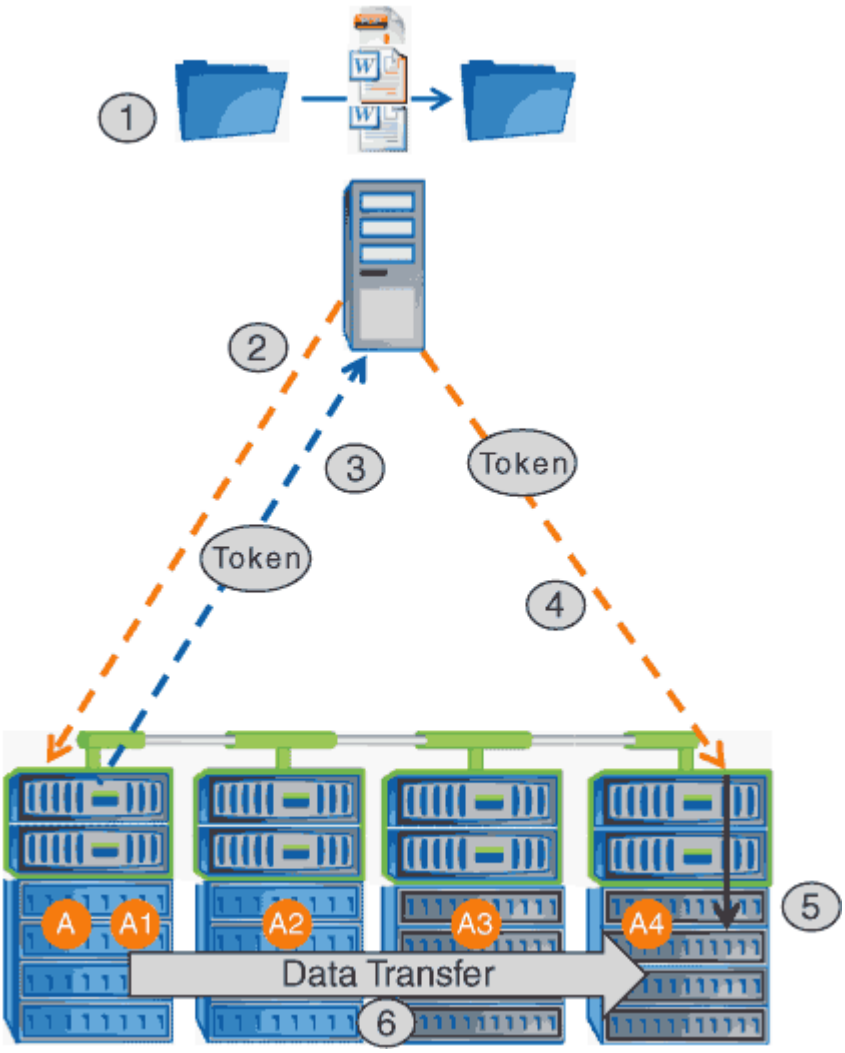
ODX クライアントは、 CIFS サーバが ODX 対応であると認識すると、ソースファイルを開いて CIFS サーバのトークンを要求します。デスティネーションファイルを開いたあと、クライアントはトークンを使用して、データをソースからデスティネーションに直接コピーするようにサーバに指示します。

ソースとデスティネーションは、コピー処理の範囲に応じて、同じ Storage Virtual Machine （ SVM ）上に存在する場合も異なる SVM 上に存在する場合もあります。

トークンは、データのポイントインタイム表現として機能します。たとえば、ストレージ間でデータをコピーする場合、データセグメントを表すトークンが要求元クライアントに返され、そのトークンをクライアントがデスティネーションにコピーするため、クライアントを介して基盤となるデータをコピーする必要がありません。

ONTAP では、 8MB のデータを表すトークンがサポートされます。8MB を超える ODX コピーは、 8MB のデータを表すトークンを複数使用して実行されます。

次の図で、 ODX コピー処理に関連する手順について説明します。



1. エクスプローラを使用するか、コマンドラインインターフェイスを使用するか、仮想マシンの移行の一環として、ユーザがファイルをコピーまたは移動します。または、アプリケーションによってファイルのコピーまたは移動が開始されます。
2. ODX 対応のクライアントが、この転送要求を ODX 要求に自動的に変換します。

   CIFS サーバに送信される ODX 要求には、トークン要求が含まれています。
3. CIFS サーバで ODX が有効になっていて、接続が SMB 3.0 経由の場合は、ソースのデータを論理的に表したものであるトークンが CIFS サーバによって生成されます。
4. クライアントは、データを表すトークンを受信し、書き込み要求を使用してそのトークンをデスティネーション CIFS サーバに送信します。

   ネットワーク経由でソースからクライアントにコピーされ、クライアントからデスティネーションにコピーされるのは、このデータだけです。
5. トークンがストレージサブシステムに送信されます。
6. コピーまたは移動が SVM によって内部的に実行されます。

   コピーまたは移動されるファイルが 8MB より大きい場合、コピーを実行するには複数のトークンが必要

になります。コピーが完了するまで、必要に応じて手順 2~6 を実行します。

ODX オフロードコピーで障害が発生した場合、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。同様に、デスティネーション CIFS サーバで ODX がサポートされていない場合、または ODX が無効になっている場合は、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。

ODXの使用要件

Storage Virtual Machine（SVM）でODXによるコピーオフロードを使用する前に、一定の要件について確認しておく必要があります。

ONTAPのバージョンの要件

ONTAPリリースでは、ODXによるコピーオフロードがサポートされます。

SMBのバージョンの要件

- ONTAPでは、SMB 3.0以降でODXがサポートされます。
- ODXを有効にする前に、CIFSサーバでSMB 3.0を有効にしておく必要があります。
  - ODX を有効にすると、 SMB 3.0 も有効になります（まだ有効になっていない場合）。
  - SMB 3.0を無効にするとODXも無効になります。

Windowsサーバとクライアントの要件

ODXによるコピーオフロードを使用するには、Windowsクライアントでこの機能がサポートされている必要があります。

"NetAppのInteroperability Matrix"サポートされるWindowsクライアントの最新情報については、を参照してください。

ボリュームの要件

- ソースボリュームは1.25GB以上である必要があります。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは8Kのみです。

  二次圧縮形式はサポートされません。

ODXの使用に関するガイドライン

コピーオフロードにODXを使用する前に、次のガイドラインを確認しておく必要があります。たとえば、ODXを使用できるボリュームのタイプや、クラスタ内およびクラスタ間のODXに関する考慮事項について理解しておく必要があります。

ボリュームに関するガイドライン

- 次のボリューム構成では、ODXをコピーオフロードに使用できません。
  - ソースボリュームサイズが 1.25GB 未満である必要があります

    ODXを使用するには、ボリュームサイズが1.25GB以上である必要があります。

  - 読み取り専用ボリューム

    負荷共有ミラー、SnapMirrorまたはSnapVaultデスティネーションボリュームにあるファイルやフォルダにはODXを使用できません。

  - ソースボリュームが重複排除されていない場合
- ODXコピーはクラスタ内のコピーでのみサポートされます。

  ODXを使用して、ファイルやフォルダを別のクラスタ内のボリュームにコピーすることはできません。

その他のガイドライン

- SMB環境でコピーオフロードにODXを使用するには、256KB以上のファイルである必要があります。

  サイズが小さいファイルは、従来のコピー処理を使用して転送されます。

- ODXコピーオフロードでは、コピープロセスの一部として重複排除が使用されます。

  データのコピーまたは移動時にSVMのボリュームで重複排除が発生しないようにするには、そのSVMでODXコピーオフロードを無効にする必要があります。

- データ転送を実行するアプリケーションは、ODXをサポートするように記述する必要があります。

  ODXをサポートするアプリケーションの処理は次のとおりです。

  - Virtual Hard Disk （ VHD ；仮想ハードディスク）の作成および変換、 Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、 Hyper-V の管理処理
  - エクスプローラでの操作
  - Windows PowerShell の copy コマンド
  - Windows コマンドプロンプトの copy コマンド

    WindowsコマンドプロンプトのRobocopyはODXをサポートしています。

    ODXをサポートするWindowsサーバまたはクライアントでアプリケーションが実行されている必要があります。

  +
  Windowsサーバおよびクライアントでサポートされる ODX アプリケーションの詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

ODXのユースケース

SVMでODXを使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODXをサポートするWindowsサーバおよびクライアントでは、リモートサーバ間でデータをコピーするデフォルトの方法として、コピーオフロードが使用されます。Windowsサーバまたはクライアントで ODXがサポートされていない場合や、ODXコピーオフロードがいずれかの時点で失敗した場合、コピー処理または移動処理は、その処理の従来の読み取りと書き込みにフォールバックされます。

ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとSVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- クラスタ間

  ソースLUNとデスティネーションLUNは、クラスタの異なるノードにある異なるボリュームにあります。これはSANでのみサポートされ、CIFSでは機能しません。

その他にも、次のような特殊なユースケースがあります。

- ONTAP ODXの実装では、ODXを使用して、SMB共有とFCまたはiSCSIで接続された仮想ドライブの間でファイルをコピーできます。

  Windowsエクスプローラ、Windows CLI（PowerShell）、Hyper-V、またはODXをサポートするその他のアプリケーションでODXコピーオフロードを使用すると、SMB共有と接続されたLUNが同じクラスタにある場合に、それらの間でシームレスにファイルをコピーまたは移動できます。

- Hyper-Vでは、その他にもODXコピーオフロードのユースケースがいくつか用意されています。
  - Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク（VHD）ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

    これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。
  - 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。

> Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

ODXの有効化または無効化

Storage Virtual Machine（SVM）でODXを有効または無効にすることができます。デフォルトでは、SMB 3.0が有効になっている場合、ODXコピーオフロードのサポートが有効になります。

開始する前に

SMB 3.0が有効になっている必要があります。

タスクの内容

SMB 3.0を無効にすると、ONTAPではSMB ODXも無効になります。SMB 3.0を再度有効にする場合は、SMB ODXを手動で再度有効にする必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ODX コピーオフロードの設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例は、SVM vs1でODXコピーオフロードを有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

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

関連情報

使用できるSMBサーバオプション

Auto Locationを使用した**SMB**自動ノードリファーラルによるクライアントの応答時間の短縮

Auto Locationの概要を使用して**SMB**自動ノードリファーラルを提供し、クライアントの応答時間を短縮

Auto Locationは、SMB自動ノードリファーラルを使用して、Storage Virtual Machine（SVM）でのSMBクライアントのパフォーマンスを向上させます。自動ノードリファーラルは、要求しているクライアントを、データが存在するボリュームをホストしているノードSVM上のLIFに自動的にリダイレクトします。これにより、クライアントの応答時間を短縮できます。

SMBクライアントがSVM上でホストされているSMB共有に接続するときに、要求されたデータを所有していないノード上のLIFを使用して接続することがあります。クライアントの接続先のノードは、クラスタネットワークを使用して別のノードが所有するデータにアクセスします。SMB接続で要求されたデータを含むノード上のLIFを使用している場合、クライアントへの応答時間が短縮されます。

- ONTAPでは、MicrosoftのDFSリファーラルを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることをSMBクライアントに通知することで、この機能を実現します。

  ノードがリファーラルを作成するのは、データを含むノード上にSVMのLIFがあることを特定した場合です。

- 自動ノードリファーラルは、IPv4とIPv6のLIFのIPアドレスでサポートされます。
- リファーラルは、クライアントの接続に使用する共有のルートの場所に基づいて作成されます。
- リファーラルはSMBネゴシエーション中に発生します。

  リファーラルは、接続が確立される前に作成されます。ONTAPがターゲット ノードに参照先のSMBクライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先LIFパスを介してデータにアクセスします。これにより、クライアントにはより高速なデータ アクセスが提供され、クラスタの余分な通信も回避されます。

共有が複数のジャンクションポイントにまたがっていて、ジャンクションの一部が他のノードに格納されているボリュームである場合、共有内のデータは複数のノードに分散されます。ONTAPは共有のルートに対してローカルなリファーラルを提供するため、ONTAPはクラスタネットワークを使用してこれらのローカルでないボリュームに格納されたデータを取得する必要があります。このタイプのネームスペースアーキテクチャでは、自動ノードリファーラルによってパフォーマンスが大幅に向上しない場合があります。

データをホストするノードに使用可能なLIFがない場合、ONTAPは、クライアントが選択したLIFを使用して接続を確立します。SMBクライアントによってファイルが開かれると、クライアントは参照された同じ接続を介してファイルに引き続きアクセスします。

何らかの理由でCIFSサーバがリファーラルを作成できない場合でも、SMBサービスは中断されません。自動ノードリファーラルが有効になっていない場合と同様に、SMB接続が確立されます。

関連情報

Microsoftリモートコピーのパフォーマンスの向上

自動ノードリファーラルの使用に関する要件とガイドライン

SMB 自動ノードリファーラル（別名 _autolocation _ ）を使用する前に、この機能をサポートする ONTAP のバージョンなど、一定の要件について理解しておく必要があります。また、サポートされるSMBプロトコルのバージョンやその他の特別なガイドラインについても確認しておく必要があります。

ONTAPのバージョンとライセンスの要件

- クラスタ内のすべてのノードで、自動ノードリファーラルがサポートされているバージョンのONTAPが実行されている必要があります。
- オートロケーションを使用するには、SMB共有でワイドリンクが有効になっている必要があります。
- CIFSのライセンスが有効になっていて、SVMにSMBサーバが配置されている必要があります。SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMBプロトコルのバージョン

- SVMについては、すべてのバージョンのSMBで自動ノード リファーラルがサポートされます。

SMBクライアントの要件

SMB自動ノード リファーラルは、ONTAPでサポートされるすべてのMicrosoftクライアントでサポートされます。

ONTAPでサポートされるWindowsクライアントの最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

データ**LIF**の要件

データLIFをSMBクライアントのリファーラルとして使用する可能性がある場合は、NFSとCIFSの両方を有効にしたデータLIFを作成する必要があります。

自動ノードリファーラルは、ターゲットノードのデータLIFでNFSプロトコルまたはSMBプロトコルのみが有効になっている場合は機能しないことがあります。

この要件が満たされていない場合でも、データアクセスには影響しません。SMBクライアントは、SVMへの接続に使用した元のLIFを使用して共有をマッピングします。

参照された**SMB**接続を確立する際の**NTLM**認証の要件

CIFSサーバが含まれているドメイン、および自動ノードリファーラルを使用するクライアントが含まれているドメインで、NTLM認証が許可されている必要があります。

リファーラルを作成する際には、SMBサーバからWindowsクライアントに参照先のIPアドレスが渡されます。IPアドレスを使用した接続ではNTLM認証が使用されるため、参照された接続ではKerberos認証は実行されません。

これは、WindowsクライアントがKerberosで使用されるサービスプリンシパル名（および `service/FQDN` の形式）を作成できず、クライアントがサービスに`Kerberos`チケットを要求できないためです `service/NetBIOS name`。

自動ノードリファーラルでホームディレクトリ機能を使用する場合のガイドライン

ホームディレクトリ共有プロパティを有効にして共有を設定すると、ホームディレクトリ設定用に1つ以上のホームディレクトリ検索パスを設定できます。この検索パスで、SVMのボリュームを含む各ノードに格納されているボリュームを指定できます。クライアントはリファーラルを受け取り、使用可能なアクティブなローカルデータLIFがある場合は、ホームユーザのホームディレクトリに対してローカルな参照されたLIFを介して接続します。

SMB 1.0クライアントで自動ノードリファーラルを有効にして動的ホームディレクトリにアクセスする場合は注意が必要です。SMB 1.0クライアントでは、認証を行う前、つまりSMBサーバでユーザの名前が指定されていない前に自動ノードリファーラルが必要になるためです。ただし、次の条件に該当する場合、SMB 1.0クライアントでSMBホームディレクトリへのアクセスは正しく機能します。

- SMB ホームディレクトリは、「 %w 」（ Windows ユーザ名）または「 %u 」（マッピングされた UNIX ユーザ名）のような単純な名前を使用するように設定されており、「 %d\%w 」（ドメイン名 \ ユーザ名 ）のようなドメイン名形式の名前では使用されません。
- ホーム・ディレクトリ共有を作成するときに、 CIFS ホーム・ディレクトリ共有名は変数（「 %w 」または「 %u 」）で設定され、「 home 」などの静的な名前では設定されません。

SMB 2.xクライアントとSMB 3.0クライアントの場合、自動ノードリファーラルを使用してホームディレクトリにアクセスする際に特別なガイドラインはありません。

参照接続が確立されている**CIFS**サーバで自動ノードリファーラルを無効にする場合のガイドライン

オプションを有効にしたあとに自動ノードリファーラルを無効にした場合、参照LIFに現在接続されているクライアントでは参照接続が維持されます。ONTAPではSMB自動ノードリファーラルのメカニズムとしてDFSリファーラルを使用するため、オプションを無効にしたあとも、参照接続用にクライアントにキャッシュされているDFSリファーラルがタイムアウトするまでは参照LIFに再接続できます。これは、自動ノードリファー

ラルがサポートされないバージョンのONTAPにリバートした場合も同様です。クライアントは、DFSリファーラルがクライアントのキャッシュからタイムアウトするまで、リファーラルを使用し続けます。

オートロケーションでは、SMB自動ノードリファーラルを使用して、SVMのデータボリュームを所有するノード上のLIFをクライアントに参照させることで、SMBクライアントのパフォーマンスを向上させます。SMBクライアントがSVM上でホストされているSMB共有に接続するときに、要求されたデータを所有しておらず、クラスタインターコネクトネットワークを使用してデータを取得しているノード上のLIFを使用して接続することがあります。SMB接続で要求されたデータを含むノード上のLIFを使用している場合、クライアントへの応答時間が短縮されます。

ONTAPでは、Microsoftの分散ファイルシステム（DFS）リファーラルを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることをSMBクライアントに通知することで、この機能を実現します。ノードがリファーラルを作成するのは、データを含むノード上にSVMのLIFがあることを特定した場合です。リファーラルは、クライアントの接続に使用する共有のルートの場所に基づいて作成されます。

リファーラルはSMBネゴシエーション中に発生します。リファーラルは、接続が確立される前に作成されます。ONTAPがターゲット ノードに参照先のSMBクライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先LIFパスを介してデータにアクセスします。これにより、クライアントにはより高速なデータ アクセスが提供され、クラスタの余分な通信も回避されます。

Mac OSクライアントで自動ノード リファーラルを使用する際のガイドライン

Mac OSはMicrosoftのDistributed File System（DFS;分散ファイルシステム）をサポートしていますが、Mac OS Xクライアントは**SMB**自動ノード リファーラルをサポートしていません。Windowsクライアントは、SMB共有に接続する前にDFSリファーラル要求を行います。ONTAPは、要求されたデータをホストしているノード上で見つかったデータLIFへのリファーラルを提供します。これによって、クライアントの応答時間が短縮されます。Mac OSでもDFSはサポートされますが、Mac OSクライアントの動作はWindowsクライアントとまったく同じではありません。

関連情報

ONTAPニオケルドウテキホームディレクトリノシクミ

"ネットワーク管理"

"NetApp Interoperability Matrix Tool"

SMB自動ノードリファーラルのサポート

SMB 自動ノードリファーラルを有効にする際に、 ONTAP の一部の機能ではリファーラルがサポートされない点に注意してください。

- SMB 自動ノードリファーラルは、次の種類のボリュームではサポートされません。
  - 負荷共有ミラーの読み取り専用のメンバー
  - データ保護ミラーのデスティネーションボリューム
- LIF が移動してもノードリファーラルは移動しません。

  クライアントが SMB 2.x または SMB 3.0 接続を介した参照接続を使用している場合、データ LIF が無停止で移動してもクライアントは引き続き同じ参照接続を使用します。 LIF がデータに対してローカルでなくなった場合も同様です。

- ボリュームが移動してもノードリファーラルは移動しません。

  クライアントがいずれかの SMB 接続による参照接続を使用している場合、ボリュームが移動してもクライアントは引き続き同じ参照接続を使用します。ボリュームがデータ LIF と異なるノードに移動した場合も同様です。

SMB自動ノードリファーラルの有効化と無効化

SMB自動ノードリファーラルを有効にすると、SMBクライアントアクセスのパフォーマンスを向上させることができます。ONTAPでSMBクライアントを参照しないようにするには、自動ノードリファーラルを無効にします。

開始する前に

Storage Virtual Machine（SVM）でCIFSサーバが設定されて実行されている必要があります。

タスクの内容

SMB自動ノードリファーラル機能は、デフォルトでは無効になっています。必要に応じて、各SVMでこの機能を有効または無効にすることができます。

このオプションは、advanced権限レベルで使用できます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. SMB自動ノードリファーラルを必要に応じて有効または無効にします。

SMB 自動ノードリファーラルの設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   このオプションの設定は、新しいSMBセッションに対して有効になります。既存の接続を使用するクライアントは、既存のキャッシュタイムアウトの期限が切れた場合にのみノードリファーラルを使用できます。

3. admin権限レベルに切り替えます。 `set -privilege admin`

関連情報

使用できるSMBサーバオプション

統計を使用して自動ノードリファーラルのアクティビティを監視する

参照されるSMB接続の数を確認するには、コマンドを使用して自動ノードリファーラルのアクティビティを監視し `statistics`ます。リファーラルを監視することで、自動リファーラルによって共有をホストするノード上の接続が割り当てられている範囲や、CIFS

サーバ上の共有へのローカルアクセスを強化するためにデータLIFを再配置する必要があるかどうかを判断できます。

タスクの内容

オブジェクトには `cifs`、SMB自動ノードリファーラルの監視に役立つadvanced権限レベルのカウンタがいくつか用意されています。

- `node_referral_issued`

  共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントのうち、共有のルートのノードへのリファーラルが発行されたクライアントの数。

- `node_referral_local`

  共有のルートと同じノードでホストされるLIFを使用して接続したクライアントの数。一般に、ローカルアクセスは最適なパフォーマンスを提供します。

- `node_referral_not_possible`

  共有のルートとは別のノードでホストされるLIFを使用して接続したあとに、共有のルートをホストするノードへのリファーラルが発行されていないクライアントの数。共有のルートのノードのアクティブなデータLIFが見つからなかったためです。

- `node_referral_remote`

  共有のルートとは別のノードでホストされるLIFを使用して接続したクライアントの数。リモートアクセスを実行すると、パフォーマンスが低下する可能性があります。

一定期間内のデータ（サンプル）を収集して表示することで、Storage Virtual Machine（SVM）の自動ノードリファーラル統計を監視できます。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

> ⓘ コマンドで収集した情報を評価して使用するには `statistics`、環境内でクライアントがどのように分散しているかを理解しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. コマンドを使用して、自動ノードリファーラルの統計を表示します `statistics`。

   次に、サンプリングされた期間のデータを収集して表示することで、自動ノードリファーラルの統計を表示する例を示します。

   a. 収集を開始します。 `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

b. 目的の収集時間が経過するまで待ちます。

c. 収集を停止します。 `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

d. 自動ノードリファーラルの統計を表示します。 `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                  Value
    ---------------------------- ----------------------------
    node_name                                               node1
    node_referral_issued                                        0
    node_referral_local                                         1
    node_referral_not_possible                                  2
    node_referral_remote                                        2
    ...

    node_name                                               node2
    node_referral_issued                                        2
    node_referral_local                                         1
    node_referral_not_possible                                  0
    node_referral_remote                                        2
    ...
```

出力には、SVM vs1に含まれるすべてのノードのカウンタが表示されます。この例では、わかりやすくするために、自動ノードリファーラルの統計に関連する出力フィールドのみを示しています。

3. admin権限レベルに戻ります。 `set -privilege admin`

関連情報

統計の表示

"パフォーマンス監視のセットアップ"

Windowsクライアントを使用して、クライアント側の**SMB**自動ノードリファーラル情報を監視する

クライアント側から発行されているリファーラルを確認するには、Windowsのユーティリティを使用し `dfsutil.exe`ます。

このユーティリティは、Windows 7以降のクライアントで使用できるRemote Server Administration Tools（RSAT）キットに含まれてい `dfsutil.exe`ます。このユーティリティを使用すると、リファーラルキャッシュの内容に関する情報を表示したり、クライアントが現在使用している各リファーラルに関する情報を表示したりできます。ユーティリティを使用して、クライアントのリファーラルキャッシュをクリアすることもできます。詳細については、Microsoft TechNetライブラリを参照してください。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

アクセスベースの列挙による共有のフォルダのセキュリティを提供する

アクセスベースの列挙による共有のフォルダのセキュリティの概要

Access-Based Enumeration（ABE；アクセスベースの列挙）がSMB共有で有効になっている場合、共有内のフォルダまたはファイルに（個人またはグループの権限制限により）アクセスする権限がないユーザの環境には、共有自体は引き続き表示されますが、その共有リソースは表示されます。

従来の共有プロパティでは、共有内のファイルやフォルダの表示や変更を許可するユーザ（個人またはグループ）を指定できます。ただし、権限のないユーザに対して共有内のフォルダやファイルを表示可能とするかどうかを制御することはできません。この状態だと、共有内のこれらのフォルダ名またはファイル名に、顧客名や開発中の製品などの重要な情報が記述されている場合に問題になることがあります。

ABEでは、共有プロパティが拡張され、共有内のファイルやフォルダの列挙も対象になりました。このため、ABEを使用すると、ユーザのアクセス権に基づいて共有内のファイルやフォルダの表示をフィルタリングできます。つまり、共有自体はすべてのユーザに表示されますが、共有内のファイルやフォルダは指定したユーザに対して表示または非表示にすることができます。ABEを使用すると、職場の機密情報を保護するだけでなく、大規模なディレクトリ構造の表示を簡素化して、すべてのコンテンツにアクセスする必要がないユーザにメリットを提供できます。たとえば、共有自体はすべてのユーザに表示されますが、共有内のファイルやフォルダは表示または非表示にできます。

詳細はこちらをご覧ください "SMB / CIFSアクセスベースの列挙を使用する際のパフォーマンスへの影響"。

SMB共有でのアクセスベースの列挙の有効化または無効化

SMB共有でAccess-Based Enumeration（ABE；アクセスベースの列挙）を有効または無効にすると、ユーザにアクセス権限のない共有リソースが表示されることを許可または禁止できます。

タスクの内容

デフォルトでは、ABE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
新しい共有でABEを有効にする	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share -properties access-based-enumeration`SMB共有の作成時に、追加のオプションの共有設定および追加の共有プロパティを指定できます。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 `vserver cifs share create`ください。
既存の共有でABEを有効にする	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`既存の共有プロパティは維持されます。ABE共有プロパティは既存の共有プロパティリストに追加されます。
既存の共有でABEを無効にする	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`その他の共有プロパティは維持されます。ABE共有プロパティのみが共有プロパティのリストから削除されます。

2. コマンドを使用して、共有設定が正しいことを確認し `vserver cifs share show`ます。

例

次の例は、SVM vs1上のパスで「sales」という名前のABE SMB共有を作成します `/sales`。共有は、共有プロパティとしてを使用して作成され `access-based-enumeration`ます。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例は、「data2」という名前のSMB共有に共有プロパティを追加します `access-based-enumeration`。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ---------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

関連情報

既存のSMB共有に対する共有プロパティの追加または削除

Windowsクライアントからのアクセスベースの列挙を有効または無効にする

SMB共有に対するAccess-Based Enumeration（ABE；アクセスベースの列挙）をWindowsクライアントから有効または無効にすることができます。これにより、CIFSサーバに接続することなく、この共有設定を行うことができます。

この `abecmd`ユーティリティは、Windows ServerおよびWindowsクライアントの新しいバージョンでは使用できません。Windows Server 2008の一部としてリリースされた。Windows Server 2008のサポートは2020年1月14日をもって終了しました。

手順

1. ABEをサポートするWindowsクライアントで、次のコマンドを入力します。 `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   コマンドの詳細については `abecmd`、Windowsクライアントのマニュアルを参照してください。

NFSトSMBノファイルオヨヒテイレクトリノメイメイキソク

NFSとSMBのファイルとディレクトリの命名規則の概要

ファイルとディレクトリの命名規則は、 ONTAP クラスタおよびクライアントの言語設定に加え、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ファイル共有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ファイル共有プロトコルによって、次の項目が決まります。

- 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

ONTAPでは、ONTAPのリリースに応じて、ファイル、ディレクトリ、およびqtreeの名前でマルチバイト文字がサポートされます。

ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、 UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン（ : ）を使用しないでください。コロンは、 MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限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。

マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。マルチプロトコル環境におけるこれらの影響と、SMB共有の作成時にパスを指定する場合や、共有内のデータにアクセスする場合に実行する必要がある対処方法を理解しておく必要があります。

SMBクライアントでという名前のディレクトリを作成すると、 `testdir`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `testdir`。ただし、SMBユーザがあとでディレクトリ名を作成しようとすると、SMBクライアントではその名前がすでに存在しているとみなされるため作成 `TESTDIR`できません。NFSユーザがあとでという名前のディレクトリを作成すると、 `TESTDIR`このディレクトリ名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ディレクトリ名の大文字と小文字が区別されるため、両方のディレクトリ名が作成したとおりにと `TESTDIR`表示されます（例：） `testdir`。
- SMBクライアントでは、2つのディレクトリを区別するために8.3形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TESTDI~1`表示され `testdir`ます。
  - ONTAPは、2つのディレクトリを区別するためにディレクトリ名を作成します `TESTDI~1`。

    この場合、Storage Virtual Machine（SVM）で共有を作成または変更するときに共有パスを指定するときは、8.3形式の名前を使用する必要があります。

ファイルについても同様に、SMBクライアントでを作成すると、 `test.txt`SMBクライアントとNFSクライアントのどちらでもファイル名はと表示されます `text.txt`。ただし、SMBユーザがあとでを作成しようとすると、 `Test.txt`SMBクライアントではその名前がすでに存在しているとみなされるため作成できません。NFSユーザがという名前のファイルをあとで作成すると、 `Test.txt`このファイル名はNFSクライアントとSMBクライアントで次のように異なって表示されます。

- NFSクライアントでは、ファイル名の大文字と小文字が区別されるため、両方のファイル名が作成したとおりに、およびと `Test.txt`表示されます `test.txt`。
- SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。1つのファイルにはベースファイル名が付いています。追加のファイルには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、とが `TEST~1.TXT`表示され `test.txt`ます。
  - ONTAPは、2つのファイルを区別するためにファイル名を作成します `TEST~1.TXT`。

> Vserver cifs character-mappingコマンドを使用して文字マッピングを有効または変更した場合、通常は大文字と小文字が区別されないWindowsでの検索で大文字と小文字が区別されるようになります。

ONTAPでのファイル名とディレクトリ名の作成方法

ONTAP は、 SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2 つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、 ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（ ~ ）と 1~5 の数字が追加されます。

  同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成する `specifications.html`と、ONTAPでは

という8.3形式のファイル名が作成されます `specif~1.htm`。この名前がすでに存在する場合、 ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという別のファイルを作成すると `specifications_new.html`、の8.3形式は `specifications_new.html`になり `specif~2.htm`ます。

マルチバイトのファイル名、ディレクトリ名、**qtree**名の**ONTAP**での処理

ONTAP 9 .5以降では、4バイトのUTF-8エンコード名がサポートされているため、基本多言語面（BMP）以外のUnicode補助文字を含むファイル名、ディレクトリ名、ツリー名を作成および表示できます。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8エンコード名のサポートを有効にするために、コマンドファミリーと `volume`コマンドファミリーで新しい_utf8mb4_言語コードを使用でき `vserver`ます。

次のいずれかの方法で新しいボリュームを作成する必要があります。

- ボリューム・オプションを明示的に設定し `-language`ます。 `volume create -language utf8mb4 {…}`
- ボリュームオプションを指定して作成または変更されたSVMからボリュームオプションを継承し `-language`ます。 `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- ONTAP 9 .6以前では、utf8mb4をサポートするために既存のボリュームを変更することはできません。新しいutf8mb4対応ボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

  SVM は utf8mb4 をサポートするように更新できますが、既存のボリュームの言語コードは元の設定のままです。

  ONTAP 9 .7P1以降を使用している場合は、utf8mb4の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください "ONTAPでの作成後にボリュームの言語を変更できますか。"。

- ONTAP 9 .8以降では、パラメータを使用して、ボリュームの言語を*。utf-8からutf8mb4に変更でき `[-language <Language code>]`ます。ボリュームの言語を変更するには、に連絡します"NetAppのサポート"。

> 4バイトのUTF-8文字を使用するLUN名は現在サポートされていません。

- 通常、Unicode文字データは、Windowsファイルシステムアプリケーションでは16-bit Unicode Transformation Format（UTF-16）を使用し、NFSファイルシステムでは8-bit Unicode Transformation Format（UTF-8）を使用して表されます。

  ONTAP 9 .5より前のリリースでは、Windowsクライアントで作成されたUTF-16の補助文字を含む名前は他のWindowsクライアントには正しく表示されましたが、NFSクライアントではUTF-8に正しく変換されませんでした。同様に、NFSクライアントで作成されたUTF-8の補助文字を含む名前は、Windowsクライアントでは正しく変換されませんでした。

- ONTAP 9 .4以前を実行しているシステムで、有効または無効な補助文字を含むファイル名を作成すると、ONTAPはファイル名を拒否し、無効なファイル名エラーを返します。

  この問題を回避するには、ファイル名にBMP文字のみを使用して補助文字を使用しないようにする

か、ONTAP 9 .5以降にアップグレードしてください。

ONTAP 9以降では、Unicode文字をqtree名に使用できます。

- qtree名を設定または変更するには、コマンドファミリーまたはSystem Managerを使用し `volume qtree` ます。
- qtree名には、日本語や中国語などのUnicode形式のマルチバイト文字を含めることができます。
- ONTAP 9 .5より前のリリースでは、BMP文字（つまり、3バイトで表現できる文字）のみがサポートされていました。

> ONTAP 9 .5より前のリリースでは、qtreeの親ボリュームのジャンクションパスに、Unicode文字を使用したqtree名とディレクトリ名を含めることができます。 `volume show`親ボリュームの言語設定がUTF-8の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定がUTF-8のいずれかでない場合は、ジャンクションパスの一部が数値のNFS名に置き換えられて表示されます。

- 9.5以降のリリースでは、utf8mb4が有効なボリュームにqtreeが含まれていれば、qtree名で4バイト文字がサポートされます。

ボリュームでの**SMB**ファイル名の変換のための文字マッピングの設定

NFSクライアントは、SMBクライアントおよび特定のWindowsアプリケーションで無効な文字を含むファイル名を作成できます。ボリュームでのファイル名の変換のための文字マッピングを設定すると、本来は無効なNFS名を持つファイルにSMBクライアントからアクセスできるようになります。

タスクの内容

SMBクライアントがNFSクライアントによって作成されたファイルにアクセスすると、ONTAPはファイル名を確認します。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、 ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、重要な情報を長いファイル名にエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステム上のクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMBクライアントで有効でない文字を含むファイル名をNFSクライアントが作成する場合は、無効なNFS文字をSMBと特定のWindowsアプリケーションの両方で使用できるUnicode文字に変換するマップを定義できます。たとえば、この機能は、CATIA MCADおよびMathematicaアプリケーションだけでなく、この要件を持つ他のアプリケーションもサポートしています。

文字マッピングはボリューム単位で設定できます。

ボリュームに文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイント全体には適用されません。

  文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字または不正な文字を表すUnicode文字は、通常はファイル名に使用されない文字であることを確認する必要があります。使用されていないと、不要なマッピングが発生します。

たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用されていれば 'Windows クライアントが "a-b`" という名前のファイルにアクセスしようとすると ' その要求は NFS 名 "a:b`" にマップされます (望ましい結果ではありません)

- 文字マッピングを適用したあともマッピングに無効なWindows文字が含まれている場合、ONTAPはWindows 8.3ファイル名にフォールバックします。
- FPolicy通知、NAS監査ログ、およびセキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- DPタイプのSnapMirror関係が作成された場合、ソースボリュームの文字マッピングはデスティネーションDPボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされたWindows名はNFS名に変わるため、名前の検索はNFSのセマンティクスに従って行われます。これには、NFS検索では大文字と小文字が区別されることも含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windowsの大文字と小文字を区別しない動作に依存してはなりません。ただし8.3形式の名前は使用可能で、大文字と小文字は区別されません。
- 部分マッピングまたは無効なマッピング：名前をマッピングしてディレクトリ列挙（「dir」）を実行するクライアントに戻ったあと、生成されたUnicode名がWindowsで有効かどうかがチェックされます。その名前に無効な文字が含まれている場合、またはWindowsで無効な文字が含まれている場合（例：「.」または空白で終わる場合）は、無効な名前の代わりに8.3形式の名前が返されます。

ステップ

1. 文字マッピング「 + 」を設定します

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, …+
```

マッピングは、「 : 」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16進数を使用して入力されたUnicode文字です。例： 3C ： E03C+

コロンで区切られた各ペアの最初の値 `mapping_text`は、変換するNFS文字の16進値です。2番目の値は、SMBで使用されるUnicode値です。マッピングペアは一意である必要があります（1対1のマッピングが存在する必要があります）。

- ソースマッピング +

次の表に、ソースマッピングで許可されるUnicode文字セットを示します。

+

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C		バックスラッシュ
0x3A	：	コロン
0x2A	*	アスタリスク

Unicode 文字	印刷された文字	説明
0x3F	?	疑問符
0x22	"	引用符
0x3C	<	より小さい
0x3E	>	次の値より大きい
0x7C		
縦線	0xB1	±

- ターゲットマッピング

  ターゲット文字には、 U+E0000…U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、 Storage Virtual Machine （ SVM ） vs1 上の「 data 」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver          Volume Name  Character Mapping
---------------  -----------  -----------------------------------------
vs1              data         3c:e17c, 3e:f17d, 2a:f745
```

関連情報

NASネームスペースでのデータボリュームの作成と管理

SMBファイル名の変換のための文字マッピングの管理用コマンド

文字マッピングを管理するには、FlexVolでSMBファイル名の変換に使用する情報を作成、変更、表示、または削除します。

状況	使用するコマンド
新しいファイル文字マッピングを作成する	`vserver cifs character-mapping create`
ファイル文字マッピングに関する情報を表示する	`vserver cifs character-mapping show`

状況	使用するコマンド
既存のファイル文字マッピングを変更する	`vserver cifs character-mapping modify`
ファイル文字マッピングを削除します。	`vserver cifs character-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。

関連情報

ボリュームでのSMBファイル名の変換のための文字マッピングの設定

NASデータへのS3クライアントアクセスの提供

ONTAPでのS3マルチプロトコルのサポート

ONTAP 9 12.1以降では、S3プロトコルを実行するクライアントが、NFSプロトコルとSMBプロトコルを使用するクライアントに提供されるデータと同じデータに再フォーマットすることなくアクセスできるようになりました。この機能により、NASデータを引き続きNASクライアントに提供しながら、S3アプリケーション（データマイニングや人工知能など）を実行するS3クライアントにオブジェクトデータを提供できます。

S3マルチプロトコル機能は次の2つのユースケースに対応します。

1. S3クライアントを使用した既存のNASデータへのアクセス

   従来のNASクライアント（NFSまたはSMB）を使用して作成された既存のデータがNASボリューム（FlexVolまたはFlexGroupボリューム）に格納されている場合は、S3クライアントで分析ツールを使用してデータにアクセスできるようになります。

2. NASプロトコルとS3プロトコルの両方を使用してI/Oを実行できる、最新のクライアント向けのバックエンドストレージ

   NASプロトコルとS3プロトコルの両方を使用して同じデータの読み取りと書き込みが可能なSparkやKafkaなどのアプリケーションに、統合アクセスを提供できるようになりました。

S3マルチプロトコルのサポートの仕組み

ONTAPのマルチプロトコルサポートでは、同じデータセットをファイル階層として、またはバケット内のオブジェクトとして表示できます。そのために、ONTAPは「S3 NASバケット」を作成します。このバケットを使用すると、S3クライアントはS3オブジェクト要求を使用してNASストレージ内のファイルを作成、読み取り、削除、列挙できます。このマッピングは、NASセキュリティ設定に準拠しており、ファイルとディレクトリのアクセス権限を監視し、必要に応じてセキュリティ監査証跡に書き込みます。

このマッピングは、指定されたNASディレクトリ階層をS3バケットとして提供することで実現されます。ディレクトリ階層内の各ファイルはS3オブジェクトとして表されます。S3オブジェクトの名前は、マッピングされたディレクトリから下への相対パスで、ディレクトリ境界はスラッシュ（/）で表されます。

ONTAPで定義されたS3ユーザは、NASディレクトリにマッピングされるバケット用に定義されたバケットポ

リシーに従って、このストレージにアクセスできます。これを実現するには、S3ユーザとSMB / NFSユーザの間にマッピングを定義する必要があります。SMB / NFSユーザのクレデンシャルはNAS権限のチェックに使用され、これらのアクセスから発生する監査レコードに含まれます。

SMBクライアントまたはNFSクライアントによって作成されたファイルは即座にディレクトリに配置されるため、クライアントからはデータが書き込まれる前に参照できます。S3クライアントは異なるセマンティクスを想定しており、すべてのデータが書き込まれるまで新しいオブジェクトはネームスペースに表示されません。S3からNASストレージへのこのマッピングでは、S3のセマンティクスを使用してファイルが作成され、S3の作成コマンドが完了するまでファイルが外部に表示されません。

S3 NASバケットのデータ保護

S3 NASの「バケット」は、S3クライアントのNASデータの単なるマッピングであり、標準のS3バケットではありません。そのため、NetApp SnapMirror S3機能を使用してS3 NASバケットを保護する必要はありません。代わりに、SnapMirrorの非同期ボリュームレプリケーションを使用して、S3 NASバケットを含むボリュームを保護できます。SnapMirror同期およびSVMディザスタリカバリはサポートされません。

ONTAP 9 .14.1以降では、MetroCluster IPおよびFC構成のミラーされたアグリゲートとミラーされていないアグリゲートでS3 NASバケットがサポートされます。

詳細はこちらをご覧ください "SnapMirror非同期"。

S3 NASバケットの監査

S3 NASバケットは従来のS3バケットではないため、バケットに対するアクセスを監査するようにS3監査を設定することはできません。詳細については、をご覧ください "S3の監査"。

ただし、S3 NASバケットにマッピングされたNASファイルとディレクトリのアクセスイベントは、従来のONTAP監査手順を使用して監査できます。そのため、S3処理でNASの監査イベントがトリガーされることがありますが、次の例外があります。

- S3クライアントアクセスがS3ポリシー設定（グループポリシーまたはバケットポリシー）で拒否された場合、イベントのNAS監査は開始されません。これは、SVMの監査チェックの前にS3権限がチェックされるためです。
- S3 GET要求のターゲットファイルのサイズが0の場合、GET要求には0のコンテンツが返され、読み取りアクセスはログに記録されません。
- S3 GET要求のターゲットファイルがユーザにトラバース権限がないフォルダにある場合は、アクセスの試行が失敗し、イベントはログに記録されません。

詳細はこちらをご覧ください "SVMでNASイベントを監査する"。

オブジェクトのマルチパートアップロード

ONTAP 9 .16.1以降では、FlexGroupボリュームで有効になっている場合にオブジェクトマルチパートアップロードがサポートされ"高度な容量分散"ます。

NASファイルストレージでのオブジェクトマルチパートアップロードを使用すると、S3プロトコルクライアントで大きなオブジェクトを小さなパートとしてアップロードできます。オブジェクトマルチパートアップロードには次の利点があります。

- オブジェクトを並行してアップロードできます。

- アップロードに失敗した場合や一時停止した場合は、まだアップロードされていないパーツのみをアップロードする必要があります。オブジェクト全体のアップロードを再開する必要はありません。
- オブジェクトのサイズが事前にわかっていない場合（大きなオブジェクトがまだ書き込まれている場合など）、クライアントはオブジェクトの一部のアップロードをただちに開始し、オブジェクト全体が作成されたあとにアップロードを完了できます。

マルチパートアップロードでは、次のS3処理がサポートされます。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

S3と**NAS**の相互運用性

ONTAP S3 NASバケットは、ここに記載されているものを除き、標準のNASおよびS3機能をサポートします。

NAS機能は現在、**S3 NAS**バケットではサポートされていません。

FabricPoolの大容量階層

S3 NASバケットをFabricPoolの大容量階層として設定することはできません。

S3機能は現在、**S3 NAS**バケットではサポートされていません。

AWSユーザメタデータ

- S3ユーザメタデータの一部として受信したキーと値のペアは、現在のリリースではオブジェクトデータとともにディスクに格納されません。
- プレフィックスが「x-amz-meta」の要求ヘッダーは無視されます。

AWSタグ

- PUT Object要求とMultipart Initiate要求では、プレフィックスが「x-amz-tagging」のヘッダーは無視されます。
- 既存のファイルのタグを更新する要求（PUT、GET、DELETE要求などに？tagging query-stringが指定されている）は、エラーで拒否されます。

バージョン管理

バケットのマッピング設定でバージョン管理を指定することはできません。

- null以外のバージョン指定（versionId=xyz query-string）を含む要求は、エラー応答を受信します。
- バケットのバージョン管理状態を変更する要求が拒否され、エラーが発生します。

S3クライアントアクセスに関するNASデータの要件

S3アクセス用にNASファイルとディレクトリをマッピングする場合は、互換性の問題がいくつかあることを理解しておくことが重要です。S3 NASバケットを使用してサービスを提供する前に、NASファイル階層の調整が必要になる場合があります。

S3 NASバケットは、S3バケット構文を使用してそのディレクトリをマッピングすることでNASディレクトリへのS3アクセスを提供し、ディレクトリツリー内のファイルはオブジェクトとして表示されます。オブジェクト名は、S3バケット設定で指定されたディレクトリに対するファイルのパス名をスラッシュで区切って指定します。

このマッピングでは、S3 NASバケットを使用してファイルとディレクトリが提供される場合、いくつかの要件が課せられます。

- S3名は1024バイトに制限されているため、パス名が長いファイルにS3を使用してアクセスすることはできません。
- ファイル名とディレクトリ名は255文字に制限されているため、オブジェクト名の連続するスラッシュ以外の文字は255文字以下にする必要があります。
- s3では、バックスラッシュ（「\」）で区切られたSMBパス名は、代わりにスラッシュ（「/」）文字を含むオブジェクト名として表示されます。
- マッピングされたNASディレクトリツリーに、合法的なS3オブジェクト名の一部のペアを共存させることはできません。たとえば、有効なS3オブジェクト名「part1/part2」と「part1/part2/part3」は、NASディレクトリツリーに同時に存在できないファイルにマッピングされます。これは、「part1/part2」が名のファイルで、もう一方のディレクトリにあるためです。
  - 「part1/part2」が既存のファイルである場合、「part1/part2/part3」のS3作成は失敗します。
  - 「part1/part2/part3」が既存のファイルである場合、S3による「part1/part2」の作成または削除は失敗します。
  - 既存のオブジェクト（バージョン管理されていないバケット内の）が既存のオブジェクトの名前に一致するS3オブジェクトの作成で置き換えられます。このオブジェクトはNASで保持されますが、完全に一致する必要があります。上記の例では、名前が衝突しても一致しないため、既存のオブジェクトが削除されることはありません。

オブジェクトストアは多数の任意の名前をサポートするように設計されていますが、NASディレクトリ構造では、1つのディレクトリに多数の名前が配置されているとパフォーマンスの問題が発生する可能性があります。特に、スラッシュ（/）文字が含まれていない名前は、すべてNASマッピングのルートディレクトリに配置されます。「NASに対応していない」名前を多用するアプリケーションは、NASマッピングではなく実際のオブジェクトストアバケットでホストする方が適しています。

NASデータへのS3プロトコルアクセスを有効にする

S3プロトコルアクセスを有効にするには、NAS対応のSVMがS3対応サーバと同じ要件（オブジェクトストアサーバの追加など）を満たしていることを確認し、ネットワークと認証の要件を確認します。

ONTAPを新規にインストールする場合は、クライアントにNASデータを提供するようにSVMを設定したあとに、そのSVMへのS3プロトコルアクセスを有効にすることを推奨します。NASプロトコルの設定については、以下を参照してください。

- "NFSの設定"
- "SMBの設定"

開始する前に

S3プロトコルを有効にする前に、次の項目を設定する必要があります。

- S3プロトコルおよび目的のNASプロトコル（NFS、SMB、またはその両方）のライセンスが設定されています。
- 必要なNASプロトコル用にSVMが設定されている。
- NFSサーバまたはSMBサーバが存在します。
- DNSおよびその他の必要なサービスが設定されている。
- NASデータがクライアントシステムにエクスポートまたは共有されています。

タスクの内容

S3クライアントからS3対応SVMへのHTTPSトラフィックを有効にするには、認証局（CA）証明書が必要です。次の3つのソースからのCA証明書を使用できます。

- SVM上の新しいONTAP自己署名証明書。
- SVM上の既存のONTAP自己署名証明書。
- サードパーティの証明書。

NASデータの提供に使用するデータLIFをS3 / NASバケットにも使用できます。特定のIPアドレスが必要な場合は、を参照してください"データLIFを作成する"。LIFでS3データトラフィックを有効にするには、S3サービスデータポリシーが必要です。SVMの既存のサービスポリシーにS3を含めるように変更できます。

S3オブジェクトサーバを作成するときは、クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。S3サーバのFQDNの1文字目をバケット名にすることはできません。

System Manager

1. NASプロトコルが設定されているStorage VMでS3を有効にします。
   a. [ストレージ]>[Storage VM]*をクリックし、NAS対応Storage VMを選択して[設定]をクリックし、[S3]の下をクリックし ます。
   b. 証明書のタイプを選択します。システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。
   c. ネットワークインターフェイスを入力します。
2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。
   ◦ 今後シークレットキーは表示されません。
   ◦ 証明書情報が再度必要な場合は、 [* ストレージ] 、 [Storage VMs] の順にクリックし、 Storage VM を選択して、 [* 設定] をクリックします。

CLI

1. SVMでS3プロトコルが許可されていることを確認します。+
   `vserver show -fields allowed-protocols`
2. このSVMの公開鍵証明書を記録します。+新しいONTAP自己署名証明書が必要な場合は、を参照してください"CA証明書を作成してSVMにインストールする"。
3. サービスデータポリシーを更新する
   a. SVMのサービスデータポリシーを表示します。+
      `network interface service-policy show -vserver svm_name`
   b. とがない場合は、を `data-s3-server services`追加し `data-core`ます。+
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. SVMのデータLIFが要件を満たしていることを確認します。+
   `network interface show -vserver svm_name`
5. S3サーバを作成します。+
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

追加のオプションは、S3サーバの作成時または作成後いつでも指定できます。

- HTTPSはポート443ではデフォルトで有効になっています。ポート番号は、-secure-listener-portオプションを使用して変更できます。+ HTTPSを有効にすると、SSL/TLSとの適切な統合にCA証明書が必要になります。ONTAP 9 .15.1以降では、S3オブジェクトストレージでTLS 1.3がサポートされます。
- HTTPはデフォルトでは無効になっています。有効にすると、サーバはポート80でリスンします。is-http-enabledオプションを指定して有効にするか、-listener-portオプションを使用してポート番号を変更できます。+ HTTPを有効にすると、すべての要求と応答がクリアテキストでネットワーク経由で送信されます。
  1. S3が設定されていることを確認します。+
     `vserver object-store-server show`

例次のコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。
cluster1::> vserver object-store-server show

```
Vserver: vs1

                        Object Store Server Name: s3.example.com
                            Administrative State: up
                          Listener Port For HTTP: 80
                  Secure Listener Port For HTTPS: 443
                                    HTTP Enabled: false
                                   HTTPS Enabled: true
              Certificate for HTTPS Connections: svm1_ca
                                         Comment: Server comment
```

S3 NASバケットの作成

S3 NASバケットは、S3バケット名とNASパスのマッピングです。S3 NASバケットを使用すると、既存のボリュームとディレクトリ構造を持つSVMネームスペースの任意の部分へのS3アクセスを提供できます。

開始する前に

- NASデータを含むSVMにS3オブジェクトサーバが設定されている。
- NASデータはに準拠してい"S3クライアントアクセスの要件"ます。

タスクの内容

SVMのルートディレクトリ内の任意のセットのファイルとディレクトリを指定するようにS3 NASバケットを設定できます。

また、次のパラメータを任意に組み合わせてNASデータへのアクセスを許可または禁止するバケットポリシーを設定することもできます。

- ファイルおよびディレクトリ
- ユーザおよびグループの権限
- S3処理

たとえば、大規模なユーザグループに読み取り専用データアクセスを許可するバケットポリシーと、そのデータのサブセットに対して限定されたグループに処理の実行を許可するバケットポリシーが必要になる場合があります。

S3 NASの「バケット」はマッピングであり、S3バケットではないため、次の標準S3バケットのプロパティはS3 NASバケットには適用されません。

- * aggr-list\aggr-list-multiplier \storage-service-level \volume\size\exclude-aggr-list\qos-policy-group *+ S3 NASバケットの設定時にボリュームまたはqtreeが作成されません。
- * role\is-protected\is-protected-on-\ is-protected-on-cloud *+ S3 ONTAPバケットは、SnapMirror S3を使用

して保護またはミラーリングされませんが、代わりにボリューム単位で使用できる通常のSnapMirror保護が使用されます。

- バージョン管理状態+ NASボリュームには、通常、異なるバージョンを保存するためのスナップショット・テクノロジーが備わっています。ただし、S3 NASバケットでは現在バージョン管理を使用できません。
- * logical-used\object-count *+と同等の統計情報は、volumeコマンドを使用してNASボリュームに対して利用できます。

System Manager

NAS対応Storage VMに新しいS3 NASバケットを追加します。

1. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。
2. S3 NASバケットの名前を入力してStorage VMを選択し、サイズを入力せずに* More Options *をクリックします。
3. 有効なパス名を入力するか、[参照]をクリックして有効なパス名のリストから選択します。+有効なパス名を入力すると、S3 NAS設定に関係のないオプションは表示されません。
4. S3ユーザをNASユーザとグループにすでにマッピングしている場合は、権限を設定し、* Save *をクリックします。+この手順で権限を設定する前に、S3ユーザをNASユーザにマッピングしておく必要があります。

それ以外の場合は、* Save *をクリックしてS3 NASバケットの設定を完了します。

CLI

NASファイルシステムを含むSVMにS3 NASバケットを作成します。+
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name -type nas -nas-path junction_path [-comment text]`

例：+
```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /vol1
```

S3クライアントユーザを有効にする

S3クライアントユーザがNASデータにアクセスできるようにするには、S3ユーザ名を対応するNASユーザにマッピングし、バケットのサービスポリシーを使用してNASデータにアクセスする権限をユーザに付与する必要があります。

開始する前に

クライアントアクセスのユーザ名（Linux / UNIX、Windows、S3クライアントユーザ）がすでに存在している必要があります。

S3の一部の機能はであることに注意して"S3 NASバケットではサポートされない"ください。

タスクの内容

S3ユーザ名を対応するLinux/UNIXまたはWindowsユーザにマッピングすると、NASファイルがS3クライアントからアクセスされたときにNASファイルの認証チェックが有効になります。S3からNASへのマッピングは、単一の名前またはPOSIXの正規表現で指定できるS3ユーザ名_Pattern_、およびLinux/UNIXまた

はWindowsのユーザ名_Replacement _を指定して指定します。

ネームマッピングが存在しない場合は、デフォルトのネームマッピングが使用され、S3ユーザ名自体がUNIXユーザ名およびWindowsユーザ名として使用されます。UNIXおよびWindowsのデフォルトのユーザ名マッピングは、コマンドを使用して変更できます `vserver object-store-server modify`。

ローカルのネームマッピング設定のみがサポートされます。LDAPはサポートされません。

S3ユーザをNASユーザにマッピングしたら、ユーザに権限を付与できます。ユーザがアクセスできるリソース（ディレクトリとファイル）と、そのユーザに対して実行を許可または許可しないアクションを指定できます。

System Manager

1. UNIXクライアントまたはWindowsクライアント（またはその両方）のローカルネームマッピングを作成します。
   a. Storage > Buckets *をクリックし、S3 / NAS対応のStorage VMを選択します。
   b. を選択し、[ネームマッピング]（[ホストユーザとグループ]*）をクリックします → 。
   c. S3からWindows または S3からUNIX へのタイル（またはその両方）で、 Add をクリックし、目的の Pattern （**S3**）および Replacement *（NAS）ユーザ名を入力します。
2. クライアントアクセスを許可するバケットポリシーを作成します。
   a. [Storage]>[Buckets]をクリックし、目的の**S3**バケットの横にあるをクリックし ⋮ て、[Edit]*をクリックします。
   b. [*追加（Add）]をクリックし、必要な値を入力する。
      - * Principal *- S3ユーザ名を指定するか、デフォルト（すべてのユーザ）を使用します。
      - エフェクト-「*許可」または「*拒否」を選択します。
      - アクション-これらのユーザーとリソースのアクションを入力します。オブジェクトストアサーバで現在S3 NASバケットに対してサポートされているリソース処理のセットは、GetObject、PutObject、DeleteObject、ListBucket、GetBucketAclです。 GetObjectAcl 、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning、ListBucketVersionsの各メソッドに対応しています。このパラメータではワイルドカードを使用できます。
      - * Resources *-アクションを許可または拒否するフォルダまたはファイルのパスを入力するか、デフォルト（バケットのルートディレクトリ）を使用します。

CLI

1. UNIXクライアントまたはWindowsクライアント（またはその両方）のローカルネームマッピングを作成します。+
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position`-マッピング評価のプライオリティ番号。1または2を入力します。
   - `-pattern`- S3ユーザ名または正規表現
   - `-replacement`- WindowsまたはUNIXのユーザ名

例+
```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. クライアントアクセスを許可するバケットポリシーを作成します。+
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}`-ユーザが操作を要求したときにアクセスを許可するか拒否するかを指定します。

- `-action <Action>, …`-許可または拒否されるリソース操作を指定しますオブジェクトストアサーバで現在S3 NASバケットに対してサポートされている一連のリソース処理は、GetObject、PutObject、DeleteObject、ListBucket、GetBucketAcl、GetObjectAcl、およびGetBucketLocationです。このパラメータではワイルドカードを使用できます。
- `-principal <Objectstore Principal>, …`-このパラメータで指定したオブジェクトストアサーバのユーザまたはグループに対して、アクセスを要求しているユーザを検証します。
  - オブジェクトストアサーバグループを指定するには、グループ名にプレフィックスグループ/を追加します。
  - `-principal-`（ハイフン文字）は、すべてのユーザにアクセス権を付与します。
- `-resource <text>, …`-権限の許可/拒否を設定するバケット、フォルダ、またはオブジェクトを指定します。このパラメータではワイルドカードを使用できます。
- `[-sid <SID>]`-オブジェクトストアサーバのバケットポリシーのステートメントのテキストコメント（オプション）を指定します。

例+

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ

Microsoft Hyper-VおよびSQL Server向けのSMBの設定の概要

ONTAP の機能を使用すると、 SMB プロトコルを介した Microsoft アプリケーション、 Microsoft Hyper-V および Microsoft SQL Server の 2 つのノンストップオペレーションを有効にできます。

これらの手順は、SMBのノンストップオペレーションを実装する場合に使用します。想定している状況は次のとおりです。

- SMBプロトコルの基本的なファイルアクセスが設定されている。
- SVM にある SMB 3.0 以降のファイル共有を有効にして次のオブジェクトを格納する。
  - Hyper-Vカソウマシンファイル
  - SQL Serverシステムデータベース

関連情報

ONTAPテクノロジおよび外部サービスとのやり取りの詳細については、次のテクニカルレポート（TR）を参照してください。** "NetAppテクニカルレポート4172：『Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices』" "ネットアップテクニカルレポート 4369 ：『 Best Practices for Microsoft SQL Server and

SnapManager 7.2 for SQL Server with Clustered Data ONTAP 』"

Microsoft Hyper-VおよびSQL Server over SMBソリューション用のONTAPの設定

SMB 3.0以降のファイル共有では、継続的可用性を備えたファイル共有を使用して、Hyper-V仮想マシンファイルまたはは SQL ServerのシステムデータベースとユーザデータベースをSVM上のボリュームに格納し、同時に計画的イベントと計画外イベントのノンストップオペレーション（NDO）を実現できます。

Microsoft Hyper-V over SMB

Hyper-V over SMBソリューションを作成するには、まずMicrosoft Hyper-Vサーバにストレージサービスを提供するようにONTAPを設定する必要があります。また、Microsoftクラスタ（クラスタ構成を使用する場合）、Hyper-Vサーバ、CIFSサーバによってホストされている共有へのSMB 3.0の継続的可用性を備えた接続、および必要に応じて、SVMボリュームに格納されている仮想マシンファイルを保護するためのバックアップサービスも設定する必要があります。

Hyper-Vサーバは、Windows Server 2012以降で設定する必要があります。Hyper-Vサーバの構成は、スタンドアロン構成とクラスタ構成の両方がサポートされます。

- MicrosoftクラスタおよびHyper-Vサーバの作成については、MicrosoftのWebサイトを参照してください。
- SnapManager for Hyper-Vは、Snapshotコピーベースの高速バックアップサービスを容易に実現するホストベースのアプリケーションで、Hyper-V over SMB構成と統合できるように設計されています。

  Hyper-V over SMB 構成での SnapManager の使用については、 SnapManager for Hyper-V インストレーションアドミニストレーションガイドを参照してください。

Microsoft SQL Server over SMB

SQL Server over SMBソリューションを作成するには、まずMicrosoft SQL Serverアプリケーションにストレージサービスを提供するようにONTAPを設定する必要があります。また、Microsoftクラスタも設定する必要があります（クラスタ構成を使用している場合）。その後、WindowsサーバにSQL Serverをインストールして設定し、CIFSサーバによってホストされている共有への継続的可用性を備えたSMB 3.0接続を作成します。必要に応じて、SVMボリュームに格納されているデータベースファイルを保護するようにバックアップサービスを設定できます。

Windows Server 2012以降にSQL Serverをインストールして設定する必要があります。スタンドアロン構成とクラスタ構成の両方がサポートされます。

- Microsoftクラスタの作成およびSQL Serverのインストールと設定の詳細については、MicrosoftのWebサイトを参照してください。
- SnapCenter Plug-in for Microsoft SQL Serverは、Snapshotコピーベースの高速バックアップサービスを容易に実現するホストベースのアプリケーションで、SQL Server over SMB構成と統合できるように設計されています。

  SnapCenter Plug-in for Microsoft SQL Serverの使用方法については、のドキュメントを参照してください "SnapCenter Plug-in for Microsoft SQL Server"。

Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨン

Hyper-V および **SQL Server over SMB** のノンストップオペレーションとは何ですか

Hyper-VおよびSQL Server over SMBのノンストップオペレーションとは、さまざまな管理タスクの間も、アプリケーションサーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持し、継続的可用性を実現できる機能のことです。これには、ストレージインフラの計画的停止と計画外停止の両方が含まれます。

SMBを介したアプリケーションサーバのノンストップオペレーションは、次のとおりです。

- 計画的なテイクオーバーとギブバック
- 計画外のテイクオーバー
- アップグレード
- 計画的なアグリゲートの再配置（ARL）
- LIF の移行とフェイルオーバー
- 計画的なボリュームの移動

SMB経由のノンストップオペレーションを実現するプロトコル

SMB 3.0のリリースに伴い、Microsoftから、Hyper-V over SMBおよびSQL Server over SMBのノンストップオペレーションのサポートに必要な機能を提供する新しいプロトコルがリリースされました。

ONTAP では、 SMB を介したアプリケーションサーバのノンストップオペレーションを実現するために、それらのプロトコルを使用しています。

- SMB 3.0
- 監視

Hyper-Vオヨヒ**SQLServeroverSMB**ノノンストツフオヘレエシヨンニカンスルキナ概念

Hyper-V over SMB または SQL Server over SMB 解決策を設定する前に理解しておくべきノンストップオペレーション（ NDO ）の概念があります。

- * 共有の継続的な可用性 *

  継続的可用性プロパティが設定されている SMB 3.0 共有。継続的可用性を備えた共有を介して接続しているクライアントは、テイクオーバー、ギブバック、およびアグリゲート移転などのシステム停止を伴うイベントが発生しても、

- * ノード *

  クラスタのメンバーである単一のコントローラ。SFO ペアの 2 つのノードを区別するために、 1 つのノードを _local node_name と呼び、もう 1 つのノードを _partner node_or_remote node_name と呼ぶことがあります。ストレージのプライマリ所有者はローカルノードです。セカンダリ所有者は、プライマリ所有者に障害が発生したストレージを制御するパートナーノードです。各ノードは、そのストレージのプラ

イマリ所有者と、そのパートナーストレージのセカンダリ所有者です。

- * 無停止でのアグリゲートの再配置 *

  クライアントアプリケーションを中断することなく、クラスタの SFO ペア内のパートナーノード間でアグリゲートを移動できること。

- * 無停止フェイルオーバー *

  テイクオーバーを参照してください。

- * 無停止での LIF の移行 *

  LIF を介してクラスタに接続されたクライアントアプリケーションを中断することなく、 LIF を移行できること。SMB 接続の場合は、 SMB 2.0 以降を使用して接続するクライアントでのみ可能です。

- * ノンストップオペレーション * 。

  クライアントアプリケーションを中断することなく、 ONTAP の主な管理およびアップグレード操作を実行でき、ノード障害に耐えられること。全体として、この用語は、無停止テイクオーバー、無停止アップグレード、および無停止移行の各機能を指します。

- * 無停止アップグレード *

  アプリケーションを中断することなくノードのハードウェアまたはソフトウェアをアップグレードできること。

- * 無停止ボリューム移動 *

  ボリュームを使用しているすべてのアプリケーションを中断することなく、クラスタ内で自由にボリュームを移動できること。SMB 接続の場合、 SMB のすべてのバージョンで無停止でのボリューム移動がサポートされます。

- * 永続的ハンドル *

  接続が切断した場合に、継続的可用性を備えた接続が透過的に CIFS サーバに再接続できるように設定する SMB 3.0 のプロパティ。永続性ハンドルと同様に、接続中のクライアントとの通信が失われたあとの一定期間、 CIFS サーバによって永続的ハンドルが維持されます。ただし、永続的ハンドルは、永続性ハンドルよりも弾力性があります。CIFS サーバは、再接続後のクライアントにハンドルを 60 秒間使用する猶予を与え、その 60 秒間は、ファイルへのアクセスを要求する他のクライアントからのアクセスを拒否します。

  永続的ハンドルに関する情報は SFO パートナーの永続的ストレージにミラー化されます。これにより、永続的ハンドルを切断したクライアントが、 SFO パートナーによってノードのストレージの所有権が引き継がれた後に、永続性ハンドルを再利用することができるようになります。永続的ハンドルは、 LIF の移動（永続性ハンドルによってサポートされる）だけでなく、テイクオーバー、ギブバック、およびアグリゲートの再配置についても無停止での処理を提供します。

- * SFO ギブバック *

  テイクオーバーイベントから戻るときにホーム位置にアグリゲートを戻します。

- * SFO ペア *

2 つのノードのどちらかが機能を停止した場合に相互にデータを処理するようにコントローラが設定されたノードのペア。システムモデルに応じて、両方のコントローラを 1 つのシャーシに配置することも、別々のシャーシに配置することもできます。2 ノードクラスタでの HA ペアを指します。

- * テイクオーバー *

  ストレージのプライマリ所有者が失敗したときに、パートナーがストレージの制御を引き継ぐプロセス。SFO の文脈では、フェイルオーバーとテイクオーバーは同義です。

SMB 3.0の機能が**SMB**共有を介したノンストップオペレーションをサポートする仕組み

SMB 3.0 には、 Hyper-V over SMB および SQL Server over SMB 共有のノンストップオペレーションをサポートするためのきわめて重要な機能があります。これには、共有プロパティおよび_persistent handle_と呼ばれるファイルハンドルの一種が含まれます `continuously-available`。このハンドルを使用すると、SMBクライアントはファイルオープン状態を再要求し、SMB接続を透過的に再確立できます。

永続的ハンドルは、継続的な可用性が設定された共有に接続する SMB 3.0 対応のクライアントに付与できます。SMB セッションが切断された場合、 CIFS サーバは永続的ハンドルの状態に関する情報を保持します。CIFS サーバは、クライアントが再接続できる 60 秒間は他のクライアント要求をブロックするため、永続的ハンドルを持つクライアントは、ネットワークの切断後にハンドルを再要求できます。永続的ハンドルを持つクライアントは、Storage Virtual Machine（SVM）のいずれかのデータLIFを使用して、同じLIFまたは別のLIFを介して再接続できます。

アグリゲートの再配置、テイクオーバー、およびギブバックはすべて、 SFO ペア間で行われます。永続的ハンドルを持つファイルを使用したセッションの切断と再接続をシームレスに管理するために、パートナーノードでは、すべての永続的ハンドルのロック情報のコピーが保持されます。イベントが計画的か計画外かに関係なく、 SFO パートナーは、永続的ハンドルの再接続を無停止で管理できます。この新機能を使用すると、従来では業務が停止する状況となるイベントでも、 CIFS サーバへの SMB 3.0 接続を、 SVM に割り当てられた別のデータ LIF に透過的に無停止でフェイルオーバーできます。

永続的ハンドルを使用すると、CIFSサーバはSMB 3.0接続を透過的にフェイルオーバーできますが、障害によってHyper-VアプリケーションがWindows Serverクラスタ内の別のノードにフェイルオーバーされた場合、クライアントは切断されたハンドルのファイルハンドルを再要求できません。このシナリオでは、切断状態のファイルハンドルによって、Hyper-Vアプリケーションを別のノードで再起動した場合に、そのアプリケーションへのアクセスがブロックされる可能性があります。「フェイルオーバークラスタリング」は、 SMB 3.0 の一部で、古い競合するハンドルを無効にするメカニズムを提供して、このシナリオに対処します。このメカニズムを使用すると、 Hyper-V クラスタノードに障害が発生した場合に、 Hyper-V クラスタを迅速にリカバリできます。

透過的なフェイルオーバーを強化するための監視プロトコルの機能

監視プロトコルにより、 SMB 3.0 の継続的な可用性が確保された共有（ CA 共有）に対するクライアントフェイルオーバー機能が強化されます。監視を使用すると、 LIF のフェイルオーバーのリカバリがバイパスされるため、フェイルオーバーにかかる時間が短縮されます。ノードを使用できなくなると、 SMB 3.0 接続のタイムアウトを待たずにアプリケーションサーバに通知されます。

フェイルオーバーはシームレスです。クライアント上で実行されているアプリケーションは、フェイルオーバーが発生したことを認識しません。監視プロトコルを使用できなくてもフェイルオーバー処理に影響はありませんが、監視プロトコルを使用しないフェイルオーバーは効率が落ちます。

監視プロトコルを使用する高度なフェイルオーバーは、次の要件が満たされた場合に実行できます。

- SMB 3.0 が有効になっている SMB 3.0 対応の CIFS サーバでのみ使用できる。
- 共有で、共有の継続的な可用性プロパティが設定されている SMB 3.0 を使用している必要があります。
- アプリケーションサーバの接続先ノードのSFOパートナーに、少なくとも1つ以上、アプリケーションサーバのデータをホストするStorage Virtual Machine（SVM）に割り当てられた稼働中のデータLIFがある。

> 監視プロトコルは、 SFO ペアの間で実行されます。LIF はクラスタ内の任意のノードに移行できるため、すべてのノードがその SFO パートナーの監視プロトコルであることが必要になる場合があります。アプリケーションサーバのデータをホスティングしている SVM がパートナーノード上にアクティブなデータ LIF を持っていない場合、監視プロトコルは、指定されたノード上で SMB 接続の迅速なフェイルオーバーを提供することはできません。したがって、そのような構成の 1 つをホスティングしている SVM には、クラスタ内のすべてのノードに少なくとも 1 つ以上のデータ LIF が必要です。

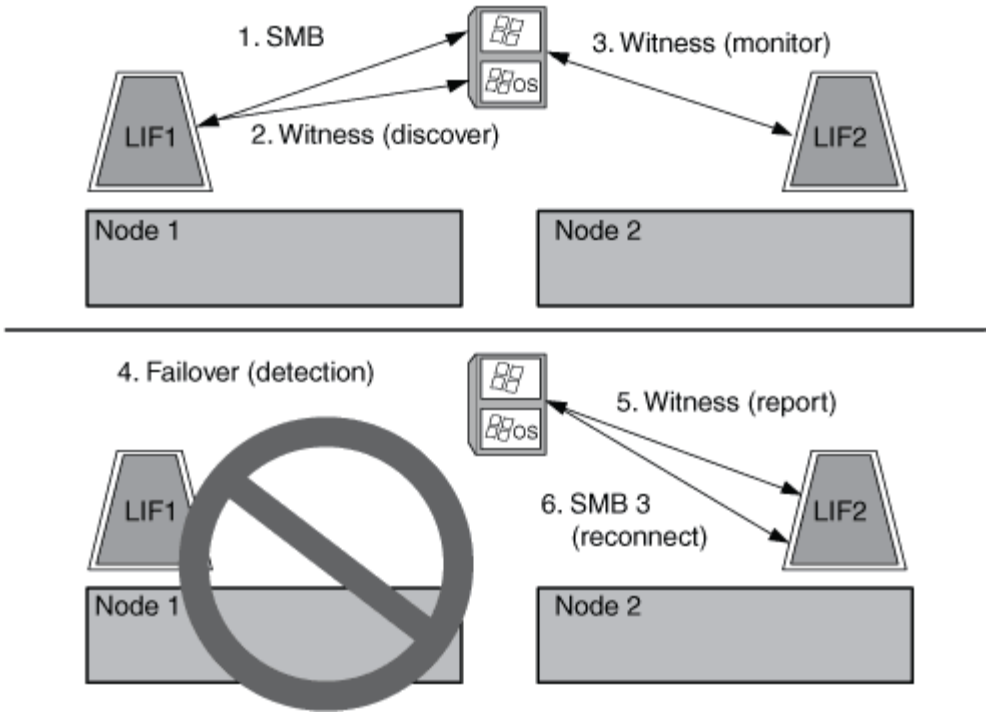
- アプリケーションサーバは、個々の LIF IP アドレスではなく、 DNS に格納されている CIFS サーバ名を使用して CIFS サーバに接続する必要があります。

監視プロトコルの仕組み

ONTAPは、ノードのSFOパートナーを監視として使用して、監視プロトコルを実装します。障害が発生した場合、パートナーは障害を迅速に検出し、SMBクライアントに通知します。

監視プロトコルでは、次のプロセスを使用してフェイルオーバーが強化されます。

1. アプリケーションサーバがノード1への継続的可用性を備えたSMB接続を確立すると、CIFSサーバからアプリケーションサーバに監視が利用可能であることが通知されます。
2. アプリケーションサーバは、ノード 1 に監視サーバの IP アドレスを要求し、 Storage Virtual Machine （ SVM ）に割り当てられたノード 2 （ SFO パートナー）のデータ LIF の IP アドレスリストを受け取ります。
3. アプリケーションサーバは、いずれかのIPアドレスを選択し、ノード2への監視接続を作成して、ノード1の継続的可用性を備えた接続を移行する必要がある場合に通知されるように登録します。
4. ノード 1 でフェイルオーバーが発生した場合、監視によってフェイルオーバーが容易になりますが、ギブバックには影響しません。
5. 監視によってフェイルオーバーイベントが検出され、監視接続を介してアプリケーションサーバに、SMB接続をノード2に移行する必要があることが通知されます。
6. アプリケーションサーバは、 SMB セッションをノード 2 に移行し、クライアントアクセスを中断することなく接続をリカバリします。



リモート**VSS**による共有ベースのバックアップ

リモート**VSS**を使用した共有ベースのバックアップの概要

リモートVSSを使用して、CIFSサーバに格納されているHyper-V仮想マシンファイルの共有ベースのバックアップを実行できます。

MicrosoftのリモートVSS（ボリュームシャドウコピーサービス）は、既存のMicrosoft VSSインフラを拡張したものです。リモートVSSでは、SMB共有のシャドウコピーをサポートするようにVSSインフラが拡張されました。また、Hyper-Vなどのサーバアプリケーションでは、SMBファイル共有にVHDファイルを格納できます。これらの拡張機能を使用すると、データと構成ファイルを共有に格納する仮想マシンに対して、アプリケーションと整合性のあるシャドウコピーを作成できます。

リモート**VSS**の概念

ここでは、リモートVSS（ボリュームシャドウコピーサービス）がHyper-V over SMB構成でバックアップサービスでどのように使用されるかを理解するために必要な概念について説明します。

- * VSS （ボリューム・シャドウ・コピー・サービス） *

  特定のボリューム上の特定の時点のデータのバックアップコピーまたはSnapshotを作成するMicrosoftのテクノロジ。VSSは、データサーバ、バックアップアプリケーション、ストレージ管理ソフトウェアを調整して、整合性のあるバックアップの作成と管理をサポートします。

- * リモート VSS （リモートボリュームシャドウコピーサービス） *

  SMB 3.0共有を介してデータにアクセスした特定の時点で整合性のあるデータの共有ベースのバックアップコピーを作成するMicrosoftのテクノロジです。Volume Shadow Copy Service と呼ばれることもあります。

- * シャドウコピー *

  共有に含まれるデータセットの明確に定義された特定の時点における複製です。シャドウコピーは、整合性のあるポイントインタイムバックアップを作成するために使用されます。これにより、システムまたはアプリケーションは元のボリューム上のデータを継続的に更新できます。

- * シャドウ・コピー・セット *

  1つ以上のシャドウコピーの集まりで、各シャドウコピーが1つの共有に対応します。シャドウコピーセット内のシャドウコピーは、同じ処理でバックアップする必要があるすべての共有を表します。セットに含めるシャドウコピーは、VSS対応アプリケーションのVSSクライアントによって識別されます。

- * シャドウ・コピー・セットの自動リカバリ *

  リモートVSSに対応したバックアップアプリケーションのバックアッププロセスの一部。シャドウコピーが格納されているレプリカディレクトリでポイントインタイムの整合性が確保されます。バックアップの開始時に、アプリケーション上のVSSクライアントは、バックアップ用にスケジュールされたデータ（Hyper-Vの場合は仮想マシンファイル）のソフトウェアチェックポイントの取得をアプリケーションにトリガーします。VSSクライアントは、アプリケーションの続行を許可します。シャドウコピーセットが作成されると、リモートVSSによってシャドウコピーセットが書き込み可能になり、書き込み可能なコピーがアプリケーションに公開されます。アプリケーションは、前の手順で作成したソフトウェアチェックポイントを使用して自動リカバリを実行し、シャドウコピーセットをバックアップ用に準備します。自動リカバリでは、チェックポイントの作成後にファイルとディレクトリに加えられた変更を展開することで、シャドウコピーを整合性のある状態にします。自動リカバリは、VSS対応バックアップのオプションの手順です。

- * シャドウ・コピー ID *

  シャドウコピーを一意に識別するGUIDです。

- * シャドウ・コピー・セット ID *

  同じサーバに対する一連のシャドウコピーIDを一意に識別するGUID。

- * SnapManager for Hyper-V *

  Microsoft Windows Server 2012 Hyper-Vのバックアップ / リストア処理を自動化して簡易化するソフトウェアです。リモートVSSと自動リカバリを使用して、SMB共有経由でHyper-Vファイルをバックアップします。

関連情報

Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨンニカンスルキナ概念

リモートVSSによる共有ベースのバックアップ

リモート**VSS**で使用されるディレクトリ構造の例

リモートVSSは、シャドウコピーの作成時に、Hyper-V仮想マシンファイルが格納されているディレクトリ構造をトラバースします。仮想マシンファイルのバックアップを正常に作成できるように、適切なディレクトリ構造について理解しておくことが重要です。

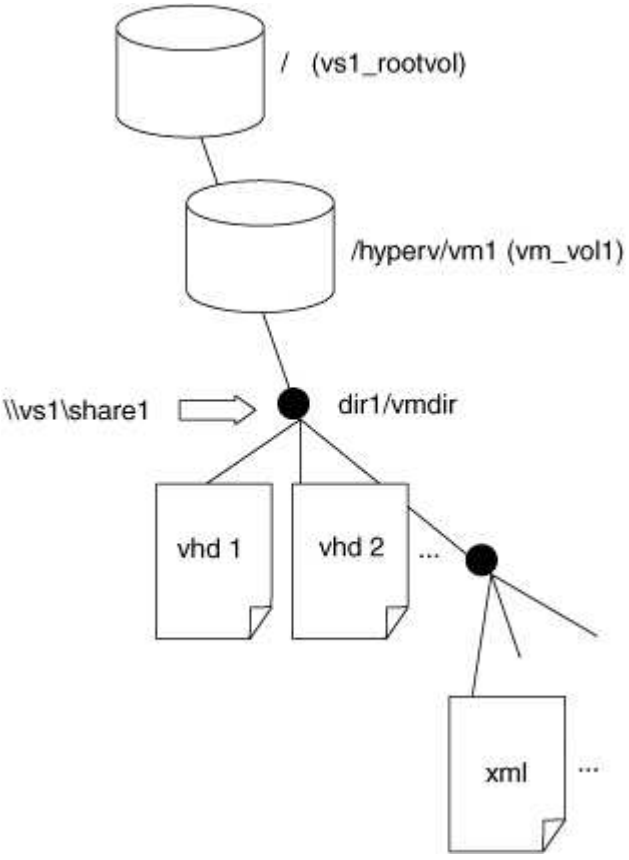
シャドウコピーを正常に作成するためにサポートされるディレクトリ構造は、次の要件を満たしています。

- 仮想マシンファイルの格納に使用されるディレクトリ構造内に存在するのは、ディレクトリと通常のファイルだけです。

  ディレクトリ構造には、ジャンクション、リンク、または通常以外のファイルは含まれません。

- 仮想マシンのファイルはすべて単一の共有内に存在します。
- 仮想マシンファイルの格納に使用されるディレクトリ構造が、設定されているシャドウコピーのディレクトリ階層を超えることはありません。
- 共有のルートディレクトリには、仮想マシンファイルまたはディレクトリのみが含まれています。

次の図では、Storage Virtual Machine（SVM）vs1上でジャンクションポイントをにしてvm_vol1という名前のボリュームが作成されています `/hyperv/vm1`。ジャンクションポイントの下に、仮想マシンファイルを格納するサブディレクトリが作成されます。Hyper-Vサーバの仮想マシンファイルには、パスのshare1を介してアクセスします `/hyperv/vm1/dir1/vmdir`。シャドウコピーサービスによって、share1の下のディレクトリ構造（設定されたシャドウコピーのディレクトリ階層まで）に格納されているすべての仮想マシンファイルのシャドウコピーが作成されます。



SnapManager for Hyper-Vによる**Hyper-V over SMB**のリモート**VSS**ベースのバックアップの管理方法

SnapManager for Hyper-V を使用して、リモート VSS ベースのバックアップサービスを管理できます。スペース効率に優れたバックアップセットを作成するには、SnapManager for Hyper-V で管理されているバックアップサービスを使用すると効果的です。

Hyper-V で管理されているバックアップ向けに SnapManager を最適化するには、次のようなものがあります。

- SnapDrive と ONTAP の統合により、 SMB 共有の場所を検出する際のパフォーマンスが最適化されます。

  ONTAP は、共有が存在するボリュームの名前を SnapDrive に提供します。

- SnapManager for Hyper-V は、シャドウコピーサービスでコピーする必要がある SMB 共有内の仮想マシンファイルのリストを指定します。

  仮想マシンファイルの対象リストを指定することで、シャドウコピーサービスで、共有内のすべてのファイルのシャドウコピーを作成する必要がなくなります。

- Storage Virtual Machine （ SVM ）に、 Hyper-V がリストアに使用するための SnapManager の Snapshot コピーが保持されます。

  バックアップフェーズはありません。バックアップは、スペース効率に優れた Snapshot コピーです。

SnapManager for Hyper-V は、次のプロセスを使用して、 Hyper-V over SMB のバックアップとリストアの機能を提供します。

1. シャドウコピー処理を準備しています

   SnapManager for Hyper-V アプリケーションの VSS クライアントが、シャドウコピーセットを設定します。VSS クライアントは、どの共有をシャドウコピーセットに含めるかに関する情報を収集し、この情報を ONTAP に提供します。セットには 1 つ以上のシャドウコピーが含まれる場合があり、 1 つのシャドウコピーが 1 つの共有に対応します。

2. シャドウコピーセットの作成（自動リカバリが使用される場合）

   シャドウコピーセットに含まれている共有ごとに、 ONTAP がシャドウコピーを作成し、シャドウコピーを書き込み可能にします。

3. シャドウコピーセットの公開

   ONTAP によって作成されたシャドウコピーが Hyper-V 用の SnapManager に公開され、アプリケーションの VSS ライターが自動リカバリを実行できるようになります。

4. シャドウコピーセットを自動的にリカバリします

   シャドウコピーセットの作成中に、バックアップセットに含まれているファイルにアクティブな変更が発生する時間帯があります。アプリケーションの VSS ライターは、シャドウコピーを更新して、バックアップ前に完全な整合性が確保された状態にする必要があります。

   自動リカバリの実行方法はアプリケーションに固有です。リモート VSS はこのフェーズには関連しません。

5. シャドウコピーセットの完了とクリーンアップを行います

   自動リカバリの完了後に、 VSS クライアントが ONTAP に通知します。シャドウコピーセットが読み取り専用になり、バックアップできる状態になります。バックアップに SnapManager for Hyper-V を使用する場合は、 Snapshot コピー内のファイルがバックアップになるため、バックアップフェーズでは、バッ

クアップセット内の共有を含むボリュームごとに Snapshot コピーが作成されます。バックアップが完了すると、シャドウコピーセットが CIFS サーバから削除されます。

Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピーオフロードの使用方法

Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _copy offloaded _ とも呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。ONTAP ODXコピーオフロードを使用すると、アプリケーションサーバでSMBインストール経由のコピー処理を実行する際のパフォーマンスが向上します。

ODX以外のファイル転送では、ソースCIFSサーバからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションCIFSサーバに転送します。要約すると、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODXファイル転送では、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現されるパフォーマンス上のメリットには、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用率（CPU、メモリ）の削減、ネットワークI/O帯域幅の使用量の削減などがあります。

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
```
ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとStorage Virtual Machine（SVM）は同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。

データは複数のSVMに所有されます。

Hyper-VソリューションでのODXコピーオフロードの具体的なユースケースには、次のようなものがあります。

- Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク（VHD）ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

  これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。

> Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

SQL ServerソリューションでのODXコピーオフロードの具体的なユースケースには、次のようなものがあります。

- ODXコピーオフロードを使用すると、マッピングされたSMB共有間、または同じクラスタ内のSMB共有と接続されたiSCSI LUNの間でSQL Serverデータベースのエクスポートとインポートを行うことができます。
- ソースとデスティネーションのストレージが同じクラスタにある場合は、ODXコピーオフロードを使用してデータベースのエクスポートとインポートを行います。

設定に関する要件と考慮事項

ONTAPとライセンスの要件

SVMでノンストップオペレーションを実現するSQL Server over SMBまたはHyper-V over SMBソリューションを作成するときは、ONTAPとライセンスの特定の要件について理解しておく必要があります。

ONTAPのバージョンの要件

- Hyper-V over SMB

  ONTAPでは、Windows Server 2012以降で実行されるHyper-VでのSMB共有を介したノンストップ オペレーションがサポートされます。

- SQL Server over SMB

  ONTAPでは、Windows Server 2012以降で実行されるSQL Server 2012以降でのSMB共有を介したノンストップ オペレーションがサポートされます。

SMB共有を介したノンストップ オペレーションがサポートされるONTAP、Windows Server、およびSQL Serverのバージョンの最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ライセンス要件

次のライセンスが必要です。

- CIFS
- FlexClone（Hyper-V over SMBのみ）

  このライセンスは、バックアップにリモートVSSを使用する場合に必要になります。シャドウ コピー サービスでは、バックアップの作成時に使用されるファイルのポイントインタイム コピーを作成するためにFlexCloneが使用されます。

  リモートVSSを使用しないバックアップ方式を使用する場合、FlexCloneライセンスはオプションです。

FlexCloneライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneがない場合は、必要に"必要なライセンスがインストールされていることを確認する"応じて、必要に応じて"インストールする"を実行する必要があります。

ネットワークとデータ**LIF**の要件

ノンストップオペレーション用にSQL Server over SMBまたはHyper-V over SMB構成を作成する場合は、一定のネットワークとデータLIFの要件について理解しておく必要があります。

ネットワークプロトコルの要件

- IPv4およびIPv6ネットワークがサポートされています。
- SMB 3.0以降が必要です。

  SMB 3.0には、ノンストップオペレーションを実現するために必要な、継続的可用性を備えたSMB接続の確立に必要な機能が用意されています。

- DNSサーバには、CIFSサーバ名をStorage Virtual Machine（SVM）上のデータLIFに割り当てられたIPアドレスにマッピングするエントリが格納されている必要があります。

  通常、Hyper-VまたはSQL Serverアプリケーションサーバは、仮想マシンまたはデータベースファイルへのアクセス時に複数のデータLIFを介して複数の接続を確立します。正常に機能するためには、アプリケーションサーバは、複数の一意のIPアドレスへの複数の接続を確立するのではなく、CIFSサーバ名を使用してこれらの複数のSMB接続を確立する必要があります。

  監視でも、個 々 のLIF IPアドレスではなく、CIFSサーバのDNS名を使用する必要があります。

  ONTAP 9 .4以降では、SMBマルチチャネルを有効にすることで、Hyper-V over SMBおよびSQL Server over SMB構成のスループットとフォールトトレランスを向上させることができます。そのためには、クラスタとクライアントに1G、10G、またはそれ以上のNICを複数導入する必要があります。

データ**LIF**の要件

- SMB経由のアプリケーションサーバソリューションをホストするSVMには、クラスタ内のすべてのノードに稼働しているデータLIFが少なくとも1つ必要です。

  SVMデータLIFは、アプリケーションサーバがアクセスするデータを現在ホストしていないノードを含む、クラスタ内の他のデータポートにフェイルオーバーできます。さらに、監視ノードは常にアプリケーションサーバが接続されているノードのSFOパートナーであるため、クラスタ内のすべてのノードが監視ノードになる可能性があります。

- データLIFは、自動的にリバートされるように設定しないでください。

  テイクオーバーまたはギブバックの発生後、データLIFをホームポートに手動でリバートする必要があります。

- すべてのデータLIFのIPアドレスがDNSにエントリを持ち、すべてのエントリがCIFSサーバ名に解決される必要があります。

  アプリケーションサーバは、CIFSサーバ名を使用してSMB共有に接続する必要があります。LIFのIPアドレスを使用して接続を確立するようにアプリケーションサーバを設定しないでください。

- CIFSサーバ名がSVM名と異なる場合は、DNSエントリがCIFSサーバ名に解決される必要があります。

Hyper-V over SMB用の**SMB**サーバとボリュームの要件

ノンストップオペレーション用にHyper-V over SMB構成を作成する場合、一定のSMBサーバとボリュームの要件について理解しておく必要があります。

SMBサーバの要件

- SMB 3.0が有効になっている必要があります。

  これはデフォルトで有効になっています。

- デフォルトのUNIXユーザのCIFSサーバオプションが、有効なUNIXユーザアカウントを使用して設定されている必要があります。

  アプリケーションサーバは、SMB接続の作成時にマシンアカウントを使用します。すべてのSMBアクセスで、Windowsユーザが1つのUNIXユーザアカウントまたはデフォルトのUNIXユーザアカウントに正常にマッピングされている必要があるため、ONTAPは、アプリケーションサーバのマシンアカウントをデフォルトのUNIXユーザアカウントにマッピングできる必要があります。

- 自動ノードリファーラルを無効にする必要があります（この機能はデフォルトで無効になっています）。

  Hyper-Vマシンファイル以外のデータへのアクセスに自動ノードリファーラルを使用する場合は、そのデータ用のSVMを別途作成する必要があります。

- SMB サーバが属しているドメインで、 Kerberos と NTLM の両方の認証が許可されている必要があります。

  ONTAPはリモートVSSに対してKerberosサービスをアドバタイズしないため、ドメインはNTLMを許可するように設定する必要があります。

- シャドウコピー機能が有効になっている必要があります。

  この機能はデフォルトで有効になっています。

- シャドウコピーサービスでシャドウコピーの作成時に使用されるWindowsドメインアカウントが、SMBサーバのローカルのBUILTIN\AdministratorsグループまたはBUILTIN\Backup Operatorsグループに属している必要があります。

ボリュームの要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

  継続的可用性を備えたSMB接続を使用してアプリケーションサーバのNDOを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したNDOに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、SMB共有を介したNDOに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です。

  使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

SQLServeroverSMBノ**SMB**サアハトホリユウムノヨウケン

ノンストップオペレーション用にSQL Server over SMB構成を作成する場合は、SMBサーバとボリュームの一定の要件について理解しておく必要があります。

SMBサーバの要件

- SMB 3.0が有効になっている必要があります。

  これはデフォルトで有効になっています。

- デフォルトのUNIXユーザのCIFSサーバオプションが、有効なUNIXユーザアカウントを使用して設定されている必要があります。

  アプリケーションサーバは、SMB接続の作成時にマシンアカウントを使用します。すべてのSMBアクセスで、Windowsユーザが1つのUNIXユーザアカウントまたはデフォルトのUNIXユーザアカウントに正常にマッピングされている必要があるため、ONTAPは、アプリケーションサーバのマシンアカウントをデフォルトのUNIXユーザアカウントにマッピングできる必要があります。

また、SQL ServerはドメインユーザをSQL Serverサービスアカウントとして使用します。サービスアカウントは、デフォルトのUNIXユーザにもマッピングする必要があります。

- 自動ノードリファーラルを無効にする必要があります（この機能はデフォルトで無効になっています）。

  SQL Serverデータベースファイル以外のデータへのアクセスに自動ノードリファーラルを使用する場合は、そのデータ用のSVMを別途作成する必要があります。

- ONTAPへのSQL Serverのインストールに使用するWindowsユーザアカウントには、SeSecurityPrivilege権限を割り当てる必要があります。

  この権限は、SMBサーバのローカルのBUILTIN\Administratorsグループに割り当てられます。

ボリュームの要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

  継続的可用性を備えたSMB接続を使用してアプリケーションサーバのNDOを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したNDOに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、SMB共有を介したNDOに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- データベースファイルを含むボリュームにジャンクションを含めることはできますが、SQL Serverではデータベースディレクトリ構造の作成時にジャンクションをまたぐことはありません。
- SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理を成功させるには、ボリュームに十分な利用可能スペースが必要です。

  SQL Serverデータベースファイルが配置されているボリュームには、データベースディレクトリ構造と、共有内に格納されているすべてのファイルを格納できる十分なサイズが必要です。

関連情報

"Microsoft TechNetライブラリ：technet.microsoft.com/en-us/library/"

Hyper-V over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートするHyper-V over SMB構成で継続的可用性を備えた共有を設定する場合は、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。

共有の要件

- アプリケーションサーバで使用される共有には、continuously-availableプロパティが設定されている必要があります。

継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイルロックを再要求できます。

- リモートVSSに対応したバックアップサービスを使用する場合は、ジャンクションを含む共有にHyper-Vファイルを配置することはできません。

  自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、シャドウコピーの作成は失敗します。自動リカバリ以外の場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

- リモートVSSに対応したバックアップサービスと自動リカバリを使用する場合は、次の内容を含む共有にHyper-Vファイルを配置できません。
  - シンボリックリンク、ハードリンク、またはワイドリンク
  - 通常以外のファイル

    シャドウコピーを実行する共有にリンクまたは通常以外のファイルがある場合、シャドウコピーの作成は失敗します。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

  - シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です（ Hyper-V over SMB の場合のみ）。

    使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

- アプリケーションサーバで使用される継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 属性のキャッシュ
  - BranchCache

考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- Hyper-V over SMB構成では、次の機能はサポートされません。
  - 監査
  - FPolicy
- パラメータがに設定され `Yes`ているSMB共有ではウィルススキャンは実行されません `continuously-availability`。

SQL Server over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートするSQL Server over SMB構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項について理解しておく必要があります。

共有の要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

  継続的可用性を備えたSMB接続を使用してアプリケーションサーバのノンストップオペレーションを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップオペレーションに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップオペレーションに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- アプリケーションサーバで使用される共有には、continuously-availableプロパティが設定されている必要があります。

  継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイルロックを再要求できます。

- データベースファイルを含むボリュームにジャンクションを含めることはできますが、SQL Serverではデータベースディレクトリ構造の作成時にジャンクションをまたぐことはありません。
- SnapCenter Plug-in for Microsoft SQL Serverの処理を成功させるには、ボリュームに十分な利用可能スペースが必要です。

  SQL Serverデータベースファイルが配置されているボリュームには、データベースディレクトリ構造と、共有内に格納されているすべてのファイルを格納できる十分なサイズが必要です。

- アプリケーションサーバで使用される継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 属性のキャッシュ
  - BranchCache

共有に関する考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- SQL Server over SMB構成では、次の機能はサポートされません。
  - 監査
  - FPolicy
- 共有プロパティが設定されているSMB共有ではウィルススキャンは実行されません `continuously-availability`。

Hyper-VoverSMBコウセイニカンスルリモオト**VSS**ニカンスルコウリヨシコウ

Hyper-V over SMB 構成用のリモート VSS に対応したバックアップソリューションを使用する場合は、一定の考慮事項について理解しておく必要があります。

一般的なリモート **VSS** の考慮事項

- Microsoft のアプリケーションサーバ 1 つにつき、最大 64 の共有を設定できます。

  1 つのシャドウコピーセットに 64 個を超える共有がある場合、シャドウコピー処理は失敗します。これはMicrosoftの要件です。

- アクティブなシャドウコピーセットは、 1 台の CIFS サーバで 1 つしか許可されません。

  同じCIFSサーバでシャドウコピー処理を実行中の場合、シャドウコピー処理は失敗します。これはMicrosoftの要件です。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、ジャンクションは許可されません。
  - 自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、シャドウコピーの作成は失敗します。
  - 自動リカバリではない場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

自動リカバリを行うシャドウコピーのみに適用されるリモート **VSS** の考慮事項

一部の制限は、自動リカバリを行うシャドウコピーにのみ適用されます。

- シャドウコピーの作成で許可される最大サブディレクトリ階層は 5 層です。

  これは、シャドウコピーサービスによってシャドウコピーバックアップセットが作成されるディレクトリ階層です。仮想マシンファイルを含むディレクトリのネストレベルが 5 よりも深い場合、シャドウコピーの作成は失敗します。この目的は、共有のクローニング時におけるディレクトリのトラバーサルを制限することです。最大ディレクトリ階層は CIFS サーバオプションを使用して変更できます。

- ボリューム上に利用可能なスペースが十分ある必要があります。

  使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、リンクまたは通常以外のファイルは許可されません。

  シャドウコピーの作成は、そのシャドウコピーに対応する共有内にリンクまたは通常以外のファイルがある場合には失敗します。これらのファイルはクローニングプロセスでサポートされていません。

- ディレクトリに対する NFSv4 ACL は許可されません。

  シャドウコピーの作成では、ファイルの NFSv4 ACL は維持されますが、ディレクトリの NFSv4 ACL は失われます。

- シャドウコピーセットの作成に許可される時間は最大 60 秒です。

Microsoft の仕様により、シャドウコピーセットの作成に許可される時間は最大 60 秒です。この時間内に VSS クライアントでシャドウコピーセットを作成できない場合、シャドウコピー処理は失敗します。したがって、シャドウコピーセット内のファイル数には制限があります。バックアップセットに含めることができる実際のファイル数または仮想マシン数は、一定ではなく、多くの要因に依存するため、お客様の環境ごとに判断する必要があります。

SQL ServerおよびHyper-V over SMBでのODXコピーオフロードの要件

アプリケーションサーバ経由でデータを送信せずに、仮想マシンファイルを移行する場合や、データベースファイルをソースストレージからデスティネーションストレージに直接エクスポートおよびインポートする場合は、 ODX コピーオフロードが有効になっている必要があります。ODX コピーオフロードと SQL Server および Hyper-V over SMB ソリューションを使用する場合は、理解しておくべきいくつかの要件があります。

ODX コピーオフロードを使用すると、パフォーマンスが大幅に向上します。この CIFS サーバオプションは、デフォルトで有効に設定されています。

- ODX コピーオフロードを使用するには、 SMB 3.0 が有効になっている必要があります。
- ソースボリュームは1.25GB以上である必要があります。
- コピーオフロードに使用するボリュームで重複排除を有効にする必要があります。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは8Kのみです。

  二次圧縮形式はサポートされません

- ODX コピーオフロードを使用して Hyper-V ゲストをディスク内やディスク間で移行するには、 Hyper-V サーバが SCSI ディスクを使用するように設定されている必要があります。

  デフォルトでは IDE ディスクが設定されますが、ディスクが IDE ディスクを使用して作成されている場合は、ゲストの移行時に ODX コピーオフロードは機能しません。

SQL ServerおよびHyper-V over SMB構成に関する推奨事項

SQL Server over SMB および Hyper-V over SMB 構成が安定して機能するようにするには、ソリューションの設定に関する推奨されるベストプラクティスについて理解しておく必要があります。

一般的な推奨事項

- アプリケーションサーバのファイルは一般的なユーザデータとは別に格納します。

  可能な場合は、 Storage Virtual Machine （ SVM ）とそのストレージ全体をアプリケーションサーバのデータ専用にします。

- パフォーマンスを最大限に高めるには、アプリケーションサーバのデータを格納する SVM で SMB 署名を無効にします。
- パフォーマンスの最適化とフォールトトレランスの向上を図るためには、 SMB マルチチャネルを有効にして、 1 つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立できるようにします。

- Hyper-VまたはSQL Server over SMB構成で使用する共有以外では、継続的可用性を備えた共有を作成しないでください。
- 継続的な可用性を確保するために使用される共有については、変更通知を無効に
- アグリゲートの再配置（ ARL ）には一部の処理が一時停止するフェーズがあるため、 ARL と同時にボリュームの移動を実行しないようにします。
- Hyper-V over SMBソリューションでは、クラスタ化された仮想マシンを作成するときにゲスト内iSCSIドライブを使用します。ONTAP SMB共有のHyper-V over SMBでは共有 `.VHDX`ファイルはサポートされません。

Hyper-VまたはSQL Server over SMB構成の計画

ボリューム構成ワークシートに記入する

このワークシートを使用すると、 SQL Server および Hyper-V over SMB 構成用のボリュームを作成する際に必要となる値を簡単に記録できます。

ボリュームごとに、次の情報を指定する必要があります。

- Storage Virtual Machine（SVM）名

  SVM 名はすべてのボリュームで同じです。

- ボリューム名
- アグリゲート名

  ボリュームは、クラスタ内のノード上のアグリゲートに作成できます。

- サイズ
- ジャンクションパス

アプリケーションサーバのデータを格納するボリュームの作成時には、次の事項を考慮してください。

- ルートボリュームのセキュリティ形式が NTFS でない場合は、ボリュームの作成時にセキュリティ形式を NTFS として指定する必要があります。

  デフォルトで、ボリュームは SVM ルートボリュームのセキュリティ形式を継承します。

- ボリュームには、デフォルトのボリュームスペースギャランティを設定する必要があります。
- 必要に応じて、スペースのオートサイズ管理を設定できます。
- Snapshotコピーのスペースリザベーションを決定するオプションは、に設定する必要があります `0`。
- ボリュームに適用される Snapshot ポリシーを無効にする必要があります。

  SVM の Snapshot ポリシーが無効になっている場合は、ボリュームの Snapshot ポリシーを指定する必要はありません。ボリュームは SVM の Snapshot ポリシーを継承します。SVM の Snapshot ポリシーが無効になっておらず、 Snapshot コピーを作成するように設定されている場合は、 Snapshot ポリシーをボリュームレベルで指定し、そのポリシーを無効にする必要があります。Snapshot コピーの作成と削除は、シャドウコピーサービス対応のバックアップと SQL Server バックアップによって管理されます。

- ボリュームに負荷共有ミラーを設定することはできません。

アプリケーションサーバで使用される共有を作成するジャンクションパスを選択する際は、共有エントリポイントの下に結合されたボリュームが含まれないようにする必要があります。

たとえば、仮想マシンファイルを「 vol1 」、「 vol2 」、「 vol3 」、および「 vol4 」という名前の 4 つのボリュームに格納する場合は、例に示すネームスペースを作成できます。その後、アプリケーションサーバの共有をパス、、 `/data1/vol2` `/data2/vol3`、およびに `/data2/vol4`作成できます `/data1/vol1`。

```
                        Junction                            Junction
Vserver Volume          Active   Junction Path              Path Source
------- ------------ -------- --------------------   -----------
vs1     data1         true     /data1                 RW_volume
vs1     vol1          true     /data1/vol1            RW_volume
vs1     vol2          true     /data1/vol2            RW_volume
vs1     data2         true     /data2                 RW_volume
vs1     vol3          true     /data2/vol3            RW_volume
vs1     vol4          true     /data2/vol4            RW_volume
```

情報の種類	値
ボリューム*1*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*2*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*3*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*4*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*5*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム*6*：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
追加ボリューム：ボリューム名、アグリゲート、サイズ、ジャンクションパス _	

SMB共有設定ワークシートに記入する

このワークシートを使用して、SQL ServerおよびHyper-V over SMB構成用の継続的可用性を備えたSMB共有を作成する際に必要となる値を記録してください。

SMB共有のプロパティと設定に関する情報

共有ごとに、次の情報を指定する必要があります。

- Storage Virtual Machine（SVM）名

  SVM 名はすべての共有で同じです

- 共有名
- パス
- 共有プロパティ

  次の2つの共有プロパティを設定する必要があります。

  - `oplocks`
  - `continuously-available`

次の共有プロパティは設定しないでください。

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - シンボリックリンクを無効にする必要があります（パラメータの値 `-symlink-properties`はnull [""]にする必要があります）。

共有パスに関する情報

リモートVSSを使用してHyper-Vファイルをバックアップする場合は、Hyper-Vサーバから仮想マシンファイルの格納場所へのSMB接続を確立する際に使用する共有パスの選択が重要になります。共有はネームスペース内の任意のポイントに作成できますが、Hyper-Vサーバで使用される共有のパスに結合されたボリュームを含めることはできません。ジャンクションポイントを含む共有パスでシャドウコピー処理を実行することはできません。

データベースディレクトリ構造を作成する場合、SQL Serverはジャンクションを横断できません。ジャンクションポイントを含むSQL Serverの共有パスは作成しないでください。

たとえば、次に示すネームスペースを例にとると、仮想マシンファイルまたはデータベースファイルをボリューム「vol1」、「vol2」、「vol3」、および「vol4」に格納する場合、アプリケーションサーバの共有をパス、、 `/data1/vol2`、 `/data2/vol3`およびに `/data2/vol4`作成する必要があります `/data1/vol1`。

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

管理用にパスと `/data2`パスに共有を作成することはできます `/data1`が、データの格納にこれらの共有を使用するようにアプリケーションサーバを設定しないでください。

計画ワークシート

情報の種類	値
ボリューム*1*：*SMB*共有名とパス	
ボリューム*2*：*SMB*共有名とパス	
ボリューム*3*：*SMB*共有名とパス	
ボリューム*4*：*SMB*共有名とパス	
ボリューム*5*：*SMB*共有名とパス	
ボリューム*6*：*SMB*共有名とパス	
ボリューム*7*：*SMB*共有名とパス	
追加ボリューム： SMB 共有名およびパス _	

Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成の作成

Hyper-Vオヨビ**SQLServeroverSMB**テノンストツフオヘレエシヨンヲシツケンスル**ONTAP**セツテイノカイヨウ

SMBを介したノンストップオペレーションを実現するHyper-VおよびSQL Server環境を使用するためには、ONTAPの設定手順をいくつか実行する必要があります。

Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成を作成する前に、次のタスクを完了しておく必要があります。

- クラスタでタイムサービスをセットアップする必要があります。
- SVM用のネットワークをセットアップします。
- SVMを作成します。
- SVMでデータLIFインターフェイスが設定されている必要があります。
- SVMでDNSが設定されている必要があります。
- SVMに必要なネームサービスをセットアップします。
- SMBサーバを作成しておく必要があります。

関連情報

Hyper-VまたはSQL Server over SMB構成の計画

設定に関する要件と考慮事項

Kerberos認証と**NTLMv2**認証の両方が許可されていることの確認（**Hyper-V over SMB**共有）

Hyper-V over SMB のノンストップオペレーションを実行する場合、データ SVM の CIFS サーバおよび Hyper-V サーバで Kerberos 認証と NTLMv2 認証の両方が許可されていなければなりません。CIFS サーバと Hyper-V サーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。

タスクの内容

Kerberos 認証は、継続的可用性を備えた共有への接続を確立する際に必要になります。また、リモート VSS のプロセスで NTLMv2 認証が使用されます。そのため、 Hyper-V over SMB 構成に対しては、両方の認証方法を使用した接続がサポートされている必要があります。

Kerberos 認証と NTLMv2 認証の両方が許可されるように、次の設定を行う必要があります。

- Storage Virtual Machine （ SVM ）で SMB のエクスポートポリシーが無効になっている必要があります。

SVM では、 Kerberos 認証と NTLMv2 認証がどちらも常に有効になりますが、エクスポートポリシーを使用することで認証方法に基づいてアクセスを制限することが可能です。

SMB のエクスポートポリシーは省略可能で、デフォルトでは無効になっています。エクスポートポリシーが無効になっている場合、 CIFS サーバでは Kerberos 認証と NTLMv2 認証の両方がデフォルトで許可されます。

- CIFS サーバと Hyper-V サーバが属するドメインで、 Kerberos 認証と NTLMv2 認証の両方を許可する必要があります。

Kerberos 認証は、 Active Directory ドメインではデフォルトで有効になります。ただし、 NTLMv2 認証は、セキュリティポリシーの設定またはグループポリシーで禁止されている場合があります。

手順

1. 次の手順に従って、 SVM でエクスポートポリシーが無効になっていることを確認します。
   a. 権限レベルをadvancedに設定します。

      ```
      set -privilege advanced
      ```

b. CIFSサーバオプションがに設定されている `false`ことを確認し `-is-exportpolicy-enabled`ます。

vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

c. admin権限レベルに戻ります。

set -privilege admin

2. SMB のエクスポートポリシーが無効になっていない場合は無効にします。

vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

ドメインで許可されている認証方法を確認する方法については、Microsoft TechNetライブラリを参照してください。

4. ドメインで NTLMv2 認証が許可されていない場合は、 Microsoft のドキュメントに記載されたいずれかの方法で NTLMv2 認証を有効にします。

例

次に、SVM vs1でSMBのエクスポートポリシーが無効になっていることを確認するコマンドの例を示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

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

ドメインアカウントがデフォルトの**UNIX**ユーザにマッピングされていることを確認する

Hyper-V および SQL Server では、継続的可用性を備えた共有への SMB 接続を作成する際にドメインアカウントを使用します。接続を作成するには、コンピュータアカウントが UNIX ユーザに正しくマッピングされている必要があります。そのための最も便利な方法は、コンピュータアカウントをデフォルトの UNIX ユーザにマッピングすることです。

タスクの内容

Hyper-V および SQL Server は、ドメインコンピュータアカウントを使用して SMB 接続を作成します。また、 SQL Server は、 SMB 接続を作成するサービスアカウントとしてドメインユーザアカウントを使用します。

Storage Virtual Machine（SVM）を作成すると、ONTAPによってデフォルトユーザ「pcuser」（UIDが）とグループ「pcuser」（GIDが 65534）が自動的に作成され 65534、デフォルトユーザが「pcuser」グループに追加されます。クラスタをData ONTAP 8 2にアップグレードする前に使用していたSVMでHyper-V over SMBソリューションを設定する場合は、デフォルトのユーザとグループが存在していない可能性があります。デフォルトの UNIX ユーザを設定していない場合は、 CIFS サーバのデフォルトの UNIX ユーザを設定する前に、デフォルトのユーザとグループを作成する必要があります。

手順

1. デフォルトの UNIX ユーザが存在するかどうかを確認します。

   vserver cifs options show -vserver *vserver_name*

2. デフォルトユーザオプションが設定されていない場合は、デフォルトの UNIX ユーザとして指定できる UNIX ユーザが存在するかどうかを確認します。

   vserver services unix-user show -vserver *vserver_name*

3. デフォルトユーザオプションが設定されておらず、デフォルトの UNIX ユーザとして指定できる UNIX ユーザも存在しない場合は、デフォルトの UNIX ユーザとデフォルトのグループを作成し、デフォルトのユーザをそのグループに追加します。

   通常、デフォルトユーザにはユーザ名「pcuser」が与えられ、のUIDを割り当てる必要があります。`65534`デフォルトのグループには ' 通常 ' グループ名として pcuser が与えられますグループに割り当てるGIDはである必要があり `65534`ます。

   a. デフォルトグループを作成します。+
      vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534

   b. デフォルトユーザを作成し、デフォルトグループに追加します。+
      vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534

   c. デフォルトのユーザとデフォルトグループが正しく設定されていることを確認します。
      vserver services unix-user show -vserver *vserver_name*++
      vserver services unix-group show -vserver *vserver_name* -members

4. CIFS サーバのデフォルトのユーザが設定されていない場合は、次の手順を実行します。

   a. デフォルトユーザを設定します。

      vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser***

   b. デフォルトの UNIX ユーザが正しく設定されていることを確認します。

      vserver cifs options show -vserver *vserver_name*

5. アプリケーションサーバのコンピュータアカウントがデフォルトのユーザに正しくマッピングされている

ことを確認するには、SVMの共有にドライブをマッピングし、コマンドを使用してWindowsユーザとUNIXユーザのマッピングを確認します `vserver cifs session show`。

このコマンドの使用方法の詳細については、マニュアルページを参照してください。

例

次のコマンドでは、 CIFS サーバのデフォルトのユーザが設定されていないことがわかりますが、「 pcuser 」ユーザと「 pcuser 」グループは存在します。「 pcuser 」ユーザは、 SVM vs1 上の CIFS サーバのデフォルトのユーザとして割り当てられています。

```
cluster1::> vserver cifs options show

Vserver: vs1

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



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser
```

```
cluster1::> vserver cifs options show

Vserver: vs1

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

SVMルートボリュームのセキュリティ形式が**NTFS**に設定されていることを確認する

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合は、ボリュームを NTFS セキュリティ形式で作成する必要があります。ルートボリュームのセキュリティ形式には、Storage Virtual Machine（SVM）で作成されたボリュームのデフォルトが適用されるため、ルートボリュームのセキュリティ形式はNTFSに設定する必要があります。

タスクの内容

- ルートボリュームのセキュリティ形式は SVM の作成時に指定できます。
- SVMの作成時にルートボリュームのセキュリティ形式をNTFS以外に設定した場合は、あとでコマンドを使用してセキュリティ形式を変更できます `volume modify`。

手順

1. SVM のルートボリュームの現在のセキュリティ形式を確認します。

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. ルートボリュームのセキュリティ形式が NTFS 以外になっている場合は、セキュリティ形式を NTFS に変更します。

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. SVM のルートボリュームのセキュリティ形式が NTFS に設定されていることを確認します。

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

例

次に、SVM vs1のルートボリュームのセキュリティ形式がNTFSになっていることを確認するコマンドの例を示します。

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

必要な**CIFS**サーバオプションが設定されていることの確認

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合、必要な CIFS サーバオプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。

タスクの内容

- SMB 2.x と SMB 3.0 が有効になっている必要があります。
- パフォーマンスが向上したコピーオフロードを使用するには、 ODX コピーオフロードが有効になっている必要があります。
- Hyper-V over SMB 解決策でリモート VSS に対応したバックアップサービスを使用する場合は、 VSS シャドウコピーサービスが有効になっている必要があります（ Hyper-V のみ）。

手順

1. Storage Virtual Machine（SVM）で必要なCIFSサーバオプションが有効になっていることを確認します。
   a. 権限レベルをadvancedに設定します。

      `set -privilege advanced`

   b. 次のコマンドを入力します。

      `vserver cifs options show -vserver *vserver_name*`

      次のオプションをに設定する必要があり `true`ます。

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled`（Hyper-Vのみ）
2. いずれかのオプションがに設定されていない場合は `true`、次の手順を実行します。

a. コマンドを使用して `vserver cifs options modify`に設定します `true`。

b. コマンドを使用して、 `vserver cifs options show`オプションがに設定されていることを確認し `true`ます。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次に、SVM vs1でHyper-V over SMB構成の必須オプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、 ODX コピーオフロードのオプションを有効にする必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

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

パフォーマンスと冗長性を確保するための**SMB**マルチチャネルの設定

ONTAP 9 .4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立できます。これにより、Hyper-V over SMBおよびSQL Server over SMB構成のスループットとフォールトトレランスが向上します。

開始する前に

SMBマルチチャネル機能は、クライアントがSMB 3.0以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMBサーバではSMB 3.0以降がデフォルトで有効になっています。

タスクの内容

SMBクライアントは、ONTAPクラスタで適切な設定が見つかると、複数のネットワーク接続を自動的に検出

して使用します。

SMBセッションでの同時接続数は、導入しているNICによって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

  クライアントはNICごとに1つの接続を確立し、すべての接続にセッションをバインドします。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

  クライアントはNICごとに最大4つの接続を確立し、すべての接続にセッションをバインドします。クライアントは、10G以上の容量の複数のNICで接続を確立できます。

また、次のパラメータを変更することもできます（advanced権限）。

- `-max-connections-per-session`

  マルチチャネルセッションごとに許可される最大接続数。デフォルトの接続数は32です。

  デフォルトよりも多くの接続を有効にする場合は、クライアント設定を調整する必要があります（デフォルトの接続数は32）。

- `-max-lifs-per-session`

  マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。デフォルトは256のネットワークインターフェイスです。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAPがSMBマルチチャネルセッションを報告していることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、すべてのSMBセッションに関する情報を表示します。1つのセッションに対する複数の接続が表示されています。

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

次の例は、セッションID 1のSMBセッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Hyper-V over SMB または SQL Server over SMB アプリケーションサーバで使用する継続的可用性を備えた共有を設定する前に、 Storage Virtual Machine （ SVM ）上に NTFS データボリュームを作成する必要があります。ボリューム構成ワークシートを使用して、データボリュームを作成します。

タスクの内容

データボリュームのカスタマイズに使用できるオプションのパラメータが用意されています。ボリュームのカスタマイズの詳細については、を参照して"論理ストレージ管理"ください。

データボリュームの作成時に、次の項目を含むボリューム内にはジャンクションポイントを作成しないでください。

- ONTAP によってシャドウコピーが生成される Hyper-V ファイル
- SQL Server を使用してバックアップされる SQL Server データベースファイル

> mixed セキュリティ形式または UNIX セキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームを NTFS セキュリティ形式のボリュームに変更して、ノンストップオペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMBおよびSQL Server over SMBのノンストップオペレーションは、この構成で使用するボリュームをNTFSセキュリティ形式のボリュームとして作成しないと正しく機能しません。ボリュームを削除してNTFSセキュリティ形式でボリュームを再作成するか、Windowsホストでボリュームをマッピングしてボリューム上部にACLを適用し、ボリューム内のすべてのファイルとフォルダにACLを適用します。

手順

1. 適切なコマンドを入力して、データボリュームを作成します。

ボリュームを作成する **SVM** のルートボリュームのセキュリティ形式	入力するコマンド
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
NTFS ではありません	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. ボリュームの設定が正しいことを確認します。

   volume show -vserver *vserver_name* -volume *volume_name*

データボリュームを作成したら、アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルと SQL Server データベースファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB 共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

手順

1. 既存のデータボリュームとそのジャンクションパスに関する情報を表示します。

   volume show -vserver *vserver_name* -junction

2. 継続的可用性を備えたSMB共有を作成します。

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - 必要に応じて、共有設定にコメントを追加できます。
   - デフォルトでは、オフラインファイル共有プロパティは共有に設定され、に設定されます。 `manual`
   - ONTAPによって、Windowsのデフォルトの共有権限である/ `Full Control`が設定された共有が作成されます `Everyone`。

3. 共有設定ワークシートのすべての共有について同じ手順を繰り返します。
4. コマンドを使用して、設定が正しいことを確認し `vserver cifs share show`ます。
5. 継続的な可用性が確保された共有に NTFS ファイル権限を設定するには、各共有にドライブをマッピングし、 Windows のプロパティ * ウィンドウを使用してファイル権限を設定します。

例

次のコマンドを実行すると、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上に「 `d ata2` 」という名前の継続的可用性を備えた共有が作成されます。シンボリックリンクを無効にするには、パラメータをに `""`設定し `-symlink`ます。

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

ユーザアカウント（**SMB**共有の**SQL Server**用）に**SeSecurityPrivilege**権限を追加する

SQL Server のインストールに使用するドメインユーザアカウントには、デフォルトではドメインユーザに割り当てられていない権限を必要とする特定の操作を CIFS サーバで実行するために、「すべてのユーザ」権限を割り当てる必要があります。

必要なもの

SQL Server のインストールに使用するドメインアカウントがすでに存在している必要があります。

タスクの内容

SQL Server インストーラのアカウントに権限を追加するときに、 ONTAP がドメインコントローラに照会してアカウントを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. “s eepleed” 権限を追加します。

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   パラメータの値 `-user-or-group-name`は、SQL Serverのインストールに使用するドメインユーザアカウントの名前です。

2. 権限がアカウントに適用されていることを確認します。

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

例

次のコマンドでは、 Storage Virtual Machine （ SVM ） vs1 の EXAMPLE ドメインにある SQL Server インストーラのアカウントに「 `s eepleed` 」権限を追加しています。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

VSSシャドウコピーのディレクトリ階層の設定（**Hyper-V over SMB**共有用）

必要に応じて、シャドウコピーを作成する SMB 共有のディレクトリの最大階層を設定できます。このパラメータは、 ONTAP によってシャドウコピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

必要なもの

VSS シャドウコピー機能を有効にする必要があります。

タスクの内容

デフォルトでは、最大 5 つのサブディレクトリにシャドウコピーが作成されます。値がに設定されている場合 `0`、ONTAPはすべてのサブディレクトリにシャドウコピーを作成します。

> シャドウコピーセットのディレクトリ階層は 6 個以上のサブディレクトリまたはすべてのサブディレクトリを含むことができますが、シャドウコピーセットの作成は 60 秒以内に完了しなければならないという Microsoft の要件があります。この時間内に完了できない場合、シャドウコピーセットの作成は失敗します。作成時間が制限時間を超えないようにシャドウコピーのディレクトリ階層原因を設定しないでください。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. VSS シャドウコピーのディレクトリ階層を目的のレベルに設定します。

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. admin権限レベルに戻ります。

```
set -privilege admin
```

Hyper-VおよびSQL Server over SMB構成を管理します。

継続的可用性を確保するための既存の共有の設定

既存の共有を変更して、継続的可用性を備えた共有にすることができます。この共有は、Hyper-VおよびSQL Serverアプリケーションサーバが Hyper-V仮想マシンおよび構成ファイルおよびSQL Serverデータベースファイルに無停止でアクセスするために使用します。

タスクの内容

既存の共有に次の特徴がある場合、SMBを介したアプリケーションサーバでノンストップオペレーションを実現する継続的可用性を備えた共有として使用することはできません。

- その共有に共有プロパティが設定されている場合 `homedirectory`
- 共有に有効なシンボリックリンクまたはワイドリンクが含まれている場合
- 共有のルートの下にジャンクションされたボリュームが含まれている場合

次の2つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files`パラメータは（デフォルト）または `none`に設定されます `manual`。
- シンボリックリンクを無効にする必要があります。

次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。現在の共有プロパティのリストに含まれている場合は、継続的可用性を備えた共有から削除する必要があります。

- `attributecache`
- `branchcache`

手順

1. 現在の共有パラメータの設定と、設定済みの共有プロパティの現在のリストを表示します。

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. 必要に応じて、コマンドを使用して共有パラメータを変更し、シンボリックリンクを無効にし、オフラインファイルをmanualに設定し `vserver cifs share modify` ます。
   - シンボリックリンクを無効にするには、パラメータの値をに `""`設定し `-symlink`ます。
   - を指定すると、パラメータを正しい設定に `manual`設定できます `-offline-files`。
3. 共有プロパティを追加し、必要に応じて共有プロパティを追加し `continuously-available` `oplocks` ます。

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   共有プロパティがまだ設定されていない場合は `oplocks`、共有プロパティと一緒に追加する必要があります `continuously-available`。

4. 継続的な可用性が確保された共有でサポートされていない共有プロパティを削除します。

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   共有プロパティをカンマで区切って指定すると、1つ以上の共有プロパティを削除できます。

5. パラメータと `-offline-files`パラメータが正しく設定されていることを確認し `-symlink`ます。

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. 設定済みの共有プロパティのリストが正しいことを確認します。

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

例

次の例は、Storage Virtual Machine（SVM）「vs1」に「share1」という名前の既存の共有をSMBを介したアプリケーションサーバでのNDO用に設定する方法を示しています。

- パラメータをに設定すると、共有でシンボリックリンクが無効になります `-symlink` `""`。
- `-offline-file`パラメータが変更され、に設定され `manual`ます。

- `continuously-available`共有プロパティが共有に追加されます。
- `oplocks`共有プロパティはすでに共有プロパティのリストに含まれているため、追加する必要はありません。
- `attributecache`共有プロパティが共有から削除されます。
- `browsable`共有プロパティは、SMBを介したアプリケーションサーバでのNDOに使用される継続的可用性を備えた共有では省略可能で、共有プロパティの1つとして保持されます。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Hyper-V over SMBバックアップ用のVSSシャドウコピーの有効化と無効化

VSS 対応バックアップアプリケーションを使用して、 SMB 共有に格納された Hyper-V 仮想マシンファイルをバックアップする場合は、 VSS シャドウコピーを有効にする必要があります。VSS 対応バックアップアプリケーションを使用しない場合は、 VSS シャドウコピーを無効にできます。デフォルトでは、 VSS シャドウコピーは有効になっています。

タスクの内容

VSS シャドウコピーはいつでも有効または無効にできます。

手順

1. 権限レベルをadvancedに設定します。

   set -privilege advanced

2. 次のいずれかを実行します。

VSS シャドウコピーの設定	入力するコマンド
有効	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true**
無効にする	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false**

3. admin権限レベルに戻ります。

   set -privilege admin

例

次のコマンドを実行すると、 SVM vs1 で VSS シャドウコピーが有効になります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

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

統計を使用して**Hyper-V**および**SQL Server over SMB**のアクティビティを監視する

使用可能な統計オブジェクトとカウンタの確認

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	**statistics catalog object show**
使用可能な特定のオブジェクト	**statistics catalog object show object** ***object_name***
使用可能なカウンタ	**statistics catalog counter show object** ***object_name***

   使用可能なオブジェクトとカウンタの詳細については、マニュアルページを参照してください。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次のコマンドを実行すると、advanced権限レベルで表示した場合の、クラスタ内のCIFSアクセスとSMBアクセスに関連する選択した統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

次のコマンドを実行すると、advanced権限レベルで表示したオブジェクトの一部のカウンタに関する情報が表示され `cifs`ます。

> この例で表示されているのはオブジェクトの使用可能なカウンタの一部ではありませ `cifs`ん。出力は省略されています。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

ONTAPの**SMB**統計を表示します。

パフォーマンスを監視して問題を診断するために、さまざまなSMB統計を表示すること

ができます。

手順

1. コマンドとオプションの `statistics stop`コマンドを使用して、 `statistics start`データサンプルを収集します。
2. 次のいずれかを実行します。

統計を表示する対象	入力するコマンド
SMBのすべてのバージョン	**statistics show -object cifs**
SMB 1.0	**statistics show -object smb1**
SMB 2.xおよびSMB 3.0	**statistics show -object smb2**
ノードのSMBサブシステム	**statistics show -object nblade_cifs**

リンクの詳細については、コマンドリファレンスを参照してください。https://docs。NetApp .com /us-en/ ONTAP CLI / statistics-show.html^]、リンク：https://docs。NetApp .com /us-en/ ONTAP CLI / statistics-start.html[`statistics start`、およびリンク：https://docs。NetApp .com /us-en/ ONTAP CLI / statistics-stop.html[`statistics stop`^]コマンドの詳細[`statistics show`については、『ONTAPコマンドリファレンス』を参照してください。

構成がノンストップオペレーションに対応していることを確認する

ヘルス監視を使用してノンストップオペレーションのステータスが正常かどうかを確認する

ヘルスモニタを使用すると、クラスタ全体のシステムヘルスステータスに関する情報が得られます。ヘルスモニタは Hyper-V over SMB および SQL Server over SMB 構成を監視して、アプリケーションサーバの Nondisruptive Operation （ NDO ；ノンストップオペレーション）を実現します。ステータスがデグレードの場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を確認できます。

ヘルスモニタはいくつかあります。ONTAP では、システム全体の健全性と個々のヘルスモニタの健全性の両方が監視されます。ノード接続ヘルスモニタには、 CIFS-NDO サブシステムが含まれています。モニタには一連のヘルスポリシーがあり、特定の物理的な条件によってシステムが停止する可能性がある場合にアラートをトリガーするポリシーと、システム停止が発生している場合にアラートが生成し、対処方法に関する情報を提供するポリシーがあります。SMB を介した NDO 構成では、アラートは次の 2 つの状態で生成されます。

アラートID	重大度	条件
HaNotReadyCifsNdo_Alert	メジャー	ノード上のアグリゲート内のボリュームでホストされている1つ以上のファイルが、継続的可用性を備えたSMB共有を介して開かれており、障害が発生した場合でも継続性が保証されるはずですが、パートナーとのHA関係が設定されていないか正常ではありません。
NoStandbyLifCifsNdo_Alert	マイナー	Storage Virtual Machine （ SVM ）はノードから SMB を介してアクティブにデータを提供しており、SMB ファイルは継続的可用性を備えた共有を介して継続的に開かれているが、そのパートナーノードが SVM のアクティブなデータ LIF を公開していない。

システムヘルスの監視を使用してノンストップオペレーションのステータスを表示します。

コマンドを使用すると、クラスタのシステムヘルス全体およびCIFS-NDOサブシステムのヘルスに関する情報の表示、アラートへの応答、以降のアラートの設定、ヘルスモニタの設定に関する情報の表示を行うことができます `system health`。

手順

1. 適切な操作を実行して、ヘルスステータスを監視します。

表示する項目	入力するコマンド
個々のヘルスモニタのステータス全体が反映された、システムのヘルスステータス	**system health status show**
CIFS-NDO サブシステムのヘルスステータスに関する情報	**system health subsystem show -subsystem CIFS-NDO -instance**

2. 適切な操作を実行して、 CIFS-NDO アラートの監視がどのように設定されているかに関する情報を表示します。

表示する情報	入力するコマンド
監視対象のノード、初期化状態、ステータスなど、CIFS-NDO サブシステムのヘルスモニタの設定とステータス	**system health config show -subsystem CIFS-NDO**
ヘルスモニタで生成される可能性がある CIFS-NDO アラート	**system health alert definition show -subsystem CIFS-NDO**

表示する情報	入力するコマンド
アラートが発行されるタイミングを決定する、CIFS-NDO ヘルスモニタのポリシー	**system health policy definition show -monitor node-connect**

詳細な情報を表示するには、パラメータを使用し `-instance`ます。

例

次の出力は、クラスタおよび CIFS-NDO サブシステムのヘルスステータス全体に関する情報を示しています。

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                    Subsystem: CIFS-NDO
                       Health: ok
         Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                         Node: node2
  Subsystem Refresh Interval: 5m
```

次の出力は、 CIFS-NDO サブシステムのヘルスモニタの設定とステータスに関する詳細な情報を示しています。

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

継続的可用性を備えた**SMB**共有の設定の確認

ノンストップオペレーションをサポートするには、 Hyper-V および SQL Server の SMB 共有が継続的可用性を備えた共有として設定されている必要があります。また、それ以外にも、いくつかの共有設定について確認が必要になります。計画的または計画外の停止が発生する状況でアプリケーションサーバのノンストップオペレーションをシームレスに実行できるように、共有が適切に設定されていることを確認してください。

タスクの内容

次の2つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files`パラメータは（デフォルト）または `none`に設定されます `manual。
- シンボリックリンクを無効にする必要があります。

ノンストップオペレーションが適切に実行されるようにするには、次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

手順

1. オフラインファイルがまたは `disabled`に設定されていること、およびシンボリックリンクが無効になっていることを確認し `manual`ます。

   vserver cifs shares show -vserver *vserver_name*

2. SMB 共有が継続的可用性を確保するように設定されていることを確認します。

   vserver cifs shares properties show -vserver *vserver_name*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 share1 」という名前の共有の共有設定を表示します。オフラインファイルはに設定され、シンボリックリンクは無効になってい `manual`ます（出力フィールドにハイフンが表示され `Symlink Properties`ます）。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
            Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例は、 SVM vs1 上の「 share1 」という名前の共有の共有プロパティを表示します。

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

LIFステータスの確認

Hyper-VおよびSQL Server over SMB構成のStorage Virtual Machine（SVM）をクラスタ内の各ノードにLIFを配置するように設定した場合でも、日常業務中に一部のLIFが別のノードのポートに移動することがあります。LIF のステータスを確認して、必要な措置を講じる必要があります。

タスクの内容

シームレスなノンストップオペレーションの運用支援を提供するには、クラスタ内の各ノードの SVM に少なくとも 1 つの LIF を配置し、すべての LIF をホームポートに関連付ける必要があります。設定されている LIF の中に現在ホームポートに関連付けられていないものがある場合は、ポートの問題を修正してから、対応するホームポートに LIF をリバートする必要があります。

手順

1. 設定されている SVM の LIF に関する情報を表示します。

   network interface show -vserver *vserver_name*

   この例では、「 lif1 」はホームポートに配置されていません。

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

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

2. 対応するホームポートに関連付けられていない LIF がある場合は、次の手順を実行します。

   a. それぞれの LIF について、 LIF のホームポートを確認します。

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

      network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

      ```
      vserver lif  home-node  home-port
      ------- ---- ---------- ---------
      vs1     lif1 node1      e0d
      ```

   b. それぞれの LIF について、 LIF のホームポートが up 状態になっているかどうかを確認します。

      network port show -node *node_name* -port *port* -fields port,link

      ```
      network port show -node node1 -port e0d -fields port,link
      ```

      ```
      node       port link
      ---------- ---- ----
      node1      e0d  up
      ```

      +
      この例では、「lif1」をホームポートに戻す必要があります `node1:e0d`。

3. LIFを関連付けるホームポートのネットワークインターフェイスが状態になっていない場合は `up`、問題を解決してup状態にします。
4. 必要に応じて、ホームポートに LIF をリバートします。

   network interface revert -vserver *vserver_name* -lif *lif_name*

```
network interface revert -vserver vs1 -lif lif1
```

5. クラスタ内の各ノードにアクティブな SVM の LIF があることを確認します。

```
network interface show -vserver vserver_name
```

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

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

SMBセッションの継続的可用性の確認

SMBセッション情報を表示する

SMB接続、SMB Session ID、セッションを使用しているワークステーションのIPアドレスなど、確立されているSMBセッションに関する情報を表示できます。セッションのSMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

タスクの内容

SVM上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのパラメータを使用すると、選択したフィールドに関する出力を表示できます `-fields`。

  と入力して、使用できるフィールドを指定できます `-fields ?`。

- パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます `-instance`。
- パラメータまたは `-instance`パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます `-fields`。

手順

1. 次のいずれかを実行します。

表示する **SMB** セッション情報	入力するコマンド
SVM上のすべてのセッション（要約形式）	**vserver cifs session show -vserver *vserver_name***
指定した接続IDのファイル	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
指定したワークステーションのIPアドレスから	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
指定したLIF IPアドレスのファイル	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
指定したノードのオブジェクト	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	指定したWindowsユーザからのセッション
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* の形式 `user_name` はです `[domain]\user`。	指定した認証メカニズムを使用している場合
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism には、次のいずれかの値を `-auth-mechanism` 指定できます。 • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	指定したプロトコルバージョンを使用している場合

表示する **SMB** セッション情報	入力するコマンド
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version には、次のいずれかの値を `-protocol-version`指定できます。 • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 継続的可用性を備えた保護とSMBマルチチャネルは、SMB 3.0以降のセッションでのみ使用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を以降に設定します。SMB3	指定したレベルの継続的可用性を備えた保護を使用しているセッション

表示する **SMB** セッション情報	入力するコマンド
vserver cifs session show -vserver *vserver_name* -continuously -available *continuously_available_protection_level* には、次のいずれかの値を `-continuously-available`指定できます。 • No • Yes • Partial	指定したSMB署名セッションステータスのセッション

例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。接続はドメインアカウントを使用して行われました。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
               Connected Time: 10m 43s
                    Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

次のコマンドを実行すると、SVM vs1上のSMB 3.0とSMBマルチチャネルを使用しているセッションに関するセッション情報が表示されます。この例では、ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するには、Kerberos認証を使用して接続を確立する必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

開いている**SMB**ファイルに関する情報を表示する

SMB接続とSession ID、ホスティングボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報も表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

タスクの内容

確立されたSMBセッションで開いているファイルに関する情報を表示できます。表示される情報は、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと継続的可用性を備えた保護を使用して開かれていないファイルがある場合（コマンド出力のフィールド `vserver cifs session show`の値 `-continuously-available`は `Partial`）、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

オプションのパラメータを何も指定せずにコマンドを実行することで、Storage Virtual Machine（SVM）上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show`。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションのパラメータを使用すると、選択したフィールドの出力を表示できます `-fields`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

- パラメータを使用すると、開いているSMBファイルに関する詳細情報を表示できます `-instance`。

  このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

手順

1. 次のいずれかを実行します。

表示する開いている **SMB** ファイル	入力するコマンド
SVM上のファイル（要約形式）	**vserver cifs session file show -vserver *vserver_name***
指定したノードのオブジェクト	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	指定したファイルIDのファイル
vserver cifs session file show -vserver *vserver_name* -file-id integer	指定したSMB接続IDのファイル
vserver cifs session file show -vserver *vserver_name* -connection-id integer	指定したSMB Session IDのファイル
vserver cifs session file show -vserver *vserver_name* -session-id integer	指定したホストアグリゲートのファイル
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	指定したボリュームのファイル
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	指定したSMB共有のファイル
vserver cifs session file show -vserver *vserver_name* -share *share_name*	指定したSMBパスのファイル

表示する開いている **SMB** ファイル	入力するコマンド
vserver cifs session file show -vserver *vserver_name* -path *path*	指定したレベルの継続的可用性を備えた保護を使用している
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* には、次のいずれかの値を `-continuously-available` 指定できます。 • No • Yes 継続的可用性のステータスがの場合は No、開いているファイルがテイクオーバーやギブバックからの無停止でのリカバリに対応していません。また、ハイアベイラビリティ関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。	指定した再接続状態のファイル

出力結果の絞り込みに使用できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

著作権に関する情報

商標に関する情報